

WHITEPAPER

Quantum-Based Cryptography Market Breakdown

Market volumes, projected CAGR, and investor-relevant
segmentation for PQC solutions and PQC-transition
services

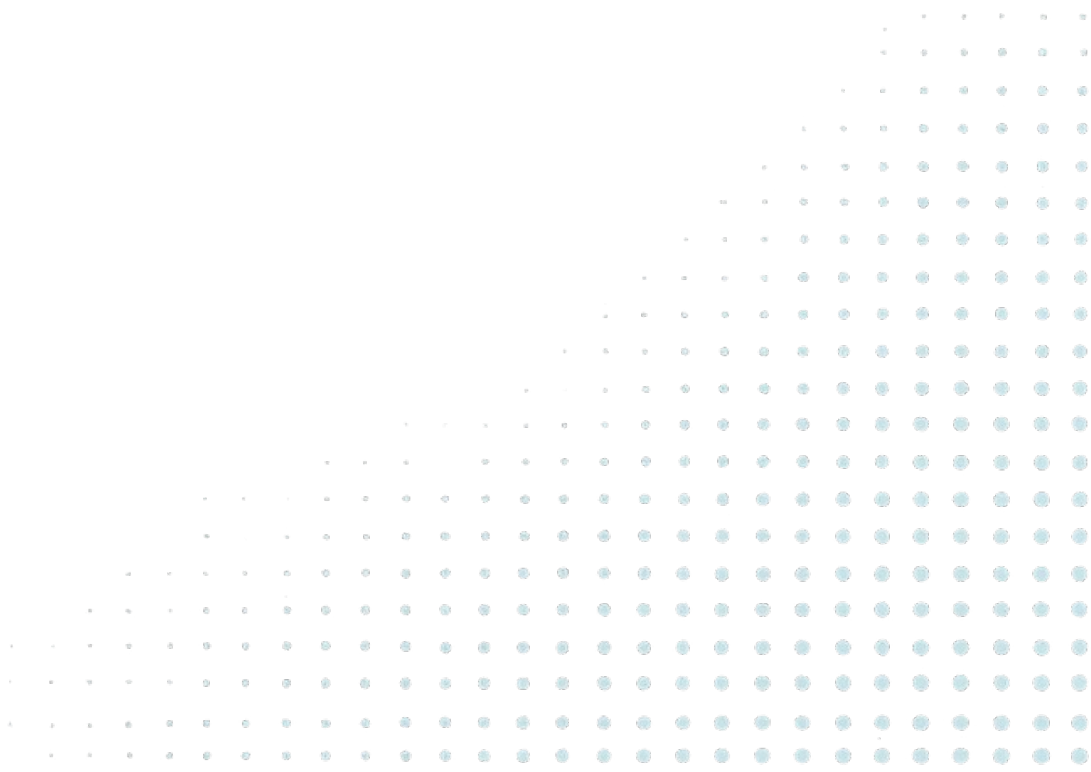
7 July 2026

Prepared as a public-source working view



Method note

This document uses public report pages, press releases, analyst abstracts, and official sources. It does not access paid report bodies. Public figures are useful for triangulation, but the market definitions are not always comparable. PQC, QKD, QRNG, quantum communications, and quantum networking should be modelled separately.



Contents

01	Scope used.....	04
02	Market summary.....	06
03	Investor-ready modelling notes.....	12
	Source index.....	14

CHAPTER

01

Scope used



- Core PQC market: post-quantum cryptography software, libraries, SDKs, protocol upgrades, PKI and certificate migration, HSM/KMS upgrades, cryptographic discovery, CBOM, risk assessment, migration services, managed services, and crypto-agility tools.
- Broader quantum-based cryptography: PQC plus QKD, QRNG, quantum communication, and quantum networking. These markets should not be added together without adjustment.
- Investor segmentation: software, HSMs, PKI, discovery/CBOM, consulting, managed services, and infrastructure should be shown as separate revenue layers.

