Preliminary Position on Post-Quantum Cryptography (PQC) for IoT Platform, Service, and Solution Providers

Public-Facing Statement | Version 1.0 | January 2026

Executive Summary

Quantum computing may, in the future, impact certain public-key cryptographic algorithms widely used today. IoT platform providers, systems integrators, and managed service providers have a responsibility to understand these developments and prepare appropriately.[1]

Because cryptographically relevant quantum computers are not yet available, and because post-quantum standards and implementations continue to mature, this position emphasizes risk-based preparation rather than immediate algorithm replacement.[1]

The primary preparation mechanisms include crypto-agility, lifecycle-aware design, secure implementation practices, and alignment with widely recognized standards as they evolve.

Scope and Applicability

This document applies to non-OEM organizations operating within the IoT ecosystem, including but not limited to:

- IoT cloud platforms and device management services
- Connectivity providers and managed service providers (MSPs)
- System integrators and solution providers
- Analytics, digital twin, and edge software platforms

Regulatory- and Standards-Aware Approach (Public Summary)

- Standards alignment: We monitor guidance and standards from recognized bodies such as NIST and ISO and plan adoption based on interoperability, maturity, and customer requirements.[1]
- U.S. Government alignment: For customers operating in government or regulated environments, we monitor relevant U.S. Government guidance, including post-quantum transition planning and crypto-agility expectations.[2]
- European Union expectations: EU cybersecurity frameworks emphasize risk-based security management, secure development, vulnerability handling, and appropriate use of cryptography. Our security program is designed to support these principles across software and service lifecycles.[3][4]

Our Current PQC Position

1) Crypto-agility as the foundation

We prioritize crypto-agile architectures that allow cryptographic algorithms and parameters to evolve without requiring disruptive platform redesigns or rapid customer migrations.[1]

2) Hybrid and phased transition strategies

Where long-term confidentiality, regulatory obligations, or customer risk profiles warrant, we evaluate phased strategies that preserve compatibility with existing ecosystems while enabling post-quantum readiness.[1]

3) Shared responsibility in the IoT ecosystem

As non-OEM providers, we recognize that cryptographic posture is shared across device firmware, platforms, networks, and applications. PQC readiness requires coordination with device manufacturers, customers, and downstream partners.

4) Implementation security and operations first

Operational security measures—secure key management, identity lifecycle control, vulnerability handling, logging, and timely updates—remain the primary determinants of real-world security and receive priority in PQC preparation efforts.[4]

What This Means for Customers and Partners

- No immediate changes are required to customer deployments solely due to PQC. Existing standards-based cryptographic protections remain appropriate for current threat models.[1]
- For deployments with long-lived data sensitivity or regulatory oversight, we support risk-based assessments and phased transition planning aligned with evolving standards.[1]
- We will communicate PQC-related updates transparently through customer documentation and security communication channels.

Important Notice (Safe Harbor)

Post-quantum cryptography standards, implementations, and recommended practices are evolving. This document is provided for informational purposes only and does not constitute a commitment to specific cryptographic algorithms, certifications, or transition timelines.

References

[1] NIST CSRC, Post-Quantum Cryptography Project (FIPS 203–205). https://csrc.nist.gov/projects/post-quantum-cryptography

[2] U.S. National Security Agency, Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

[3] NIS2 Directive, Article 21 – Cybersecurity risk-management measures. https://www.nis2-info.eu/article-21-cybersecurity-risk-management-measures/

[4] EU Cyber Resilience Act – Regulation (EU) 2024/2847 (lifecycle security obligations). https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI%282022%2973 9259_EN.pdf