Post Quantum Cryptography in IoT Ecosystem

Version 1.0

25/11/2024

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

Table of Contents

1 Introduction

1.1 Overview

The Internet of Things (IoT) is a disruptive technology that plays an increasingly important role in digital transformation, as the number of connected devices and applications increase. The collection of data from different sources enables the ability to gain insights, make data-driven decisions, and automate processes, and this is being used by consumers, governments and businesses in an expanding range of sectors, use cases and applications.

In our increasingly connected world, IoT security and privacy is an ongoing concern against the backdrop of an evolving threat landscape, complex value chains and the expanding criticality and complexity of IoT use cases. As consumers, businesses and governments increasingly rely on more devices that collect and communicate more information and make more decisions on our behalf, security vulnerabilities in the IoT domain could produce severe consequences.

In this regard, as quantum computing technologies mature, it is necessary to consider the impact of the quantum threat; namely the prospect that bad actors armed with a cryptographically relevant quantum computer could compromise the cryptographic algorithms currently used to secure IoT systems. Post Quantum Cryptography (PQC) refers to cryptographic algorithms that are resistant to the attack of both classical and quantum computers. Over the past decade the global cryptography community has engaged in the development and testing of such algorithms, resulting in a first set of post quantum cryptography standards [1],[2],[3]. These new algorithms are not a drop-in replacement for legacy algorithms and may therefore pose challenges to IoT solutions in use cases where there are performance constraints, such as limited bandwidth, limited processing or limited storage.

This document aims to provide a first impact analysis regarding the quantum threat in the IoT context, with a view on providing information and guidance on how to mitigate the threat over the coming years, including the introduction of post quantum cryptography and crypto agility. Due to the nature of IoT and the breadth of solutions and use cases it underpins, a balanced and risk-based approach will be required, to manage the complex and evolving technology, regulatory and certification landscape that may impact deployment of new solutions or the migration strategy of existing solutions.

1.2 Scope

This document analyses the risks posed by the advancement of quantum computing on IoT systems, focusing on solutions that are connected using 3GPP based connectivity, in both terrestrial and non-terrestrial networks [4], in the first instance. It aims to provide stakeholders and decision makers with an understanding of the challenges and actionable insights, to enable an informed strategy for securing IoT solutions against emerging quantum risks and future proofing strategies.

The quantum threat should be considered within a broader landscape of cyber security threats, with the implication that existing vulnerabilities will not by default be addressed through the implementation of quantum safe solutions.

1.3 Intended Audience

The document is designed for a diverse group of stakeholders involved in the design, deployment, operation, security and use of IoT systems, including the providers/developers of system components. It is also expected to be of interest to those that are leveraging IoT solutions in their business and to regulators and policy makers developing guidance to address quantum related challenges at a national level and/or for specific sectors.

By addressing these groups, the document aims to foster an understanding and awareness of the quantum threat and promote ecosystem collaboration towards building secure, quantum resilient IoT solutions.

1.4 Abbreviations

Term	Description
3GPP	3rd Generation Partnership Project (organisation)
AES	Advanced Encryption Standard
AMQP	Advanced Message Queuing Protocol
ANSSI	National Cyber Security Agency of France (Agence nationale de la sécurité des systèmes d'information)
API	Application Programming Interface
APN	Access Point Name (in 3GPP)
Ascon	A family of lightweight authenticated ciphers
BACnet	Building Automation and Control Networks
BIKE	Bit Flipping Key Encapsulation
BSI	Germany's Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
CAMARA	Open-source project within Linux Foundation
CAN	Controller Area Network
CAT-M1	Category M1, a low-power wide area cellular technology
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
CRQC	Cryptographically Relevant Quantum Computers
DH	Diffie–Hellman
DNS	Domain Name System
DSA	Digital Signature Algorithm

DTLS	Datagram Transport Layer Security
EDHOC	Ephemeral Diffie-Hellman Over COSE
ECDH	Elliptic-curve Diffie–Hellman (key agreement protocol)
eSIM	Embedded SIM
eUICC	Embedded Universal Integrated Circuit Card
FIPS	Federal Information Processing Standard
FN-DSA	Falcon Digital Signature Algorithm
FTP	File Transfer Protocol
HQC	Hamming Quasi-Cyclic
HTTP(S)	Hypertext transfer protocol (secure)
IANA	Internet Assigned Numbers Authority
ID	Identity
IETF	Internet Engineering Taskforce
IKE	Internet Key Exchange
IoT	Internet of Things
IP-SEC	Internet Protocol Security
IKEv2	Internet Key Exchange version 2
IPSECME	IP Security Maintenance and Extensions
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
iSIM	Integrated SIM
KEM	Key Encapsulation Mechanism
LMS	Leighton-Micali Signatures
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
LTE-M	Long Term Evolution Machine Type Communication
M2M	Machine To Machine
MFA	Multi-Factor Authentication
ML-DSA	Module-Lattice-Based Digital Signature Algorithm Standard
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism Standard
MQTT	Message Queuing Telemetry Transport
MQTT-SN	MQTT for Sensor Networks

MNO	Mobile Network Operator
NB-IoT	Narrowband Internet of Things (radio technology standard)
NCSC	UK's National Cyber Security Centre
NEF	Network Exposure Function
NIDD	Non-IP data delivery
NIST	National Institute of Standards and Technology
NSA	U.S. National Security Agency
OAuth 2.0	Open Authorization, an open standard
OIDC	OpenID Connect, identity authentication protocol
OMA	Open Mobile Alliance
OMA DM	OMA Device Management
OMA LwM2M	Lightweight M2M
OneM2M	One Machine to Machine
PKI	Public Key Infrastructure
PROFINET	PROcess FIeld NETwork
PQC/T	Post-Quantum Traditional
PQC	Post Quantum Cryptography
PQTN TF	Post Quantum Telco Network Task Force
RAM	Random Access Memory
RAN	Radio Access Network
REST	Representational State Transfer
RFC	Request for Comment (type of IETF publication)
ROM	Read Only Memory
RSA	Rivest–Shamir–Adleman, a public-key cryptosystem
RSP	Remote SIM Provisioning
RTOS	Real Time Operating System
SAML	Security Assertion Markup Language
SDO	Standardisation Bodies
SESIP	Security Evaluation Standard for IoT Platforms
SCEF	Service Capability Exposure Function
SIM	Subscriber Identity Module
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SNDL	Store now decrypt later

SoC	System on Chip
SSH	Secure Shell (network protocol)
SSO	Single Sign-On
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UK	United Kingdom
URL	Uniform Resource Locator (web address)
USIM	Universal Subscriber Identity Module
VPN	Virtual Private Network
WebRTC	Web Real-Time Communication
WS-FED	Web Services Federation
XMSS	eXtended Merkle Signature Scheme

Table 1: Abbreviations

1.5 References

Ref	Doc Number	Title
[1]	FIPS 203	Module-Lattice-Based Key-Encapsulation Mechanism Standard https://doi.org/10.6028/NIST.FIPS.203
[2]	FIPS 204	Module-Lattice-Based Digital Signature Standard https://doi.org/10.6028/NIST.FIPS.204
[3]	FIPS 205	Stateless Hash-Based Digital Signature Standard https://doi.org/10.6028/NIST.FIPS.205
[4]	PQ.03 v2.0	Post Quantum Cryptography – Guidelines for Telecom Use Cases Version 2.0 https://www.gsma.com/newsroom/wp-content/uploads//PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-Cases-v2.0-2.pdf
[5]	The Mobile Economy 2024	The Mobile Economy 2024 https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf
[6]	SGP.31 v1.2	eSIM IoT Architecture and Requirements https://www.gsma.com/solutions-and-impact/technologies/esim/wp-content/uploads/2024/04/SGP.31-v1.2.pdf
[7]	SGP.32 v1.2	eSIM IoT Technical Implementation https://www.gsma.com/solutions-and-impact/technologies/esim/wp-content/uploads/2024/06/SGP.32-v1.2.pdf