CHAPTER

02

Market summary



The pure PQC market is still early, but public forecasts show high growth. Public forecasts found for core PQC range from USD 0.42 billion to USD 1.68 billion in 2025. By 2030, public estimates range from USD 2.84 billion to USD 4.60 billion. Longer forecasts reach USD 8.49 billion by 2032, USD 20.5 billion by 2033, USD 29.95 billion by 2034, or USD 13 billion by 2035.

The public CAGR range for core PQC is about 30% to 46%. A practical investor base case is 35% to 40% CAGR through 2030 for core PQC solutions. PQC-transition services can be modelled higher in the early phase, around 45% to 50%, because discovery, CBOM, risk assessment, and migration planning precede broad product replacement.

The broader quantum cryptography market is not the same market. It often includes QKD, quantum communication, and quantum-security hardware. These figures are useful for context, but not for a pure PQC TAM.

The main growth driver is now a compliance and procurement cycle, not only a future quantum-risk story. NIST standards, US federal deadlines, the UK NCSC timeline, the EU coordinated roadmap, NSA guidance, and defence procurement rules create concrete migration demand.

Table 1. Investor at-a-glance market model

Market layer	Public sizing signal	Investor treatment
Core PQC solutions	2025: USD 0.42bn-1.68bn. 2030: USD 2.84bn-4.60bn. Longer forecasts: USD 8.49bn by 2032, USD 20.5bn by 2033, USD 29.95bn by 2034, USD 13bn by 2035.	Use 35%-40% CAGR base case through 2030. Keep definitions tight.
PQC-transition services	No clean standalone public TAM found. Public segment indicators: MarketsandMarkets services CAGR 48.4%; Mordor services CAGR 46.03%; IDC expects 40% of G2000 to use services for quantum risk assessment by 2027.	Model as first revenue wave. Discovery and assessment should convert into platform, PKI, HSM, and migration pull-through.
Broader quantum cryptography	Public estimates include markets such as QKD and quantum communication. Fortune: USD 270.78mn in 2025 -> USD 2.263bn by 2034. Grand View: USD 518.3mn in 2023 -> USD 4.623bn by 2030.	Use as adjacent context only. Do not use as pure PQC TAM.
QKD, QRNG, quantum communication	QKD and QRNG are infrastructure/hardware-heavy markets. They have different buyers, cycles, and adoption barriers than PQC software migration.	Keep separate from PQC. Count only where a vendor has direct QKD/QRNG revenue.

Table 2. Top ten public reports and analyst sources

Source	Market definition	Public sizing / CAGR	Key investor finding
1. Gartner	Analyst guidance, not a public TAM report.	No public market-size figure in the accessible abstract.	Strong timing signal. Gartner supports planning and execution toward a 2030 target.
2. IDC	Analyst guidance on services demand.	No public TAM figure in the accessible article.	Strong signal for PQC-transition services and quantum risk assessment demand.
3. Forrester	Analyst guidance, not a public market-size report.	No public TAM figure in the accessible article.	Useful board narrative: PQC is a multi-year migration, not a point product purchase.
4. MarketsandMarkets	Core PQC. Includes solutions and services.	USD 0.42bn in 2025 -> USD 2.84bn in 2030; CAGR 46.2%. Services CAGR 48.4%.	Good lower-bound 2030 estimate for pure PQC. Strong signal for migration services.

Source	Market definition	Public sizing / CAGR	Key investor finding
5. Grand View Research	Core PQC.	USD 1.6bn in 2025; USD 2.2bn in 2026 -> USD 20.5bn in 2033; CAGR 37.8%.	Good upside case. Likely broader solution and service inclusion than lower estimates.
6. Juniper Research	Core PQC.	USD 1.2bn in 2026 -> USD 13bn in 2035; implied CAGR about 30%.	More conservative long-range CAGR. Useful as a low-growth long-range case.
7. Precedence Research	Core PQC with broad segmentation across services, type, solution, enterprise size, vertical, and region.	USD 1.68bn in 2025 -> USD 29.95bn in 2034; CAGR 37.72%.	High long-range upside case. Also useful for service segmentation.
8. Verified Market Research	Core PQC.	USD 1.18bn in 2024 -> USD 8.49bn by 2032; quoted CAGR 32.6% from 2026 to 2032.	Useful cross-check. Handle carefully because endpoint-implied CAGR differs from quoted 2026-2032 CAGR.
9. Mordor Intelligence	Core PQC with detailed public segmentation.	USD 0.88bn in 2025 -> USD 4.60bn in 2030; CAGR 39.27%.	Good 2030 base case. Gives useful public segment data for software, services, cloud, and regions.
10. Fortune Business Insights	Broader quantum cryptography; likely includes QKD and quantum-security hardware. Not pure PQC.	USD 270.78mn in 2025; USD 345.5mn in 2026 -> USD 2.263bn by 2034; CAGR 26.50%.	Use as adjacent quantum-cryptography context only. Do not use as pure PQC TAM.

