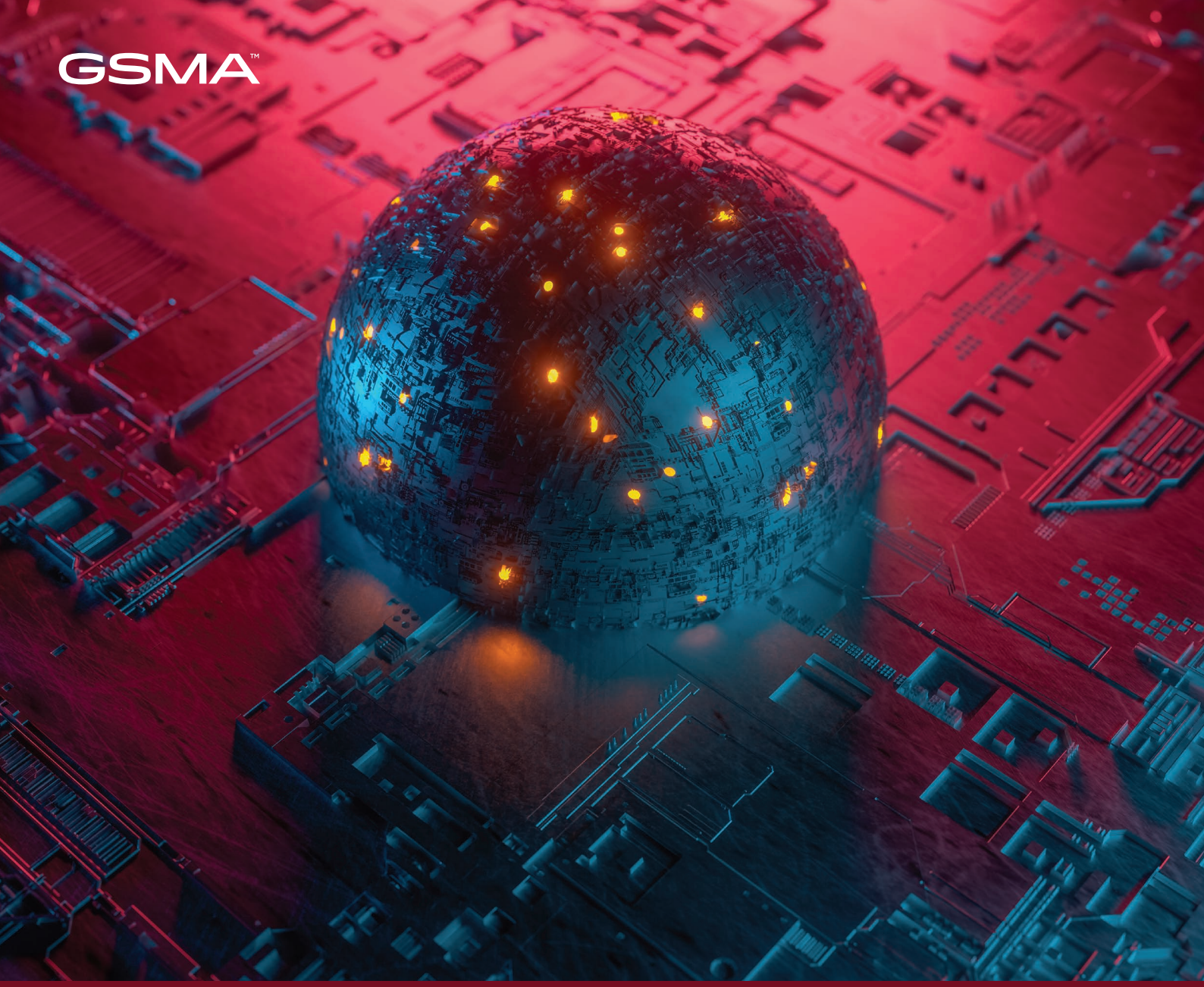
GSMA



Post Quantum Cryptography in IoT

Executive Summary

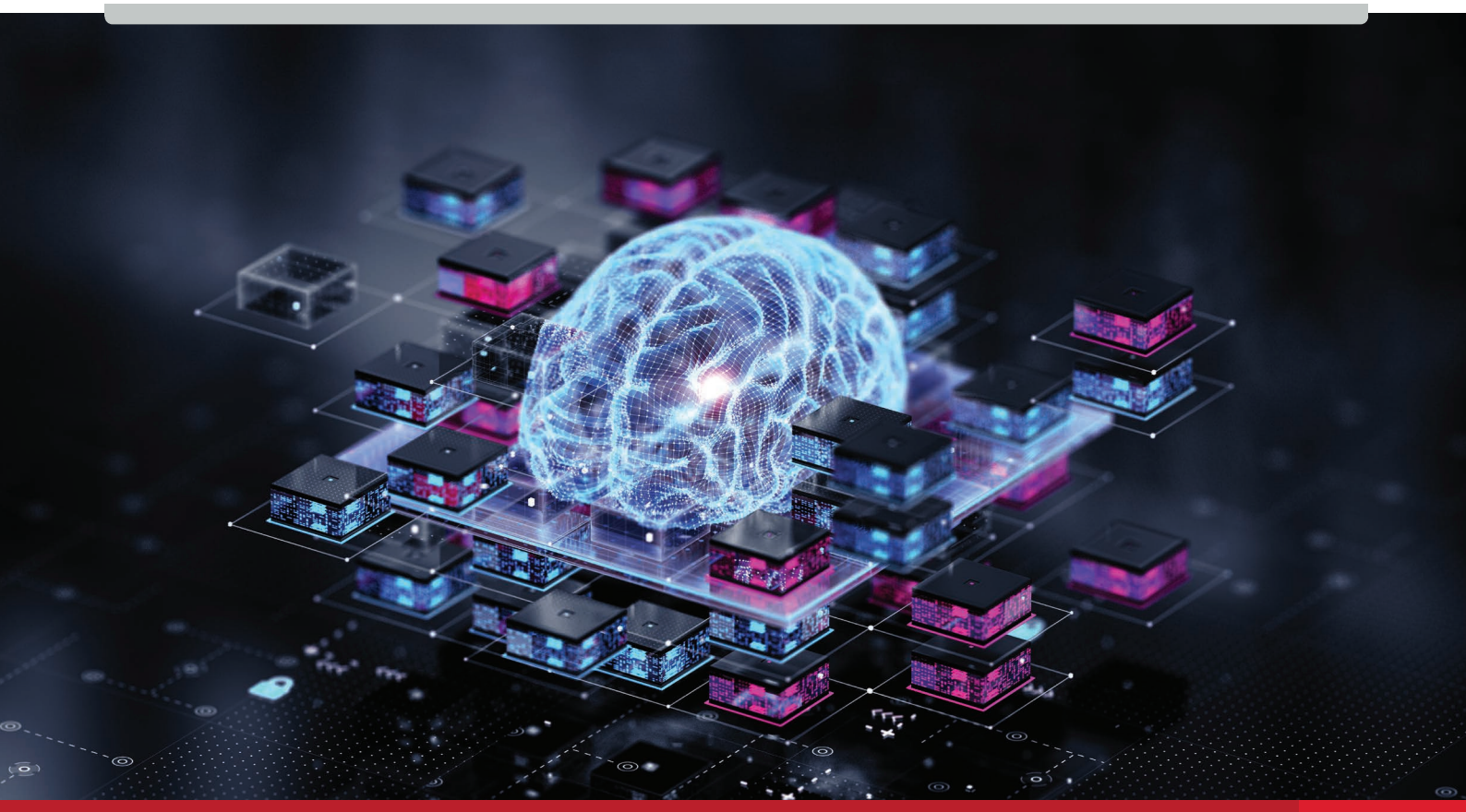
February 2025

1.0
Post Quantum Cryptography in IoT

In a rapidly expanding ecosystem of connected devices, cybersecurity is more critical than ever. The advent of quantum computers poses a threat to the cryptography that currently secures IoT solutions. This report, which is the result of a collaboration between the Post Quantum Telco Network Task Force and the 5G IoT Strategy Group, focuses on IoT systems connected using 3GPP-based connectivity, including both terrestrial and non-terrestrial networks. It builds on the topics covered in the Post Quantum Post Quantum Cryptography – Guidelines for Telecom Use Cases v2, focusing on the IoT context.

