+357 96 030922
info@marketpublishers.com

The Global Post-Quantum Cryptography Market 2026–2036

https://marketpublishers.com/r/G3728B901453EN.html
Date: May 2026
Pages: 130
Price: US$ 1,400.00 (Single User License)
ID: G3728B901453EN

Abstracts

Post-quantum cryptography (PQC) addresses the most consequential security transition in a generation: the replacement of public-key cryptography that a sufficiently powerful quantum computer would render obsolete. The algorithms securing virtually all digital communication today — RSA, elliptic-curve cryptography, and Diffie-Hellman key exchange — rest on mathematical problems that Shor's algorithm, running on a cryptographically relevant quantum computer (CRQC), can solve efficiently. The arrival of such a machine, termed "Q-Day," is estimated by most observers to fall between 2030 and 2040, though with considerable uncertainty. PQC algorithms are designed to resist both classical and quantum attack while running on conventional hardware, which makes broad, software-driven migration possible.

The market reached an inflection point with the conclusion of the US National Institute of Standards and Technology (NIST) standardization process, which finalized ML-KEM, ML-DSA, and SLH-DSA as Federal Information Processing Standards in 2024. Standardization converted PQC from a research field into a procurable, mandatable technology and gave governments and regulated industries a concrete migration target.

A defining feature of the market is that the algorithms themselves are a small economic prize, while the migration to them is a very large one. The NIST standards compile to a few hundred kilobytes of code; deploying them across decades of accumulated cryptographic infrastructure — protocols, applications, hardware security modules, certificate hierarchies, firmware, and supply chains — is an enterprise-wide undertaking. Migration framework documents from NSA, NIST, ENISA, and major consultancies converge on a consistent estimate: services and integration spending will exceed underlying PQC product revenue by a factor of roughly 8–12? across the migration window.

+357 96 030922
info@marketpublishers.com

Demand is driven by NIST standardization, government migration mandates such as NSA CNSA 2.0, the harvest-now-decrypt-later threat to long-lived data, sector regulation in finance, telecommunications and critical infrastructure, and the structural need for crypto-agility. The principal restraints are organizational inertia, backward-compatibility concerns arising from larger post-quantum key sizes, scarce specialist talent, and uncertainty over Q-Day's exact timing.

Banking and defence anchor near-term demand; embedded and IoT migration grows fastest later in the forecast. North America leads the market, supported by the earliest and most prescriptive mandates, with Europe and Asia-Pacific following. The total addressable market — products plus migration services — is projected to expand from a few billion dollars in 2026 to several tens of billions by 2036, making PQC one of the defining cybersecurity markets of the coming decade.

The Global Post-Quantum Cryptography Market 2026–2036 examines the post-quantum cryptography opportunity across products, services, technologies, end-use industries, and regions over a ten-year horizon. As quantum computing advances toward the point at which it can break the public-key cryptography securing modern digital communication, organizations worldwide face an urgent and complex migration. This report quantifies that opportunity and provides the strategic analysis needed by vendors, investors, integrators, and security leaders.

The report opens by establishing the quantum threat — Shor's and Grover's algorithms, the concept of a cryptographically relevant quantum computer, the Q-Day timeline, and the harvest-now-decrypt-later attack model that makes migration urgent regardless of when Q-Day arrives. It examines the four families of post-quantum cryptography — lattice-based, hash-based, code-based, and multivariate — and the NIST-standardized algorithms ML-KEM, ML-DSA, SLH-DSA, and FN-DSA, including the practical consequences of their larger key and signature sizes.

A detailed treatment of the standards and regulatory landscape covers the NIST process, the FIPS standards, NSA CNSA 2.0, the IETF, ETSI, ISO/IEC and ITU bodies, and national guidance from ENISA, BSI, NCSC, and ANSSI. The report then analyses the quantum-safe migration stack layer by layer — cryptographic discovery, crypto-agility, hybrid cryptography, HSMs, quantum-safe TLS and PKI, code signing, and embedded systems — and the central finding that migration services outweigh product revenue by 8–12?.

+357 96 030922
info@marketpublishers.com

The report provides extensive market analysis: drivers and restraints, SWOT analysis, a technology-readiness assessment, an opportunity-assessment framework, and per-segment SWOTs. It develops industry-specific migration programmes for banking, defence, government, telecommunications, critical infrastructure, cloud, healthcare, and automotive/IoT/manufacturing, and analyses the migration-services market and its provider landscape. Granular ten-year forecasts (2026–2036) are provided for the total addressable market and segmented by cryptographic approach, product category, end-user group, and region, with conservative, base, and optimistic scenarios. A regional analysis covers North America, Europe, Asia-Pacific, and the Rest of World.

The report includes profiles of 42 key companies active in post-quantum cryptography, covering their country, business description, funding, and PQC products and technology. Supported throughout by data tables and figures, the report is an essential strategic resource for any organization seeking to understand, enter, or invest in the post-quantum cryptography market.

Contents include:

+357 96 030922
info@marketpublishers.com

signing, embedded and IoT

PQC Products and Delivery Models — cryptographic libraries, software and firmware, PQC-enabled browsers, chips and accelerators, HSMs and tape drives, cloud/VPN/PQCaaS, product market structure

Market Analysis and Opportunity Assessment — drivers, restraints, net impact, SWOT, services-to-product ratio, technology readiness, opportunity framework, end-use opportunities, per-segment SWOTs

Industry-Specific Migration Programs — banking, defence, government, telecommunications, critical infrastructure, cloud and SaaS, healthcare, automotive/IoT/manufacturing, comparative summary

Migration Services and Consulting — market structure, pure-play consultancies, systems integrators, cloud-vendor services, specialty hardware vendors, managed services, strategic implications

Market Forecasts 2026–2036 — total addressable market, forecasts by cryptographic approach, product category, end-user group, and region, migration services forecast, growth scenarios

Regional Analysis — North America, Europe, Asia-Pacific, Rest of World, regional forecast and share dynamics

Company Profiles — 42 company profiles

The report profiles the following 42 companies active in the post-quantum cryptography market: 01 Quantum Inc., Aires Applied Quantum Technology (AAT), Atos, BTQ Technologies, China Telecom Quantum Group, Cisco Systems, Cloudflare, Crypto4A Technologies, Crypto Quantique, CryptoNext Security, DigiCert, Entrust, evolutionQ, Google, IBM, Infineon Technologies, Intel, ISARA, KETS Quantum Security, Microsoft, Patero, Post-Quantum (PQ Solutions), PQSecure Technologies, PQShield, Project Eleven, QAN Platform, QuantiCor Security, Quantropi, Quantum Secure Encryption Corp. (QSE), QuBalt and more...

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

List Of Figures

LIST OF FIGURES

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: The Global Post-Quantum Cryptography Market 2026–2036
Product link: https://marketpublishers.com/r/G3728B901453EN.html
Price: US$ 1,400.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/G3728B901453EN.html