Table 3. Market-sizing triangulation by market bucket

Market bucket	Public market-size range	CAGR range	Include / exclude	Investor use
Core PQC software and services	2025: USD 0.42bn-1.68bn. 2030: USD 2.84bn-4.60bn. Longer range: USD 8.49bn-29.95bn by 2032-2034; Juniper also gives USD 13bn by 2035.	About 30%-46%.	Include PQC libraries, SDKs, crypto-agility, PQC-enabled TLS/VPN/API security, PKI migration, HSM/KMS upgrades, discovery, CBOM, risk assessment, consulting, managed services. Exclude QKD and pure quantum networking.	Main investor TAM. Use 35%-40% CAGR as base case.
PQC-transition services	No single public TAM found. Public signals: MarketsandMarkets services CAGR 48.4%; Mordor services CAGR 46.03%; IDC expects 40% of G2000 to use cybersecurity professional services for quantum risk assessments by 2027.	About 46%-48% in public segment indicators.	Include crypto inventory, CBOM, quantum risk assessment, roadmap, architecture, testing, migration execution, assurance, and compliance evidence. Exclude generic cybersecurity services not linked to cryptographic migration.	Near-term revenue wedge. Likely first spend before product roll-out.
Broader quantum cryptography	Fortune: USD 270.78mn in 2025 -> USD 2.263bn by 2034. Grand View: USD 518.3mn in 2023 -> USD 4.623bn by 2030. Mordor: USD 0.70bn in 2025 -> USD 2.98bn by 2031.	About 26%-38%, depending on definition.	Include QKD, quantum encryption, some quantum-security hardware, and sometimes PQC. Exclude pure PQC if the report does not separate it.	Use only for adjacent market story and definition check.
QKD market	Grand View: USD 446.0mn in 2024 -> USD 2.488bn by 2030.	33.5%.	Include dedicated QKD systems, optical links, trusted nodes, telecom/security hardware. Exclude PQC software migration, PKI migration, CBOM, and HSM upgrades unless bundled.	Adjacent telecom and government infrastructure market. Not a substitute for broad PQC migration.
Quantum communication market	Grand View: USD 1.103bn in 2024 -> USD 5.399bn by 2030. Fortune: USD 1.275bn in 2026 -> USD 11.974bn by 2034.	About 31.8%-32.31%.	Include quantum communication systems, QKD networks, quantum networking, and QRNG sub-segments. Exclude enterprise PQC software and transition services unless explicitly included.	Useful for infrastructure investors, not for pure PQC valuation.
QRNG / quantum entropy	Grand View QRNG segment in quantum communication: USD	About 12.8%-31%, depending on parent market.	Include QRNG chips, modules, entropy services, and secure random	Adjacent security hardware. Useful for HSM, IoT, telecom, and national

Market bucket	Public market-size range	CAGR range	Include / exclude	Investor use
	140mn in 2024 -> USD 660mn by 2030. Another Grand View TRNG view places quantum QRNG at USD 798.3mn in 2024 -> USD 1.636bn by 2030.		generation hardware. Exclude PQC algorithms and migration services.	security use cases.