Ref	Doc Number	Title
[8]	IoT SAFE	https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/iot-safe/
[9]	CAMARA API	CAMARA APIs Access and User Consent Management, https://github.com/camaraproject/IdentityAndConsentManagement/blob/main/documentation/CAMARA-API-access-and-user-consent.md
[10]	PQ.02 v1.0	Guidelines for Quantum Risk Management for Telco
[11]	NIST SP 800-232	Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions https://csrc.nist.gov/pubs/sp/800/232/ipd
[12]	RFC 9528	Ephemeral Diffie-Hellman Over COSE https://datatracker.ietf.org/doc/rfc9528/
[13]	NIST SP 800-208	Recommendation for Stateful Hash-Based Signature Schemes https://csrc.nist.gov/pubs/sp/800/208/final
[14]	Open Quantum Safe	Open Quantum Safe: Algorithms in liboqs Algorithms | Open Quantum Safe
[15]	IETF ipsecme	IP Security Maintenance and Extensions (ipsecme) https://datatracker.ietf.org/group/ipsecme/documents/
[16]	RFC9370	Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) https://datatracker.ietf.org/doc/rfc9370/
[17]	RFC9242	Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2) https://datatracker.ietf.org/doc/rfc9242/
[18]	draft-ietf-tls-hybrid-design-11	Hybrid key exchange in TLS 1.3 https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
[19]	FIPS 140-3	Security Requirements for Cryptographic Modules https://csrc.nist.gov/pubs/fips/140-3/final
[20]	draft-becker-cnsa2-tls-profile-00	Commercial National Security Algorithm (CNSA) Suite Profile for TLS 1.3 https://datatracker.ietf.org/doc/html/draft-becker-cnsa2-tls-profile
[21]	draft-connolly-tls-mlkem-key-agreement-05	ML-KEM Post Quantum Key Agreement for TLS 1.3 https://datatracker.ietf.org/doc/html/draft-connolly-tls-mlkem-key-agreement-05
[22]	draft-reddy-tls-composite-mldsa	Use of Composite ML-DSA in TLS 1.3 https://datatracker.ietf.org/doc/html/draft-reddy-tls-composite-mldsa

Ref	Doc Number	Title
[23]	draft-tls-westerbaan-mldsa	Use of ML-DSA in TLS 1.3 https://datatracker.ietf.org/doc/html/draft-tls-westerbaan-mldsa
[24]	draft-reddy-tls-slhdsa	Use of SLS-DSA in TLS 1.3 https://datatracker.ietf.org/doc/html/draft-reddy-tls-slhdsa
[25]	draft-ietf-tls-key-share-prediction-01	TLS Key Share Prediction https://datatracker.ietf.org/doc/draft-ietf-tls-key-share-prediction/
[26]	RFC 9147	The Datagram Transport Layer Security (DTLS) Protocol Version 1.3 https://datatracker.ietf.org/doc/html/rfc9147
[27]	draft-reddy-uta-pqc-app-0	Post-Quantum Cryptography Recommendations for Applications https://www.ietf.org/archive/id/draft-reddy-uta-pqc-app-04.html
[28]	draft-kampanakis-curdle-ssh-pq-ke-04	PQ/T Hybrid Key Exchange in SSH https://datatracker.ietf.org/doc/html/draft-kampanakis-curdle-ssh-pq-ke-04
[29]	draft-josefsson-ntruprime-ssh-03	Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512 https://datatracker.ietf.org/doc/draft-josefsson-ntruprime-ssh/
[30]	IoT Guide	IoT Guide: Global IoT Regulation https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/gsma_resources/iot-guide-global-iot-regulations/
[31]	ENISA IoT	Baseline Security Recommendations for IoT https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[32]	NSA's CNSA 2.0	The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ

Table 2: References

2 Executive Summary

This report provides an initial analysis of the impact of quantum computing and crypto-agility on IoT systems and the necessary steps to mitigate associated risks. As quantum computing technologies advance, they pose a significant threat to the cryptographic algorithms currently used to secure IoT systems in multiple industry sectors. The goal is to provide stakeholders with an understanding of these challenges and actionable insights to secure IoT solutions against emerging quantum risks.

The report focuses on IoT systems connected using *3GPP-based connectivity*, including both terrestrial and non-terrestrial networks. This version is intended as an introduction for stakeholders involved in the design, deployment, operation, security, and use of IoT systems, as well as regulators and policymakers.

The increasing reliance on IoT devices and solutions raises security and privacy concerns. This is especially true with the advent of quantum computing, which bad actors can potentially use to compromise currently deployed asymmetric cryptography systems, necessitating the adoption of quantum-resilient PQC. The present document outlines the specific challenges posed by quantum computing to IoT security. It emphasises the importance of considering the quantum threat throughout the lifecycle of IoT solutions, particularly for long-lived devices with limited upgrade capabilities.

The document briefly summarizes the various components of IoT architecture and the role of cryptography in securing these components. Quantum-robust mutual authentication, end-to-end encryption, and secure firmware updates are essential to ensure the security of IoT devices. An overview of relevant standards for cryptographic algorithms and communication protocols using such algorithms in the context of IoT is provided. This is followed by a discussion of the challenges of integrating PQC algorithms into existing security protocols like IPSec, TLS, DTLS, and SSH. The new quantum-safe cryptography algorithms and the way communication protocols like TLS will likely use these algorithms, both pose new requirements on IoT devices and potentially impact performance.

The document outlines a roadmap for implementing PQC in IoT systems, considering the ecosystem, policy, and regulatory aspects, emphasizing the need for a balanced and risk-based approach to manage the complex and evolving technology landscape.

As a main conclusion it is important to implement proactive measures to address the quantum threat in IoT systems. By adopting PQC and ensuring crypto-agility, stakeholders can future-proof IoT solutions and maintain security in the face of advancing quantum computing technologies.

3 IoT and the Quantum threat

Due to the diverse nature of the solutions addressed, security in IoT poses specific challenges. These challenges and how they should be addressed depends on the use case: relevant considerations include business criticality as well as technology and cost constraints throughout the solution lifecycle.

IoT is a groundbreaking technology that has a disruptive impact on society and businesses across all sectors, providing an intersection between the physical and digital world. The vast

and increasing number of interconnected IoT devices unlock opportunities for automation, efficiency, data driven decision making and monitoring, radically evolving, for example, how we use and interact with vehicles or how patient care is delivered. IoT is underpinned by different connectivity technologies (standard and proprietary), which impact the level of security of an overall solution and connected systems. Examples of connectivity technologies include Wi-Fi, Bluetooth, LoRaWAN, 5G, 4G, 3G, and 2G. This document focuses on standard, 3GPP-based connectivity. In many cases, the choice of using a standard, cellular based technology for IoT solutions is driven, amongst other considerations, by a requirement for higher security. Currently, cellular networks account for approximately 15% of total IoT connections and are expected to reach 5.8Bn connections globally by 2030 [5] The Mobile Economy 2024.

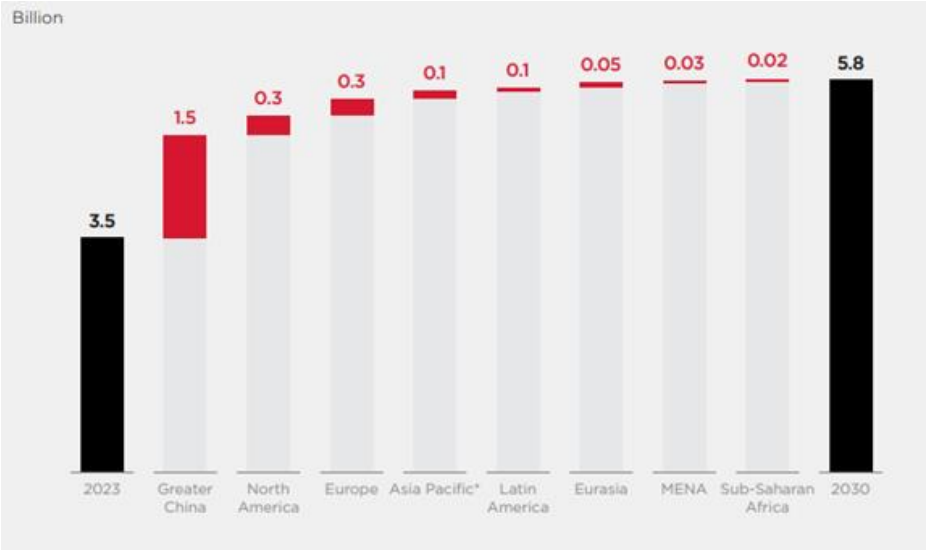

Figure 1*:* Licensed cellular IoT connections, GSMA Intelligence

The widescale adoption of IoT by consumers and across industries, often involving sensitive data and critical systems, is closely intertwined with security and trust: the convergence of IoT and cybersecurity is integral to future growth. The breadth of IoT solutions reflects the broad set of use cases that IoT addresses, which means there is no one-solution-fits-all: IoT security challenges are linked to commercial viability, operational aspects (such as long device lifecycles or device upgrade/accessibility limitations) and technology constraints.

As the number of IoT devices and IoT solutions increase, so do opportunities for attackers. Tampering, eavesdropping, malware, and unauthorised access are some examples of how confidentiality, integrity of data and availability of systems can be compromised. Cryptography underpins the security of IoT solutions: keeping the data secure through encryption, securing communications, providing user authentication to prevent unauthorised access, validating data integrity.