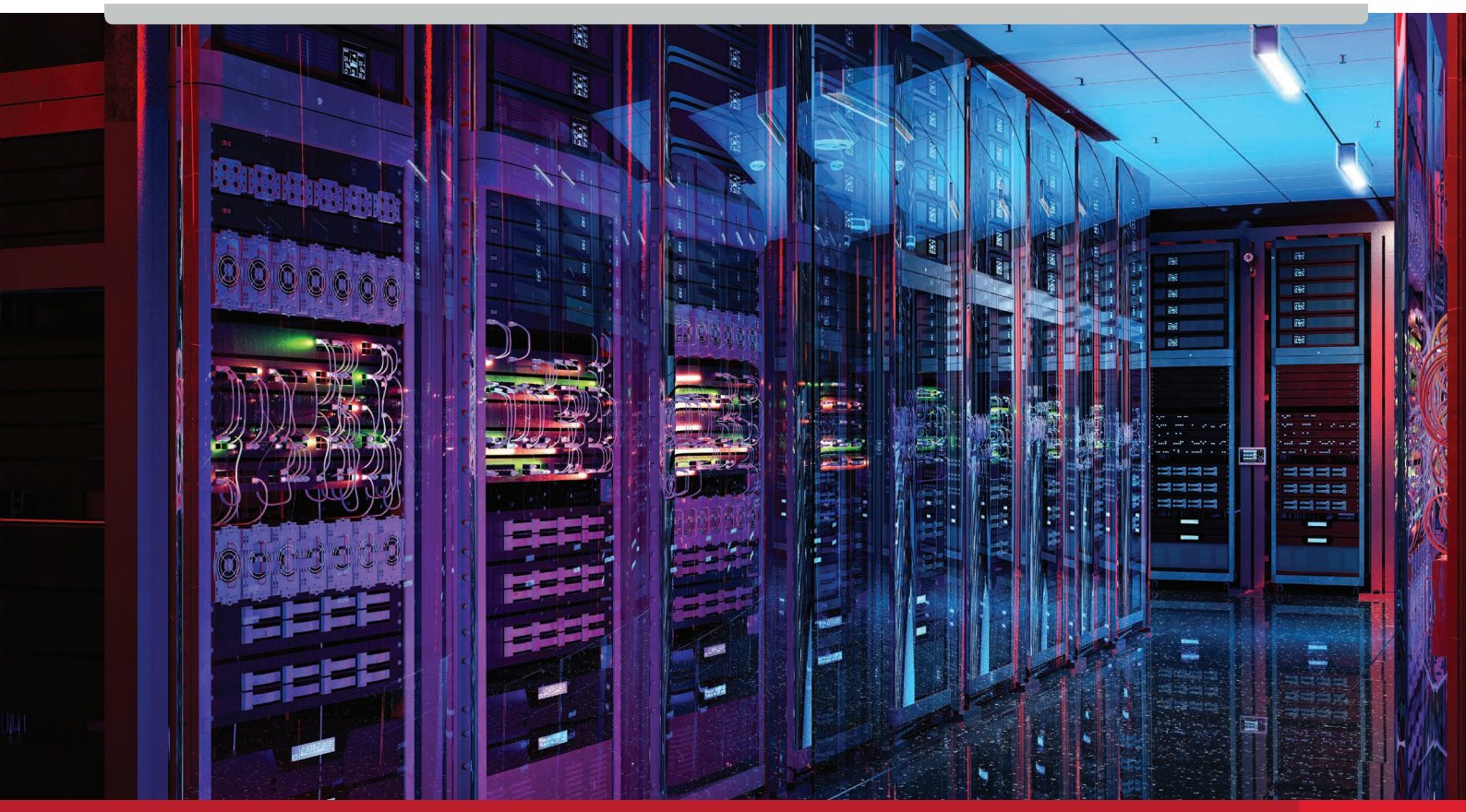
Analysing the constituent components of IoT solutions in conjunction with a categorisation based on use case requirements (including performance, operational and commercial considerations), highlights key aspects to consider in the design of future proof IoT solutions, as well as when planning the post quantum cryptography and crypto-agility transformation of legacy systems.

The purpose of this document is to provide information and guidance on the implementation of post-quantum cryptography and crypto-agility. It aims to offer actionable insights and future-proofing mechanisms to inform strategies for securing both existing and new IoT solutions against emerging quantum risks. This document seeks to enhance understanding and awareness of the quantum threat and promote ecosystem collaboration



towards developing secure, quantum-resilient IoT solutions. The target audience is a diverse group of stakeholders involved in the design, deployment, operation, security and use of IoT systems, including providers/developers of system components.