Table 4. Market developments - general market and PQC-specific impact

Development	General quantum-based cryptography impact	PQC-specific impact	Investor read-through
NIST final standards	Separates standards-based PQC from quantum hardware markets.	FIPS 203, 204, and 205 create the technical basis for procurement.	Turns PQC from R&D into migration and compliance spend.
US federal deadlines	Strong pull for federal suppliers and critical infrastructure.	Key establishment by 2030; digital signatures by 2031; covered contractors by 2030.	Creates a procurement calendar for SaaS, HSM, PKI, cloud, security vendors, and contractors.
CBOM and cryptographic asset discovery	Creates a new evidence and audit layer across cybersecurity.	Requires discovery of algorithms, protocols, keys, certificates, libraries, and dependencies.	Strong signal for discovery, CBOM, crypto inventory, and continuous monitoring tools.
UK migration milestones	Sets a clear timeline for large and regulated organisations.	Discovery by 2028, priority migration by 2031, full migration by 2035.	Supports multi-year budget plans and early service revenue.
EU coordinated roadmap	Reduces fragmentation across EU member states.	Gives a harmonised transition plan for PQC adoption.	Good for EU public sector, telecom, finance, identity, and critical infrastructure pipelines.
NSA CNSA 2.0 / national security systems	Pushes high-assurance users away from waiting.	CNSA 2.0 algorithms will be required for national security systems.	Strong signal for defence, aerospace, government cloud, secure communications, HSMs, and long-life systems.
US defence PQC strategy	Distinguishes PQC from QKD and quantum networking for defence migration.	Lines of effort include inventory, algorithm/protocol development, commercial integration, and quantum-resistant device deployment.	Defence buyers need both commercial PQC products and integration services.
Internet-scale key exchange migration	Shows that PQC is already moving through web infrastructure.	TLS key exchange is the first large-scale PQC deployment area.	Supports cloud, CDN, SASE, VPN, API security, and protocol-stack vendors.
Cloudflare deployment signal	Shows practical deployment at internet scale.	PQC key exchange can be deployed before full certificate/signature migration.	Proof point for product adoption in internet infrastructure.
Post-quantum Web PKI path	Moves PQC from encryption to authentication and certificates.	Lets Encrypt targets staging for Merkle Tree Certificates in late 2026 and production-ready environment in 2027.	PKI and certificate lifecycle management will be a large migration layer.
IETF TLS ML-KEM standardisation	Shows standards work moving into internet protocols.	Defines ML-KEM groups for TLS 1.3 key establishment.	Supports productisation in TLS stacks, browsers, proxies, gateways, VPNs, and service meshes.
Migration duration and cost	Quantum-safe transition is an enterprise change programme.	Discovery, planning, implementation, and assurance can take more than five years.	Supports services, managed migration, tooling, testing, and audit evidence.
QKD remains separate	QKD is a hardware and network market.	QKD does not replace broad PQC migration across software, PKI, applications, and devices.	Do not include QKD revenue in core PQC TAM unless the vendor sells both.

Table 5. PQC solution and transition-services segmentation

Segment	Buyer problem	Revenue model	Adoption signal	Include in PQC TAM?
Cryptographic discovery and CBOM	Organisations do not know where RSA, ECC, DH, ECDSA, certificates, keys,	SaaS, asset scanning, agent-based discovery, API discovery,	White House requires guidance on CBOM elements; NCSC requires	Yes. Core transition-services and tooling TAM.