The quantum threat to cryptography in the context of IoT should be considered throughout the lifecycle of the solution and across all components: a plan for the implementation of measures to mitigate risks for existing and for new solutions will provide opportunities to reduce costs and manage risks. Lifecycle security considerations with regard to the quantum threat can be particularly relevant in the IoT context. IoT devices may be deployed with embedded cryptography that is expected to function securely, in the field, for many years. If

there is no easy or feasible way to update this cryptography during the lifecycle of a device, as may occur, for example, with hardware-based solutions, the embedded cryptography may fail to retain the intended security properties in the face of unanticipated emerging threats. As a concrete example, an IoT device with embedded cryptography that achieves authentication via methods that are vulnerable to quantum attack may nonetheless be sufficiently secure to use in the present-day, since no present-day quantum computer can undertake real-time authentication attacks, and future quantum computers cannot retrospectively invalidate authentication processes for expired sessions/connections. However, if such an IoT device with quantum-vulnerable cryptography remains deployed in the field at a future point when real-time or quasi-real-time quantum computing based attacks become viable, security could be compromised. This example emphasises the importance of lifecycle considerations, particularly for IoT devices with long lifecycles and with limited ability to upgrade or update embedded cryptography.

Devices deployed with quantum-vulnerable cryptography with expectation of a long lifecycle may lose their security properties as quantum computing technologies advance. This quantum threat differs to the Store Now, Decrypt Later (SNDL) attack, in which bad actors harvest and store encrypted traffic with the aim to decrypt it with a future, sufficiently powerful, quantum computer to reveal long-lived secrets. For the SNDL attack, the lifecycle of the communicated data is a key consideration, whereas for IoT devices deployed in the field, the above example shows that the lifecycle of the device itself can also be an important factor. Hence for long-lived IoT devices, the quantum threat may already be a relevant consideration. The SNDL threat is already present, and other threats (as listed in Figure 2) may also be already problematic today in circumstances where IoT devices cannot be upgraded and have a long lifecycle, and will likely become an issue for other IoT devices when a Cryptographically Relevant Quantum Computer (CRQC) becomes available in the future.

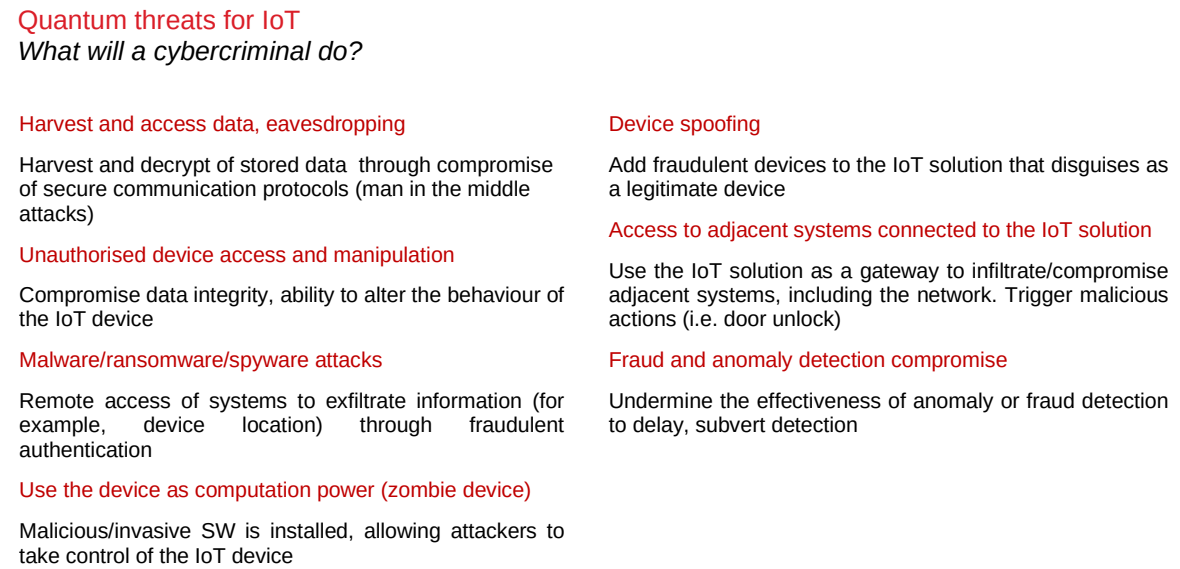

Figure 2: Cyber risks to classically protected IoT systems from quantum computing.

4 Cryptography in IoT

4.1 IoT Categorisation

Cellular IoT devices can be categorised into several types based on their network specifications, functionality/role, use cases, and capabilities:

Based on Network Specification:

- Low Power Wide Area (LPWA) Network Devices:
    - Narrow Band Internet of Things (NB-IoT): Such devices are characterised by low data usage, low mobility, and reliance on long-term battery lifetime.
    - Category M1, a low-power wide area cellular technology (CAT-M1) Long Term Evolution Machine Type Communication (LTE-M): similar to NB-IoT but with slightly different specifications, such as extended coverage and low device cost.
- Cellular network devices (5G, 4G, 3G, 2G):
    - Used for applications requiring higher data rates and broader coverage, though they consume more power.

Based on Functionality and Role:

- Connected endpoints: e.g. IoT devices which collect data, like sensors and video cameras. Examples are cellular sensor platforms for smart cities including environmental monitoring, and 4G LTE security cameras (including solar powered devices for off-the-grid monitoring).
- Connected enablers: e.g. wireless gateways, whose role ranges from providing wireless (cellular) connectivity to providing extra processing capability to other devices connected to them through other means (in turn wireless like Bluetooth, Zigbee, Matter or non-wireless protocol technologies like Modbus (industrial automation, PROcess FIeld NETwork (PROFINET (automation)), Controller Area Network (CAN) Bus (vehicles), Building Automation and Control Networks (BACnet) (building automation), and others).
- Connected controllers: e.g. control units and smart hubs, whose key role is to manage and control additional IoT devices connected to them. Examples of such connected devices are smart lights, thermostats, industrial sensors, and wearable devices.

Based on Use Cases and Solutions:

- Mobile Asset Tracking: Devices used for tracking mobile assets (from a bag to a container).
- Connected Cabinets: Devices used for monitoring and controlling connected cabinets.

- Remote Monitoring & Control: Devices used for remote monitoring and control applications.
- Internet in the Car: Devices providing internet connectivity in vehicles.
- Stolen Vehicle Tracking: Devices used for tracking stolen vehicles.
- Usage-Based Insurance: Devices used for insurance purposes based on usage.
- Fleet Telematics: Devices used for fleet management and telematics.
- Digital Buildings: Devices used for managing and monitoring digital buildings.

Based on Capabilities:

- Constrained devices, whereby the constraints result from
    - *Processing constraints* (e.g. low-cost processors, lack of hardware accelerators),
    - *Memory constraints* (e.g. very limited amount of RAM for computations or ROM to store code for multiple algorithms),
    - *Power supply constraints* (e.g. reliant on battery with long lifetime),
    - *Security constraints* (e.g. no trusted platform module/secure element or dedicated secure key storage in the device).

  An example for constrained devices is a cellular asset tracker.
- *Unconstrained devices:* Examples can be cellular consumer and industrial smart hubs.

A given IoT device can fall into multiple (orthogonal) categories. The categories which apply to a device under consideration can provide useful hints regarding, for example:

- The importance or criticality of migrating to quantum-safety. For instance, considering the category “Use Cases”, remote monitoring & control using ruggedised IoT terminals for utilities (national critical infrastructure) will be more mission critical than consumer IoT devices.
- The importance and impact of quantum vulnerabilities from an overall system architecture perspective. For example, based on the category “Functionality and Role”, the economic risk associated with a cellular connected controller that manages dozens of industrial devices is likely higher than the economic risk associated with a single connected sensor.
- How well a device is equipped to support new PQC algorithms (e.g. based on the category “Capabilities”). There is a distinction between the evolution of existing devices and the design of new ones.
- Whether particular quantum-safety considerations are inherited from a wider class of cellular devices (e.g. mass market 5G and 4G smartphones), based on the category

"Network Specification". For instance, quantum safety considerations identified for 5G/4G smartphones will also be largely applicable for 4G IoT devices.

4.2 IoT Architecture

Figure 3 illustrates the main components of IoT solutions considered as part of this document. The architectures that underpin different IoT solutions will vary depending on the business task being addressed and, in some cases, will rely on external components that will need to be considered in the context of the IoT solution lifecycle.