Feedback from the wider Telco ecosystem is essential for the continued relevance of the document. The GSMA PQTN Task Force and 5G IoT Strategy Group welcome the opportunity to engage and cooperate.



2.0
IoT and the quantum threat

IoT solutions are by nature, diverse: they address different sectors, use cases and different levels of business criticality. An important aspect is the lifecycle and longevity of IoT devices.

The widescale adoption of IoT by consumers and across industries and a growing number of interconnected devices, often involving sensitive data and critical systems, means that security requires careful consideration. Cryptography underpins the security of IoT solutions and is embedded in each of the IoT solution components and protocols: the figure below provides examples of potential threats to an IoT system if cryptographic algorithms employed by the system were compromised. The business risk posed, should any of these scenarios materialise, needs to be evaluated for each IoT solution, as it will vary by use case.

Quantum threats for IoT

What will a cybercriminal do?

Harvest and access data, eavesdropping

Harvest and decrypt of stored data through compromise of secure communication protocols (man in the middle attacks)

Unauthorised device access and manipulation

Compromise data integrity, ability to alter the behaviour of the IoT device

Malware/ransomware/ spyware attacks

Remote access of systems to exfiltrate information (for example, device location) through fraudulent authentication

Use the device as computation power (zombie device)

Malicious/invasive SW is installed, allowing attackers to take control of the IoT device authentication

Device spoofing

Add fraudulent devices to the IoT solution that disguises as a legitimate device

Access to adjacent systems connected to the IoT solution

Use the IoT solution as a gateway to infiltrate/ compromise adjacent systems, including the network. Trigger malicious actions (i.e. door unlock)

Fraud and anomaly detection compromise

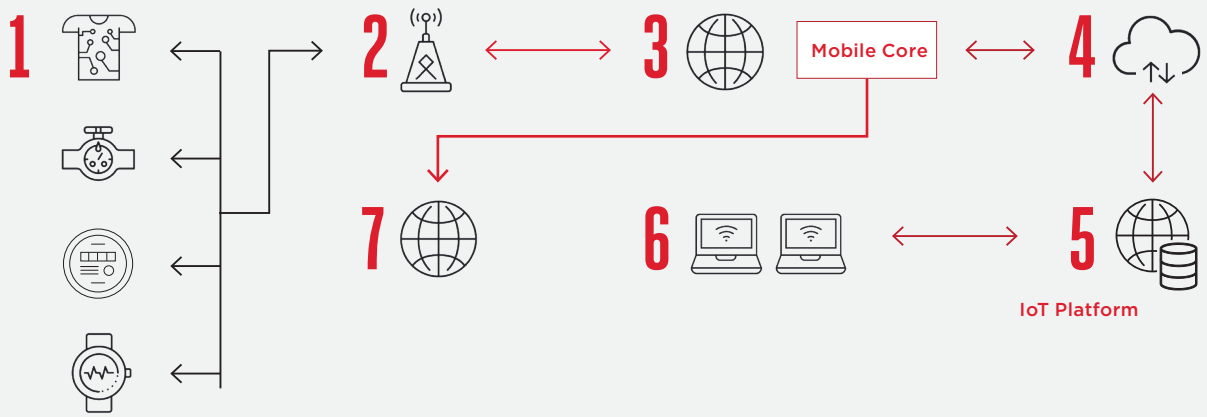
Undermine the effectiveness of anomaly or fraud detection to delay, subvert detection

3.0
Considerations for PQC implementation in IoT solutions

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.