Segment	Buyer problem	Revenue model	Adoption signal	Include in PQC TAM?
	libraries, and protocols are used.	SBOM/CBOM modules, audit reports.	discovery by 2028.	
Quantum risk assessment	Boards need to know which data and systems are exposed to harvest-now-decrypt-later risk.	Consulting, assessment projects, managed risk register, roadmap.	IDC predicts 40% of G2000 will use professional services for quantum risk assessments by 2027.	Yes. Near-term service wedge.
Crypto-agility platform	Organisations need to replace algorithms without large future rework.	SaaS platform, policy engine, orchestration, compliance module, managed service.	Gartner recommends inventory, then encryption/key exchange, PKI, and signatures in waves.	Yes. Core PQC control-plane TAM.
PQC software libraries and SDKs	Developers need NIST-standard algorithms in applications, devices, and infrastructure.	Developer libraries, enterprise SDKs, support subscriptions, embedded licensing.	Mordor says software libraries and SDKs captured 41% of market size in 2024.	Yes. Core PQC solution TAM.
PQC-enabled TLS, VPN, API, SASE, and service mesh	Network traffic needs quantum-resistant key establishment.	Product upgrade, cloud security subscriptions, gateway licensing, SASE bundles.	Google, Cloudflare, and IETF show real deployment and protocol work.	Yes, if product revenue is tied to PQC capability.
PKI, certificate lifecycle, and digital signatures	Certificates, code signing, device identity, document signing, and authentication need PQC-safe signatures.	CLM software, CA services, managed PKI, signing services, HSM-backed signing.	White House sets digital-signature transition by 2031; Lets Encrypt is preparing post-quantum Web PKI paths.	Yes. Large second-wave PQC TAM.
HSM, KMS, secure elements, and cryptographic modules	Keys and signatures need certified hardware/software modules with PQC support.	Hardware refresh, cloud KMS, HSM subscription, validation services.	Forrester has a dedicated report on HSM requirements for the post-quantum era; the HSM market is forecast around USD 1.8bn-2.0bn in 2026 and USD 4.55bn-6.7bn by 2034/2035.	Partly. Count only PQC-driven uplift in core PQC TAM; keep base HSM market separate.
Migration consulting and implementation	Enterprises need programme design, vendor selection, testing, rollout, and change control.	Consulting, systems integration, migration factory, managed service.	Precedence says design, implementation, and consulting had the biggest service share in 2024; MarketsandMarkets puts services CAGR at 48.4%.	Yes. Core transition-services TAM.
Managed PQC operations	Organisations need continuous crypto posture management after migration.	Managed detection, managed PKI/HSM, compliance evidence, periodic recertification.	NIST says products, services, and protocols need updates and organisations must identify vulnerable algorithms.	Yes. Recurring services TAM.
Compliance evidence and assurance	Regulators, customers, and procurement teams need proof of PQC readiness.	SaaS evidence layer, supplier portal, audit exports, policy mapping.	White House procurement rules and UK/EU roadmaps create compliance demand.	Yes. Strong fit for regulated sectors.
QKD infrastructure	Point-to-point quantum-secure key exchange for selected networks.	Hardware, optical network integration, telecom services.	Grand View estimates QKD at USD 446.0mn in 2024 -> USD 2.488bn by 2030.	No for core PQC TAM. Adjacent only.
QRNG / entropy hardware	High-quality randomness for keys, HSMs, chips, IoT, telecom, and security modules.	Chips, modules, entropy-as-a-service, embedded licensing.	Grand View has QRNG segment estimates from USD 140mn or USD 798.3mn in 2024, depending on market definition.	No for core PQC TAM. Adjacent only.

Table 6. Investment and macro sources

Source	What it adds	Key data point	Use in investor deck
McKinsey Quantum Technology Monitor 2026	Private investment context across quantum technology.	Quantum technology start-up investment reached USD 12.6bn in 2025, 6.3x 2024; 90% went to quantum computing.	Use as quantum-sector momentum, not as PQC TAM.
McKinsey public/private split	Shows the shift from public to private capital in 2025.	Public sources were about one-third of investment in 2024, but 3% in 2025.	Useful to show private capital acceleration.
European Commission Quantum Technologies Flagship	EU public investment context.	Expected EU budget of EUR 1bn over 10 years.	Use as public-sector quantum infrastructure signal, not PQC sizing.