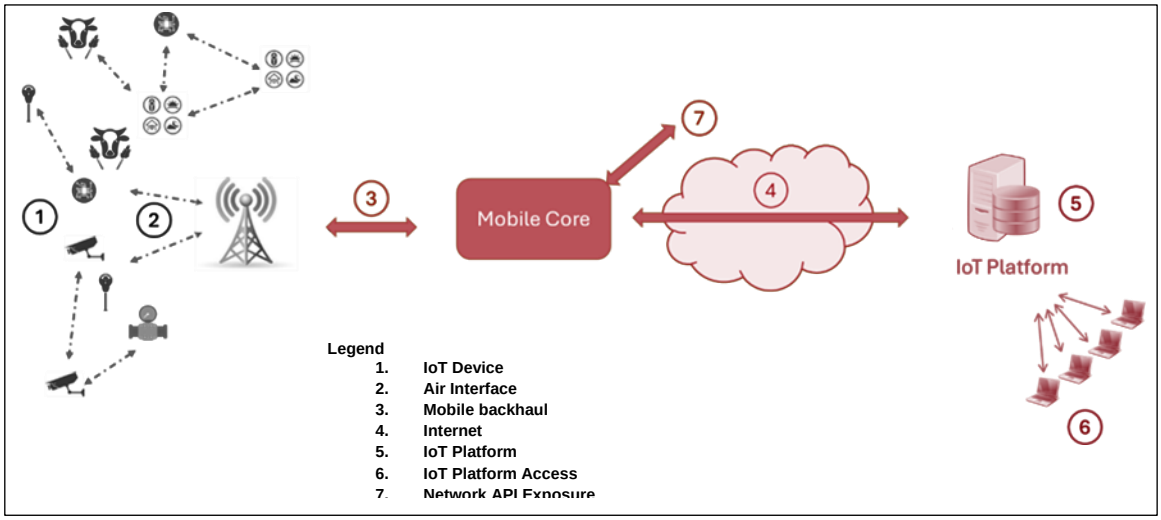

Figure 3: Main components of IoT solutions in scope of this document.

4.2.1 IoT device

As described in Section 4.1, IoT devices support a diverse range of use cases with differing requirements, capabilities and constraints. For example, the CPU processing power in an LPWA IoT device used for remote sensing of temperature and humidity is typically much less than that in a cellular handset.

Some IoT devices are Android or Linux based but many only support a simple real-time operating system (RTOS). Depending on the application / use case, some devices may also be fitted with separate cryptography chips with limited or no ability to support a software update.

Like a mobile handset, cellular IoT devices will be fitted with some sort of SIM and therefore face the same authentication issues faced by handsets. However, as indicated in Figure 3, IoT devices should also mutually authentice to an IoT platform, and, as such, the security of that is an additional consideration for PQC migration. Some IoT devices may utilise end-to-end encryption using (D)TLS or similar, whereas others may rely on encryption on a per-hop basis.

Remote SIM Provisioning (RSP) in IoT allows for the remote provisioning of operator profiles on the embedded Universal Integrated Circuit Card (eUICC, part of, for example, an eSIM in an IoT device). This means that operator profiles can be installed, switched, and deleted either via the user or over-the-air (OTA) without the need for physical access to the device.

The GSMA has published several documents to support the adoption of RSP for IoT. These include the *eSIM IoT Architecture & Requirements* (SGP.31 [6]) and the *eSIM IoT Technical Specification* (SGP.32 [7]). From a quantum safety point of view, RSP for IoT is vulnerable to quantum attacks due to the recommended use of TLS, DTLS and recommended cipher suites that include asymmetric cryptography (e.g. in form of ECDHE, ECDSA, etc.). There are several communication interfaces between the RSP system with its RSP servers and the eUICC platform, which are not quantum resistant today. For more details, see Section 5.6 of reference [4]. The GSMA eSIM Group is actively working on a PQC version of RSP.

Additionally, some IoT devices may be using the GSMA IoT SAFE application [8], which leverages the SIM as a hardware root of trust, and the post quantum security of that usage would need to be considered.

Ultra secure devices may be using a trusted platform module for their system on chip (SoC) and the device application firmware may even be encrypted and stored in memory integral to the system on chip with the code being decrypted on the fly. Such applications are few and far between, but they do exist to prevent well-resourced attackers from reverse engineering the code.

4.2.2 Air Interface

Similar to a handset, the air interface provides encryption services and integrity checking. IoT applications that are not using end-to-end encryption will be relying on this over-the-air encryption, though this encryption is removed at the base station.

Whilst strictly speaking not an air interface function, many IoT applications may be using a dedicated Access Point Name (APN) or network slice for their operation to ringfence the application.

IoT devices may use free, but regulated, radio frequencies (which vary depending on the geographical area). This implies that the frequency of messages sent and received, and the amount of data sent and received may be narrowed (i.e. resulting in possible impact on latency to deliver or receive messages).

4.2.3 Mobile Backhaul

Mobile backhaul may be transported over fibre or high-speed microwave. It can be provided directly by the mobile network operator, a third-party transport provider or even through tunnelling over the Internet.

Typically, IoT traffic is multiplexed into the same transport bearer as other mobile user plane data and control plane signalling. Encryption of these transport bearers is at the discretion of the mobile network operator (MNO).

Some MNOs only encrypt the transport bearer using IP-SEC tunnels or similar if the traffic is carried by 3rd party providers or over the Internet. Otherwise, they rely on the physical security of the bearer, e.g. fibre.

4.2.4 Internet

Connection between the mobile core and the IoT platform is not that different to mobile backhaul, although whereas many operators may predominantly be using their own fibre or

high-speed microwave for mobile backhaul, the reverse is probably the case for connection to the IoT platform. That is, use of dedicated fibre or high-speed microwave to connect to an IoT platform is likely to be limited.

Most connections to the IoT platform are likely to be through IP-SEC tunnels or even over the open Internet. If instead the open Internet is used, the use of end-to-end encryption would be prudent.

4.2.5 IoT Platform

In the above Figure 3, the IoT platform has been shown as a single entity, however, in reality it may consist of multiple platforms. For example, in the case of smart metering, it could be that one platform (the meter management platform) is used for device management and a second platform (the meter data management platform) is used to manage and process the data obtained by the device management platform.

The IoT platform may be hosted in the cloud which introduces another level of complexity. In the case of multiple platforms, it's possible for the device management platform to be cloud-based and the meter data management platform to be on premises or both could be cloud-hosted.

The connection between a pair of platforms needs to be considered if they aren't collocated. For example, how is the data shifted securely between platforms (using an API, FTP, etc.)? The IoT platform may be located off-shore in relation to the devices and this may create sovereignty issues. Mutual authentication should be used and there are post-quantum security issues related to that.

Similarly, the device management platform may be the source of firmware and configuration updates for devices and the security of those is a consideration. Alternatively, some devices may source their firmware updates from a 3rd party platform and there may be authentication and repudiation issues with that.

4.2.6 IoT Platform Access

This topic is more of an issue for cloud-based IoT platforms and is included for completeness.

The secure connection from (enterprise) customers' premises to the hosted cloud platform should be considered from the perspective of quantum safety. Especially since raw data is associated with private data, such as names, addresses, etc, inside the IoT platform. A second secure connection, again, often not confined to be on-premises, is in place to enable 'terminal access' for administrators and operations personnel of a (cloud hosted) IoT platform.

Often, enterprise users/customers and administrators/owners of an IoT platform can access the platform via APIs (e.g. for activating IoT devices, sending messages to the device, invoking services on data sent from a connected IoT device, managing a device, managing the platform itself etc.). A common technique is to use REST APIs based on HTTP(S), A REST client (browser or dedicated client software) is used on the user's side, to communicate with the IoT platform.

A user (or their device) needs to authenticate towards the IoT platform. Commonly deployed methods that are currently secure, but potentially quantum-vulnerable, include:

1. Username and password, possibly enhanced with multi-factor authentication (MFA).
2. Single Sign-On (SSO): allows users to authenticate once and gain access to multiple services without needing to log in again. SSO is often integrated with identity providers to streamline the authentication process. SSO can be realised using protocols like SAML, WS-FED, OAuth 2.0 or OpenID Connect (OIDC), which in turn builds on OAuth 2.0.
3. Biometric Authentication: uses unique biological characteristics such as fingerprints, facial recognition, or voice recognition to verify a user's identity.
4. Application Key: is a security token associated with a user. Typically, a separate appKey is created for each end user device. Such an appKey is passed as an authentication credential in form of a URL query string parameter or as a request header in the RESTful HTTP request sent from a user's device to the IoT platform.
5. OAuth 2.0: is a widely adopted authorisation framework that allows third-party applications to obtain limited access to user accounts without exposing passwords. It is commonly used for granting access to APIs. Importantly, it is also utilised within cloud services and hosted IoT platforms to authenticate and authorise users. OAuth 2.0 can be used to directly secure APIs, but can also be a component within higher level authorisation frameworks like OpenID Connect and Single Sign-On.