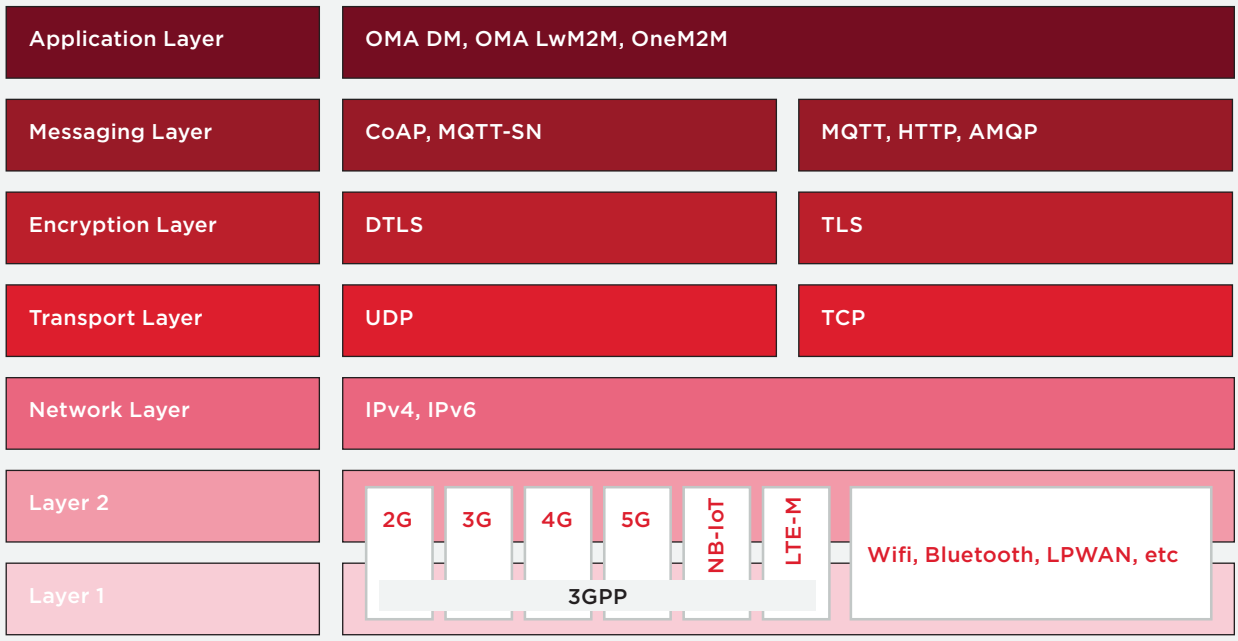
A balanced, risk-based approach to PQC implementation for IoT solutions is recommended and can be achieved by conducting a comprehensive risk assessment to identify and prioritise actions. To this end, the use of cryptography in IoT solutions has been analysed for each solution component and in relation to the most commonly used standards, adopted in IoT.

Figure 1
IoT Architecture



1. IoT Device | **2.** Air Interface | **3.** Mobile backhaul
4. Internet | **5.** IoT Platform | **6.** IoT Platform Access | **7.** Network API Exposure

Figure 2
IoT Standards



For each IoT component, the document highlights the cryptographic impact and security considerations related to post quantum cryptography.

The information provided supports an analysis, which can be used to engage the broader IoT supply chain and plan a PQC implementation strategy, taking into consideration technical aspects, such as performance constraints and operational aspects, such as device/solution lifecycle, ease of upgrade/replacement.

4.0 Conclusions and Recommendations

IoT systems face unique challenges in implementing Post-Quantum Cryptography (PQC) and crypto-agility to ensure long-term security and resilience in the quantum era. This document provides an initial impact assessment, guiding key stakeholders in taking proactive steps to mitigate quantum threats in IoT and navigating the evolving standards and regulations.

Recommendations:

- **Balanced, risk-based approach** to PQC implementation.
- **Implementation roadmap** for crypto-agility and PQC, particularly for critical infrastructure and/or solutions with longer lifecycles.
- **Early planning and proactive engagement** with procurement/technology vendors, providing opportunities to shape PQC implementation strategies for IoT.
- **PQC related policy and regulation management**, including geography and sector specific aspects. Areas likely to be impacted include data privacy and protection, security baselines and certification.
- **Establish testing frameworks** to assess and address system performance constraints and algorithm performance. Highlight gaps and inform technical Implementation, evolution options and implications for standardisation.
- **Collaboration** with industry, regulators and standards organisations, enabling organisation to manage security and compliance of IoT solutions going forward.

Supporting Companies:

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
Infineon Technologies AG
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 Co Ltd.
SandboxAQ
Singtel
SK Telecom Co., Ltd.
stc Group
STMicroelectronics
Telcel
Telefónica
Telstra Limited
TELUS Communications Inc.
Thales DIS France SAS
The MITRE Corporation
TIM S.p.A
Turkcell Iletisim Hizmetleri A.S.
Utimaco TS GmbH
Verizon
Vodacom (Pty) Ltd.
Vodafone

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