Source	What it adds	Key data point	Use in investor deck
UK National Quantum Strategy	UK public investment context.	UK commits GBP 2.5bn over 10 years.	Use as sovereign quantum-policy support.
IMF	Financial-system risk framing.	IMF says financial institutions should inventory public-key cryptography and migrate to PQC.	Useful for financial-sector urgency.
JPMorgan	Large-bank awareness and R&D context.	JPMorgan frames post-quantum encryption preparation as a current need.	Use as enterprise buyer validation, not market sizing.
Goldman Sachs	Investor and security context.	Notes that quantum computing could overwhelm existing encryption protocols.	Use as capital-market awareness signal.
BlackRock iShares Quantum Computing UCITS ETF	Public-market exposure to the quantum theme.	ETF gives exposure to companies in the quantum computing theme.	Use only as investor interest signal. Not a PQC source.
World Bank digital identity / PKI materials	Digital public infrastructure and PKI risk context.	World Bank sources discuss PKI and digital signatures in digital ID. No World Bank PQC TAM or CAGR source was found in the prior public-source scan.	Use for DPI and identity-risk context, not for market sizing.

CHAPTER

03

Investor-ready modelling notes



Table 7. TAM rings for investor modelling

TAM ring	Definition	Baseline	2030 / long-range view	Suggested treatment
Ring 1: Core PQC solutions	Libraries, SDKs, PQC-enabled protocols, PKI, HSM/KMS PQC uplift, crypto-agility tools.	2025: USD 0.42bn-1.68bn.	2030: USD 2.84bn-4.60bn. Upside: USD 20.5bn by 2033 and USD 29.95bn by 2034.	Use 35%-40% CAGR as base case.
Ring 2: PQC-transition services	Discovery, CBOM, quantum risk assessment, migration planning, implementation, testing, assurance.	No clean standalone TAM.	Service CAGR indicators around 46%-48%.	Model as first spend wave. It should convert into product pull-through.
Ring 3: Adjacent security infrastructure	HSMs, KMS, PKI/CLM, certificate authorities, secure elements, IoT/device identity, SASE, VPN, API security.	HSM market alone is around USD 1.8bn-2.0bn in 2026 across public estimates.	HSM forecasts reach USD 4.55bn-6.7bn by 2034/2035.	Do not count the full market as PQC. Count PQC-driven refresh, attach, or price uplift.
Ring 4: Quantum communication / QKD / QRNG	QKD, quantum networks, quantum communication systems, QRNG hardware.	Quantum communication: USD 1.103bn in 2024. QKD: USD 446mn in 2024.	Quantum communication: USD 5.399bn by 2030. QKD: USD 2.488bn by 2030.	Keep separate. Useful for strategic adjacency, not for core PQC revenue.

Key messages for slides or investor discussion

- Use a three-ring model for PQC: core PQC software, PQC-transition services, and adjacent security infrastructure. Keep QKD, QRNG, and quantum communication as a separate adjacency.
- Near-term revenue is services-led. Discovery, CBOM, quantum risk assessment, and migration planning should come before broad replacement.
- The first product wave is key establishment: TLS, VPN, SASE, cloud, and API security.
- The second product wave is authentication and digital signatures: PKI, certificate lifecycle management, code signing, document signing, device identity, object identity, and trust chains.
- Base-case CAGR for core PQC should be 35%-40%. Use 45%-50% for transition services in the early phase. Do not use broad quantum cryptography CAGRs unless the deck clearly states that QKD, QRNG, and quantum communication are included.