Vulnerabilities to potential quantum attacks may become more apparent when (implementation-dependent) protocol dependencies are uncovered. For example, MFA can be implemented using different techniques - among them PKI and asymmetric cryptography (e.g., for smart cards and hardware tokens), which can induce a quantum risk.

Similarly, SSO implementation protocols often rely on asymmetric cryptography: e.g.

- SAML can rely on TLS, on PKI to sign and encrypt SAML assertions,
- WS-FED relies on TLS and uses digital signatures,
- OAuth 2.0 has multiple dependencies on asymmetric cryptography (see below).

Biometric Authentication also often uses TLS to secure the channel between biometric user device and an authentication server. Moreover, biometric data is often digitally signed. Application Keys are often transferred between end user device and IoT platform using HTTPS with TLS and OAuth 2.0 relies on TLS to secure the communication channels between the client, authorisation server, and resource server.

4.2.7 Network API Exposure

For IoT it is possible that network APIs are used to connect to devices. An example enabling technology is Non-IP Data Delivery (NIDD), a standardised functionality specifically tailored for NB-IoT devices by 3GPP. This technology allows efficient communication between IoT devices and enterprise applications, not using the IP layer, instead directly transmitting non-IP data between the IoT device and the network infrastructure. This delivery method can be specifically useful for applications which infrequently transact small amounts of data. It also avoids the need to maintain pools of static IP addresses for IoT devices. The interface between the NIDD functionality and an enterprise application hosted, e.g., outside a mobile

network in the cloud can build on either the Service Capability Exposure Function (SCEF) or the Network Exposure Function (NEF).

Such an interface between 3rd party enterprise applications and the mobile network may have to support features like inquiring about the status of an IoT device, sending a message to a device, sending a callback from network to enterprise application to confirm data delivery or non-delivery within a maximum permitted delivery time. Overall, key interfaces need to be secured against quantum threats and the importance of this will depend on how mission critical the use case is. Note that both SCEF and NEF commonly use RESTful APIs to expose network capabilities to third parties.

Whilst most NIDD activities today have been predominantly trials, it's a consideration for the future.

Depending on the type of implemented GSMA CAMARA APIs [9] and their use in the context of IoT solutions, quantum-safe access to such APIs might be a further consideration (e.g. mutual authentication to CAMARA or a similar API platform, how the data is transported back from the API platform to an IoT enterprise application). CAMARA API [9] access is secured using OpenID Connect on top of the OAuth 2.0 protocol following the CAMARA Security and Interoperability Profile.

Thus, in Network API Exposure, similar vulnerabilities to quantum threats occur as for IoT Platform Access due to the use of similar security protocols and frameworks.

4.3 Security Considerations

IoT solutions will pose specific security challenges in relation to post quantum cryptography, which should be considered in the design of new IoT solutions, and when planning the post quantum cryptography transformation of legacy systems. Items listed below are aspects that may contribute to solution, migration and operational choices. Not all will be relevant to all IoT solutions.

Organisations should adopt a balanced, risk-based approach to PQC implementation for IoT solutions, conducting a comprehensive risk assessment to identify and prioritise actions [10].

Specific issues apply to IoT when considering post-quantum security:

1. Physical security: side-channel and fault attacks (i.e., the adversary is in possession of the IoT device; potentially an issue if cryptographic operations involving secret parameters (signature/decryption private key) are executed by the device). Security of the standardised PQC algorithms in the context of physical attacks is a relatively new topic of research and, as a result, vendors and certification bodies will have to respond to developments in this area appropriately.
2. Transition: legacy systems may include devices that are already deployed in the field, without update mechanisms. This could lead to discrepancies in expected security properties, subject to how a future adversary equipped with a CRQC is able to attack such devices. It may be the case that a risk analysis exercise identifies some devices in a system as not being worth the cost of updating in a short timeframe leading to, e.g., a phased transition for the system itself.
3. Type of threat: the SNDL attack must be considered, though in some IoT contexts data confidentiality may not be so crucial (e.g. short data lifespan for smart meters). Due to

the time needed to update an IoT device, the authentication mechanisms may have to be considered, to protect against future adversaries empowered with a CRQC .

4. Lifecycle: for use cases with longer lifecycles and, in particular, in instances where it's difficult to access the device (e.g., lack of remote update), intermediate strategies may have to be applied rather than replacing the traditional cryptographic primitives with post-quantum counterparts. For instance, if an upper level already provides post-quantum security, or can easily be updated, then updating the IoT device itself might be postponed (at the cost of a slightly weakened security model). This might be sufficient until the IoT device is eventually decommissioned and replaced by a new device that implements post-quantum cryptographic primitives (in that perspective, see the GSMA document PQ.03 v2.0 [4], sections 5.6.9.3-5.6.9.5, for such a phased and partial transitions, though the context is not exactly the same).

Furthermore, there are two dimensions that affect algorithm performance:

5. Efficiency of the (quantum-resistant) cryptographic algorithms (mainly RAM, code size, latency, computation time).
6. Energy: large parameters (public key, signature, ciphertext) will contribute to a lot of energy consumption in relation to transmission on the air interface.

These issues can cause different outcomes for a device and/or a system. Dedicated hardware will provide acceleration for some algorithms, however, hardware vendors must make decisions about which schemes to provide acceleration for. From this perspective, increased cryptographic agility will come at a cost in terms of chip area and code size.

For PQC capability delivered via software/firmware update, some devices will be capable of performing PQC algorithms to an acceptable standard immediately however they may not have hardware roots of trust (for example, to verify future updates via verification keys stored in ROM/fuses). In other cases the on-device performance may slow down considerably, particularly if only a small amount of memory is available. In either case, the large ciphertexts, signatures and keys (and certificates) will play a role on the communication channel. System providers should therefore consider the function and criticality of devices in the system in the presence of the quantum threat and plan their migration strategy accordingly. Part of this analysis will be to perform testing at various points in the system.

4.4 Data

Data transmitted by IoT devices connected to cellular networks can be encrypted with symmetric cryptographic algorithms over the air interface, as usually happens for the encryption of data from user equipment. The quantum threat is much less severe for symmetric cryptography, so these methods are expected to remain sufficiently secure (perhaps requiring an increased key length; see the discussion on Grover's algorithm in section 5a below). As data transits from a base station to a network security gateway, it may be secured with IPSec, typically using asymmetric (quantum vulnerable) methods for key exchange. Similar to other contexts in which IPSec is used to secure data in transit, it is expected that the asymmetric key exchange methods currently used will need to be modified to PQC variants, either as standalone PQC or in a hybrid mode combining currently used methods with PQC algorithms.

More generally, any IoT context in which data in transit is secured by standard VPN methods, such as IPSec or TLS, will require upgrading to quantum-safe status. Data in transit that is secured by symmetric methods, as per the RAN air interface example, is expected to remain secure against the quantum threat.

Of particular relevance for the IoT context is the release of Ascon standards by NIST [11]. The Ascon family of symmetric algorithms are suitable for use by constrained lightweight devices, as relevant for multiple IoT contexts. Ascon algorithms have low latency and high throughput, and although performance is typically slower than (e.g.) AES, Ascon algorithms have a smaller memory footprint and therefore avail a broader range of applications, as relevant for compact IoT systems. Similar to other symmetric algorithms (such as AES), the quantum threat is less relevant for the symmetric Ascon algorithms. Data at rest or in transit encrypted symmetrically in IoT contexts by algorithms such as AES and Ascon is expected to remain secure against quantum attacks, modulo a possible need to use larger keys.

5 Standards - an Overview

The IoT ecosystem is supported by a wide variety of standards and protocols that are an integral part of the IoT solution stack. Some are specially designed to meet the specific needs of IoT use cases (i.e. NB-IoT), others are also used more widely. Proprietary solutions, developed by individual companies are also extensively used in IoT. PQC algorithms are not drop-in replacements for legacy algorithms, therefore an assessment of the performance impacts must be considered in the evolution of standards, products and end-to-end solutions.

Furthermore, PQC implementation and migration planning for IoT must take into consideration aspects related to dependencies on standards readiness, product roadmaps and ability to update/evolve deployed solution components.

Figure 4 below lists examples of commonly used protocols.

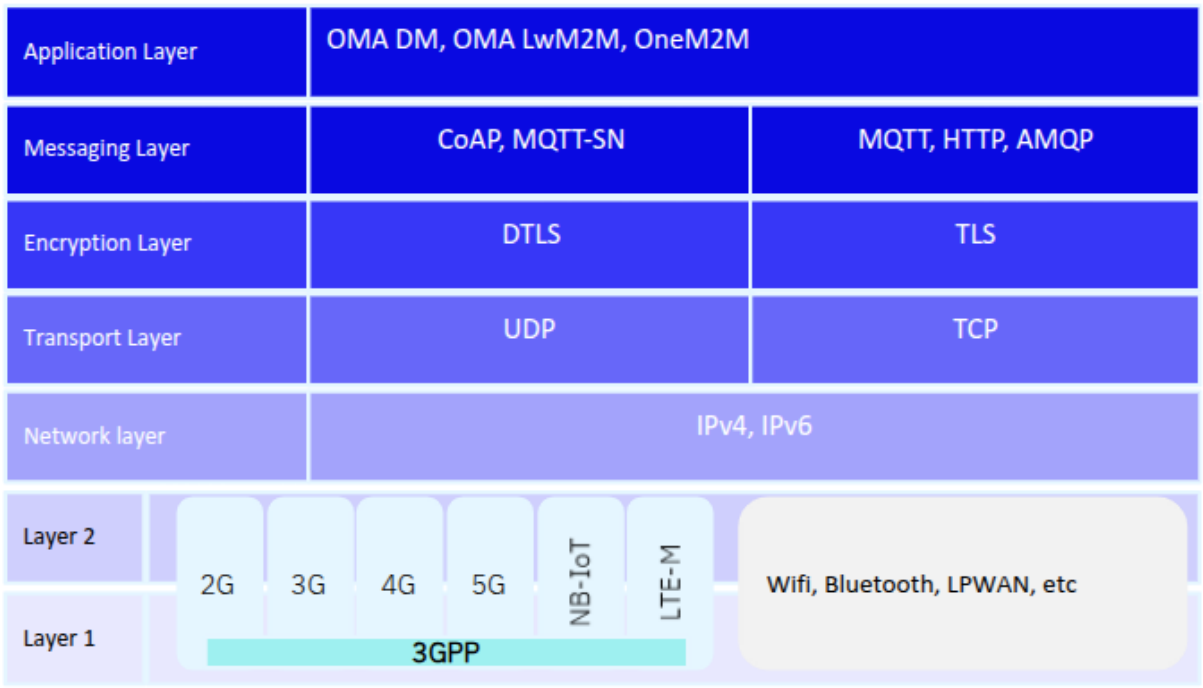

Figure 4: Commonly used Protocols

At the application level, many IoT platforms interface directly with messaging protocols, but to avoid duplication of effort and foster interoperability, protocols have been developed to provide device and life-cycle management services for IoT systems. OMA LwM2M is a protocol which provides IoT-specific services such as device activation and management, data management and firmware updates. It typically runs over CoAP but may also use MQTT or HTTP for messaging. OMA DM is similar but targets less constrained devices such as vehicle infotainment systems or tablets. OneM2M provides a complete framework for building interoperable IoT platforms.

Communication between the IoT platform and the devices is generally handled by a messaging protocol. Some examples of message types include sensor readings pushed to the platform from a smart metering device, or an “on” control pushed from the IoT platform to a smart streetlight. In many cases, IoT data transfers are small in size, and infrequent, although this is dependent on the use case and, even for such constrained devices, larger transfers may be required to perform firmware upgrades.

Probably the three most common messaging protocols are CoAP, MQTT and HTTP. CoAP is targeted towards constrained devices and is based on a REST framework. HTTP is also common due its ubiquity as a REST API transport. MQTT, on the other hand, is based on a publish/subscribe model, and has a lightweight version called MQTT-SN.

Both HTTP and MQTT use TCP for transport, which may not be suitable for highly constrained applications due to protocol complexity and memory requirements. CoAP and MQTT-SN, on the other hand, are designed to run over UDP or other connectionless transports, making them more suitable for constrained applications.

For the encryption layer, TCP may use TLS, and UDP may use DTLS, to provide authentication, confidentiality and data integrity. Either way these protocols add a burden and, in some cases, existing network encryption may be used instead of providing end-to-

end encryption between device and platform (see “IoT Architecture”, section 4.2). Whilst saving resources on the device, this approach has the disadvantage of relying on multiple independent encrypted channels which may be provided by different operators. For end-to-end encryption, TLS will be the most common choice for TCP transport, with DTLS for UDP, although given that UDP is often chosen for its characteristics in constrained applications, adding DTLS may not be practical in all cases. Often, in IoT applications, TLS is used with mutual authentication (sometimes called MTLS) to allow a device to authenticate itself to the IoT platform.

Note also that the EDHOC protocol [12] is a very compact and lightweight protocol (in terms of message size) intended for usage in constrained scenarios. As with (D)TLS, it incorporates an authenticated key exchange mechanism and a secure tunnel establishment to carry application data. EDHOC frames are transported over CoAP.

5.1 Algorithm Standards

5.1.1 Standards related to asymmetric cryptography

PQC standardisation has been primarily managed by the National Institute of Standards and Technology (NIST). NIST started a program in 2016 to solicit, evaluate and standardise quantum-resistant cryptographic algorithms. The algorithms were divided into two categories: key encapsulation and digital signature.

After multiple rounds of submissions, the first standards were published in August 2024. Standards were published for one key encapsulation and two digital signature algorithms as follows:

FIPS 203 [1]	Crystals Kyber	ML-KEM	Key Encapsulation
FIPS 204 [2]	Crystals Dilithium	ML-DSA	Digital Signature
FIPS 205 [3]	Sphincs+	SLH-DSA	Digital Signature

Table 3*:* NIST standards for PQC algorithms

In addition, one other algorithm was selected for standardisation and is expected to be published in 2025:

FIPS 206	Falcon	FN-DSA	Digital Signature

Table 4: Additional NIST PQC standard

Moreover, independent of the NIST PQC process, NIST also selected two additional quantum-safe (stateful hash-based) signature schemes: eXtended Merkle Signature Scheme (XMSS) and Leighton-Micali Signatures (LMS) (and derivatives) [13].

Producing signatures via the algorithm FN-DSA/Falcon requires double-precision floating point hardware which is extremely difficult to do securely on embedded/constrained devices. It is therefore expected that only signature verification (for example to verify part of a received certificate) on IoT devices will be viable with this algorithm. Similarly, NIST mandate

that producing keys and signatures for XMSS and LMS is only allowed on a very restricted class of devices and therefore signature verification is expected to be the only component that is widely supported for IoT endpoints [13].

It is further expected that one additional key encapsulation algorithm will be standardised by NIST in the near future, either BIKE or HQC, to provide a choice between lattice-based and code-based approaches. These schemes have considerably larger keys and ciphertexts than ML-KEM, which may restrict adoption in IoT environments.

In addition, the decision of whether to standardise the Classic McEliece algorithm is still ongoing, pending use case proposals. This algorithm is unlikely to be viable for IoT due to its large key sizes.

Each standardised key encapsulation algorithm was required to be specified in three encryption strengths:

- Level 1: 128-bit equivalent AES encryption
- Level 3: 192-bit equivalent AES encryption
- Level 5: 256-bit equivalent AES encryption

In the FIPS-203 standard [1], NIST recommends L3 strength for general use, however L1 is likely to be a better choice for many constrained IoT applications.

In order to better understand the challenge presented by the different sizes of cipher texts, public keys, private keys and signatures for PQC algorithms, the tables below [14] illustrate the size of these for both classical and Post Quantum Cryptography algorithms, allowing easy comparison (classical algorithms are displayed *in italics*).