APPENDIX

Source index



Table 8. Source index with full URLs

#	Publisher	Source title	Citation and full URL
1	Gartner	Postquantum Cryptography: Why You Need to Be Ready by 2030.	Citation: Gartner. (various years). Postquantum Cryptography: Why You Need to Be Ready by 2030. Evidence quote: Full source URL listed below. Full URL: https://www.gartner.com/en/documents/7116630
2	Gartner	Postquantum Cryptography Migration Is Advancing in 3 Waves.	Citation: Gartner. (various years). Postquantum Cryptography Migration Is Advancing in 3 Waves. Evidence quote: Full source URL listed below. Full URL: https://www.gartner.com/en/documents/7967605
3	IDC	Is Your Business Quantum-Ready? Why Risk Assessments Are Critical Now.	Citation: IDC. (various years). Is Your Business Quantum-Ready? Why Risk Assessments Are Critical Now. Evidence quote: Full source URL listed below. Full URL: https://www.idc.com/resource-center/blog/is-your-business-quantum-ready-why-risk-assessments-are-critical-now/
4	Forrester	It's Time To Start Planning Your Postquantum Migration.	Citation: Forrester. (various years). It's Time To Start Planning Your Postquantum Migration. Evidence quote: Full source URL listed below. Full URL: https://www.forrester.com/blogs/its-time-to-start-planning-your-postquantum-migration/
5	Forrester	Hardware Security Module Requirements For The Post-Quantum Era.	Citation: Forrester. (various years). Hardware Security Module Requirements For The Post-Quantum Era. Evidence quote: Full source URL listed below. Full URL: https://www.forrester.com/report/hardware-security-module-requirements-for-the-post-quantum-era/RES190874
6	MarketsandMarkets	Post-Quantum Cryptography Market.	Citation: MarketsandMarkets. (various years). Post-Quantum Cryptography Market. Evidence quote: Full source URL listed below. Full URL: https://www.marketsandmarkets.com/Market-Reports/post-quantum-cryptography-market-126986626.html
7	Grand View Research	Post-Quantum Cryptography Market Report.	Citation: Grand View Research. (various years). Post-Quantum Cryptography Market Report. Evidence quote: Full source URL listed below. Full URL: https://www.grandviewresearch.com/industry-analysis/post-quantum-cryptography-market-report
8	Juniper Research	Post-quantum Cryptography Market to Exceed \$13 Billion by 2035.	Citation: Juniper Research. (various years). Post-quantum Cryptography Market to Exceed \$13 Billion by 2035. Evidence quote: Full source URL listed below. Full URL: https://www.juniperresearch.com/press/post-quantum-cryptography-market-to-exceed-13-billion-by-2035-as-q-day-awareness-accelerates/
9	Precedence Research	Post Quantum Cryptography Market.	Citation: Precedence Research. (various years). Post Quantum Cryptography Market. Evidence quote: Full source URL listed below. Full URL: https://www.precedenceresearch.com/post-quantum-cryptography-market
10	Verified Market Research	Post-Quantum Cryptography Market.	Citation: Verified Market Research. (various years). Post-Quantum Cryptography Market. Evidence quote: Full source URL listed below. Full URL: https://www.verifiedmarketresearch.com/product/post-quantum-cryptography-pqc-market/
11	Mordor Intelligence	Post-Quantum Cryptography Market Size	Citation: Mordor Intelligence. (various years). Post-

#	Publisher	Source title	Citation and full URL
		& Share Analysis.	Quantum Cryptography Market Size & Share Analysis. Evidence quote: Full source URL listed below. Full URL: https://www.mordorintelligence.com/industry-reports/post-quantum-cryptography-market
12	Fortune Business Insights	Quantum Cryptography Market Size, Share & Industry Analysis.	Citation: Fortune Business Insights. (various years). Quantum Cryptography Market Size, Share & Industry Analysis. Evidence quote: Full source URL listed below. Full URL: https://www.fortunebusinessinsights.com/industry-reports/quantum-cryptography-market-100211
13	NIST	Post-Quantum Cryptography FIPS Approved.	Citation: NIST. (various years). Post-Quantum Cryptography FIPS Approved. Evidence quote: Full source URL listed below. Full URL: https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved
14	NIST	Post-Quantum Cryptography project page.	Citation: NIST. (various years). Post-Quantum Cryptography project page. Evidence quote: Full source URL listed below. Full URL: https://csrc.nist.gov/projects/post-quantum-cryptography
15	The White House	Securing the Nation Against Advanced Cryptographic Attacks.	Citation: The White House. (various years). Securing the Nation Against Advanced Cryptographic Attacks. Evidence quote: Full source URL listed below. Full URL: https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/
16	UK NCSC	PQC migration timelines.	Citation: UK NCSC. (various years). PQC migration timelines. Evidence quote: Full source URL listed below. Full URL: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
17	European Commission	Coordinated implementation roadmap for transition to PQC.	Citation: European Commission. (various years). Coordinated implementation roadmap for transition to PQC. Evidence quote: Full source URL listed below. Full URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
18	NSA	Future quantum-resistant algorithm requirements for national security systems.	Citation: NSA. (various years). Future quantum-resistant algorithm requirements for national security systems. Evidence quote: Full source URL listed below. Full URL: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/
19	DoD CIO	Post-Quantum Cryptography Strategy.	Citation: DoD CIO. (various years). Post-Quantum Cryptography Strategy. Evidence quote: Full source URL listed below. Full URL: https://dodcio.defense.gov/Portals/0/Documents/Library/DoW-PQC-Strategy.pdf
20	Google Chromium Blog	Advancing our amazing bet on asymmetric cryptography.	Citation: Google Chromium Blog. (various years). Advancing our amazing bet on asymmetric cryptography. Evidence quote: Full source URL listed below. Full URL: https://blog.google/chromium/advancing-our-amazing-bet-on-asymmetric/
21	Cloudflare	Post-quantum roadmap.	Citation: Cloudflare. (various years). Post-quantum roadmap.