Estimated Security Strength	Signature Algorithm	Signature Size (bytes)	Public Key Size (bytes)	Private Key Size (bytes)
128 bits	*ECDSA-256*	*64*	*64*	*32*
	RSA-3072	*384*	*384*	*384*
	ML-DSA-44	2420	1312	2560
	Falcon-512	666	897	1281
	SLH-DSA-128f(s)	17088 (7856)	32	64
192 bits	*ECDSA-384*	*96*	*96*	*48*
	RSA-7680	*960*	*960*	*960*
	ML-DSA-65	3309	1952	4032
	SLH-DSA-192f(s)	35664 (16224)	48	96
256 bits	*ECDSA-512*	*128*	*128*	*64*
	RSA-15360	*1920*	*1920*	*1920*
	ML-DSA-87	4627	2592	4896
	Falcon-1024	1280	1793	2305
	SLH-DSA-256f(s)	49856 (29792)	64	128

Table 5: Signature and key sizes for signature algorithms

Estimated Security Strength	Key Establishment Algorithm	Ciphertext Size (bytes)	Public Key Size (bytes)	Private Key Size (bytes)
128 bits	*ECDH-256*	*64*	*64*	*32*
	ML-KEM-512	768	800	1632
	BIKE-L1	1573	1541	5223
	HQC-128	4497	2249	2305
	FrodoKEM-640	9720	9616	19888
	Classic McEliece-348864	96	261120	6492
192 bits	*ECDH-384*	*96*	*96*	*48*
	ML-KEM-768	1088	1184	2400
	BIKE-L2	3115	3083	10105
	HQC-192	9042	4522	4586
	FrodoKEM-976	15744	15632	31296
	Classic McEliece-460896	156	524160	13608
256 bits	*ECDH-512*	*128*	*128*	*64*
	ML-KEM-1024	1568	1568	3168
	BIKE-L3	5154	5122	16494
	HQC-256	14485	7245	7317
	FrodoKEM-1344	21632	21520	43088
	Classic McEliece-6688128	208	1044992	13932

Table 6: Ciphertext and key sizes for key establishment algorithms

5.1.2 Standards related to symmetric cryptography

Regarding symmetric-key cryptography, AES is widely used in IoT and in recent years Ascon was selected as winner of the 2023 NIST Lightweight Cryptography Standardisation Process [11].

The impact of quantum attacks on symmetric-key algorithms, as of writing, is mainly due to Grover's algorithm. The practical implications of the latter are still discussed among the expert community, and no consensus has emerged so far, as illustrated by the positions of different national cybersecurity agencies. Some (e.g. NIST, NSA, NCSC in UK) deem that AES-128 can continue to be used securely, even if in certain scenarios AES-256 is instead recommended (see for example NSA's CNSA 2.0 for National Security Systems [32]). The latter, other approach is also suggested by other agencies (e.g. ANSSI, BSI), which recommend using AES-256, at least as a reasonable option given the little effort required in most cases.

In any case, when opting for a symmetric-key algorithm one should consider the quantum security assessment for that algorithm. In turn, such an analysis relies upon the technical characteristics of the quantum circuit that implements Grover's algorithm for that specific target (i.e. the envisaged symmetric-key algorithm).

In order to compensate for the security properties not always provided by symmetric-key cryptography (e.g. forward security), integrating public-key cryptography can be a valuable option. In such a case, considerations related to the quantum security of asymmetric algorithms (in particular those included in this document) should be taken into account.

More information about symmetric cryptography in the context of PQC can be found in reference [4].

5.2 Protocol Standards

To integrate post-quantum algorithms into security protocols, existing standards need to be extended. At a minimum, this involves allocation of new identifiers for the new algorithms, however other factors may also have to be considered, such as larger key sizes, more transactions, etc. The following sections discuss the extension of common security protocols.

5.2.1 IPSec

Extensions to IPSec are managed by the IETF IP Security Maintenance and Extensions (IPSECME) group [15]. Two new standards have been developed by that group to allow post-quantum key encapsulation mechanisms to be integrated into IPSec's signalling protocol (IKEv2).

From a pure protocol standpoint, there were two issues to deal with:

1. The addition of multiple post-quantum key exchange steps during tunnel setup. The decision to allow multiple parallel algorithms was to minimise the risk of algorithms being broken. For example, it may be prudent to combine a lattice-based algorithm with a code-based algorithm, so that if one of those schemes is broken, the data is protected by the other. In addition, it is possible (and indeed advised) to keep the classical key exchange and combine classical and additional post-quantum key exchanges together. This ensures that if post-quantum algorithms are broken, there is a minimum level of security corresponding to the classical algorithm strength. The above extensions are covered by RFC9370 [16].

2. The support of long keys. IKEv2 does not allow fragmentation (at the protocol level) in its initial exchange, so RFC9242 [17] defines a new message type to overcome this limitation and support the longer key lengths of post-quantum algorithms, which can easily exceed typical network packet size limitations.

Finally, IANA has assigned IKEv2 Key Exchange Method Transform IDs for the three strengths of the ML-KEM algorithm as follows:

L1	ML-KEM-512	35
L2	ML-KEM-768	36

L3	ML-KEM-1024	37

Table 7: *IKEv2 key exchange method transform IDs*

5.2.2 TLS

Extensions to TLS are managed by the IETF TLS group. There are no RFC standards released at the time of writing, but a mature draft specifies the integration of post-quantum algorithms with TLS version 1.3 [18].

The integration with TLS is similar to IPSec, except there are no fragmentation restrictions to deal with. As such the extensions proposed in the draft are less complex.

In the draft, the negotiation of key exchange algorithms is unchanged, except that it adds the provision to mix post-quantum algorithms with classical algorithms. The approach differs from IPSec in the sense that only one exchange transaction is made in each direction, and so if multiple algorithms need to be combined, they need to be negotiated as a single group. Essentially this means that each combination of algorithms needs to be assigned an Identity (ID). At the time of writing, the most used combination is x25519 (Classical Diffie Hellman group 31) with ML-KEM-768, however this combination is geared towards web browsers, and more combinations are likely to be defined to cover other use cases such as IoT.

Another downside of this approach is that for each combination of classical/post-quantum algorithms, a key share is usually transmitted in the TLS ClientHello message, and this can consume a lot of bandwidth, especially if many proposals are being offered. For IoT devices, it is expected that only one proposal will be offered, however if offering multiple proposals is a requirement, the protocol allows for the key share for only the most likely proposal to be sent. In this case, if the server accepts one of the other proposals, then a second ClientHello exchange is required.

Using the hybrid mode is recommended by several (mainly European) cybersecurity agencies. As noted in the discussion of IPSec above, the goal of combining pre- and post-quantum algorithms in a hybrid approach is to protect against "Store Now, Decrypt Later" attacks while maintaining the current (pre-quantum) security level. Similarly for digital signatures, a hybrid approach ensures entity authentication as long as one of the two component schemes is still secure.

For hardware vendors to get devices certified it is often necessary that cryptography implementations meet the requirements of multiple standardisation bodies (e.g. FIPS 140-3 [19] and SESIP). The ongoing discussions between the IETF and national SDOs aim to provide alignment on precisely what is allowed for hybrid implementations of protocols including TLS.

However, other cybersecurity agencies (e.g. NSA) deem that the post-quantum algorithms selected by NIST are mature enough and can be used in standalone. As such, NSA has proposed an IETF document [20] defining the use of PQC only algorithms with TLS 1.3 (ML-KEM for key exchange and ML-DSA for server authentication). Another IETF draft is proposed based on ML-KEM only for the key exchange [21]. IETF drafts also exist which

propose post-quantum methods (standalone or hybrid) for the authentication phase with ML-DSA [22],[23] and SLH-DSA [24].

See also IETF TLS Key Share Prediction [25], which proposes a method of retrieving this information via DNS.

5.2.3 DTLS

Some IoT client devices securely communicate with application servers through application protocols which rely on or benefit from the DTLS protocol (e.g. DTLS 1.3 RFC9147 [26]) for encryption, authentication and data integrity. An example application protocol in IoT is the Constrained Application Protocol CoAP which is bound to UDP and for security optionally to DTLS. Protocol versions of DTLS are based on the corresponding TLS versions. For instance, DTLS 1.3 is based on TLS 1.3. In the context of DTLS, the hybrid key exchange mechanism is designed to ensure that communication remains secure even in the presence of quantum computing threats. This is achieved by integrating post-quantum security into the key exchange process, similar to what is done in TLS 1.3.

IETF is in the process of addressing quantum-safety also for DTLS. The Post-Quantum Cryptography Recommendations for Internet Applications draft [27] highlights challenges and best practices for deploying Quantum-ready usage profiles for applications using both TLS and DTLS. However, the version from 18 Dec 2024 doesn't address any specific IoT use cases yet. It discusses quantum-readiness issues with DTLS in the context of the WebRTC application.

5.2.4 SSH

For SSH, there is a current internet draft PQ/T Hybrid Key Exchange in SSH [28] which specifies a hybrid key exchange, consisting of a classical Diffie Hellman exchange and a single post-quantum exchange.

Three options are specified in this draft:

- mlkem768nistp256-sha256 (ML-KEM-768 with DH P256)
- mlkem1024nistp384-sha384 (ML-KEM-1024 with DH P384)
- mlkem768x25519-sha256 (ML-KEM-768 with DH x25519)

The shared secret is then calculated by combining the results of the two algorithms executed.

The draft Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512 [29] combines X25519 with the post-quantum KEM NTRU Prime (sntrup761).

6 Algorithm Performance for IoT

As part of a cryptographic inventory, IoT (/edge/constrained) devices should be assessed regarding the purpose of the cryptographic protocol/operation in question. In particular, the current capability of devices can and should be assessed relative to the requirements of the

cryptography being used. A single device may use digital signature verification for secure updates and secure boot, in addition to entity authentication in secure channel establishment using TLS. The threat analysis discussed earlier in this document will inform which components of a system should be migrated to quantum safety in which order, however if one component cannot be migrated then this clearly could have a major impact on the entire system migration and/or the level of risk exposure of the whole system.

The impact of a performance slowdown should also be considered. A software update procedure is much less time-critical than secure boot and secure channel establishment, and will often be performed much less frequently (however it might not be possible to provide meaningful post-quantum security to the software update process without a secure way of delivering post-quantum verification keys for that update process). For providing post-quantum confidentiality in TLS 1.3 connections, one entity needs to perform ephemeral key generation and decapsulation while the other needs to perform encapsulation. For this to be fast, it would be beneficial for the less powerful device of the pair to only have to perform encapsulation if possible, where the standards allow.

Performance is very difficult to assess in generality, and many factors play a role in how efficiently a cryptographic algorithm will run. The factors, such as available runtime memory and availability of hardware acceleration, vary greatly in deployed IoT devices. For battery-powered devices and devices connected with low-bandwidth channels, the increased size of post-quantum signatures, ciphertexts and certificates will likely cause major challenges, and a migration plan should identify these bottlenecks.

It is necessary for system providers and migration planners to assess the performance of their current and future devices for their use cases, ideally through in-field testing. Performance statistics in academic papers and other sources may often be unreliable: reference implementations for PQC algorithms do not attempt to reduce memory usage and therefore the algorithms may appear to perform slowly or require a lot of memory when used on a constrained device. Dedicated implementations for embedded platforms can reduce memory usage dramatically and use the features of the hardware available, including hardware accelerators. Protections against physical attacks - needed for embedded devices used in IoT systems - have a significant impact on performance which can be difficult to assess. Vendor estimates for performance of next-generation products will therefore provide a much better guide for system operators.

7 Transformation/migration approach

7.1 Implementation Roadmap

The implementation roadmap for PQC in IoT solutions should consider two scenarios, which present different challenges and opportunities: new and legacy (existing) solutions. In both cases, the solution lifecycle, timelines and data shelf-life play a critical role in informing the strategy adopted.

7.2 Policy and regulation

IoT solutions and services present specific challenges in relation to policy and regulation. The global nature of IoT means that regulation across multiple countries and geographies

may need to be considered [30]. Sector specific aspects may apply, in addition to cross-sector ones.

Areas likely to be impacted include:

- Data privacy and protection

Different countries have different data protection laws, so compliance will need to consider the most stringent to ensure that data collected is protected and used in compliance with applicable legislation.

- Security baselines

Security baselines may be issued in the form of guidelines, as in the case of the European Union Agency for Network and Information Security (ENISA), which has developed the Baseline Security Recommendations for IoT [31] or in the form of regulation/legislation. As with Data privacy and protection, IoT solutions must be designed to comply to the applicable aspects across the geography in which the solution operates and to evolve to meet changes in regulation.

- Certification

The certification landscape covers different aspects of IoT, including IoT solutions, devices, technologies and operational processes.

PQC adds a layer of complexity due to the evolving guidelines and regulations that are being developed. Addressing these challenges requires a strong collaboration between industry stakeholders, governments and regulators to create a coherent regulatory framework that results in secure and future proof IoT solutions.

8 Conclusion

This report has provided an initial analysis of the impact of quantum computing on IoT systems and the necessary steps to mitigate associated risks. It outlines the specific challenges posed by quantum computing to IoT security and highlights the need for quantum-robust mutual authentication, end-to-end encryption, and secure firmware updates to ensure the security of IoT devices.

Some important takeaways are:

The quantum threat to IoT is real: Quantum computing poses a significant threat to the cryptographic algorithms currently used to secure IoT systems. Depending on the nature of the IoT devices and the use cases, this threat must be considered across the overall system architecture of end-to-end IoT solutions, including components from (embedded) SIM card to API-based access to cloud-hosted IoT platforms, all with the appropriate urgency, taking into account not only the shelf-life of transmitted data but also the lifecycle of the IoT devices.

Post Quantum Cryptography is here to mitigate risk: PQC refers to cryptographic algorithms that are resistant to attacks from both classical and quantum computers. A first set of PQC algorithms for key exchange and digital signatures has already been standardised by NIST and additional candidate algorithms are expected to be standardised in the near future.

Some PQC algorithms might a better match than others for particular IoT solutions: The various quantum-safe key establishment algorithms and digital signature algorithms differ in their characteristics (size of private and public keys, size of ciphertext and signature) which further depend on the desired strength of security. In particular, for constrained IoT devices, trade-offs must be carefully considered between desired security strength (appropriate for a use case) and potential performance implications on IoT solution and application. A further dimension is the availability of most suitable cryptographic algorithms either in form of international standards or currently still candidates for standards, and the status of their incorporation into higher-level communication protocols used in IoT.

Communication protocols widely used in IoT are being enhanced with PQC: Work is under way, in particular, in the Internet Engineering Task Force to incorporate quantum-safe cryptography algorithms into Internet communication protocols which are widely used in IoT.

Lifecycle considerations are key: IoT devices with long lifecycles and limited upgrade capabilities are particularly vulnerable to quantum threats. It is crucial to plan for the implementation of measures to mitigate these risks.

Recommendations from this report are:

Conduct comprehensive risk assessments for IoT solutions: Organisations should conduct quantum risk assessments to identify and prioritise actions to mitigate risk.

Adopt PQC and ensure crypto-agility: Stakeholders should adopt PQC and work towards achieving crypto-agility to future-proof IoT solutions and maintain security in the face of advancing quantum computing technologies. Adoption of PQC means, e.g., incorporating PQC into updates of industry-wide IoT security frameworks and architectures (which might be sector specific as for smart metering or healthcare) and planning for the use and integration of system components into end-to-end IoT solutions, where the components are deemed quantum-safe due to incorporation of new PQC algorithms into communication protocols stacks, public key infrastructure, hardware components and systems on chip.

Plan early enough for lifecycle security: It is important to consider lifecycle security, particularly for IoT devices with long lifecycles and limited upgrade capabilities. Intermediate strategies may be necessary until devices can be replaced with new ones that implement PQC primitives.

Collaborate with industry and regulators: Strong collaboration between industry stakeholders, governments, and regulators is essential to create a coherent regulatory framework that results in secure and future-proof IoT solutions. Such collaboration can be nurtured by industry organisations which are unique to IoT market segments (e.g. healthcare, security, environmental services, utilities, automotive) and therefore have deep understanding of required security levels and the trade-offs to be considered.

Stay informed on developments regarding standards and protocols: International standards and frameworks for IoT, often sector specific, will evolve and new versions will emerge which leverage already existing and newly emerging standards for quantum-safe cryptography. This enables organisations to remain secure and compliant with the latest guidelines.

In summary, it is crucial to take proactive steps to mitigate the quantum threat in IoT systems. By integrating Post-Quantum Cryptography and maintaining crypto-agility, stakeholders can ensure that IoT solutions remain secure and resilient against the advancements in quantum computing technologies.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	24 January 2025	PQTN TF	TG	Yolanda Sanz, GSMA

Ackowledgement – Companies that have contributed to this document:

AKAYLA, AT&T Mobility, C Spire, China Mobile, China Telecom, China Unicom, CK Hutchison, Deutsche Telekom AG, EE Limited, Ericsson. Fortinet, Giesecke+Devrient, Hewlett Packard Enterprise, Huawei, IBM, IDEMIA, IMDA, Infobip Ltd, Juniper Networks, Kigen, KT Corporation, Maxis Broadband Sdn. Bhd., Millicom International Cellular S.A., MTN Group, National Cyber Security Centre, Nokia, NXP, OFCOM, Orange, PQ Shield, Proximus, Qualcomm, Samsung Electronics, SandboxAQ, Singtel, SK Telecom, STC Group, STMicroelectronics, Telcel, Telefónica, Telstra Limited, TELUS Communications Inc., Thales, The MITRE Corporation, TIM S.p.A, Turkcell, , Utimaco TS GmbH, Verizon, Vodacom and Vodafone

A.2 Other Information

Type	Description
Document Owner	PQTN
Editor / Company	Yolanda Sanz, GSMA

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.