#	Publisher	Source title	Citation and full URL
			Evidence quote: Full source URL listed below. Full URL: https://blog.cloudflare.com/post-quantum-roadmap/
22	Let's Encrypt	Post-quantum certificates.	Citation: Let's Encrypt. (various years). Post-quantum certificates. Evidence quote: Full source URL listed below. Full URL: https://letsencrypt.org/2026/06/03/pq-certs
23	IETF	ML-KEM Post-Quantum Key Agreement for TLS 1.3.	Citation: IETF. (various years). ML-KEM Post-Quantum Key Agreement for TLS 1.3. Evidence quote: Full source URL listed below. Full URL: https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem/
24	TNO / AIVD / CWI	PQC migration handbook.	Citation: TNO / AIVD / CWI. (various years). PQC migration handbook. Evidence quote: Full source URL listed below. Full URL: https://publications.tno.nl/publication/34643386/fXcP VHsX/TNO-2024-pqc-en.pdf
25	Grand View Research	Quantum Key Distribution Market Report.	Citation: Grand View Research. (various years). Quantum Key Distribution Market Report. Evidence quote: Full source URL listed below. Full URL: https://www.grandviewresearch.com/industry-analysis/quantum-key-distribution-market-report
26	Grand View Research	Quantum Communication Market Report.	Citation: Grand View Research. (various years). Quantum Communication Market Report. Evidence quote: Full source URL listed below. Full URL: https://www.grandviewresearch.com/industry-analysis/quantum-communication-market-report
27	Grand View Research	QRNG statistics - TRNG market.	Citation: Grand View Research. (various years). QRNG statistics - TRNG market. Evidence quote: Full source URL listed below. Full URL: https://www.grandviewresearch.com/horizon/statistics/true-random-number-generator-market/type/quantum-random-number-generator-qrng/global
28	Grand View Research	QRNG statistics - quantum communication market.	Citation: Grand View Research. (various years). QRNG statistics - quantum communication market. Evidence quote: Full source URL listed below. Full URL: https://www.grandviewresearch.com/horizon/statistics/quantum-communication-market-outlook/solutions/quantum-random-number-generator-qrng/global
29	Persistence Market Research	Hardware Security Modules Market.	Citation: Persistence Market Research. (various years). Hardware Security Modules Market. Evidence quote: Full source URL listed below. Full URL: https://www.persistencemarketresearch.com/market-research/hardware-security-modules-market.asp
30	McKinsey & Company	Quantum Technology Monitor 2026.	Citation: McKinsey & Company. (various years). Quantum Technology Monitor 2026. Evidence quote: Full source URL listed below. Full URL: https://www.mckinsey.com/capabilities/mckinsey-technology/our-insights/mckinsey-quantum-technology-monitor-2026-a-commercial-tipping-point
31	McKinsey & Company	Quantum investment surge.	Citation: McKinsey & Company. (various years). Quantum investment surge. Evidence quote: Full source URL listed below. Full URL: https://www.mckinsey.com/featured-insights/week-in-charts/quantum-investment-surge
32	European Commission	Quantum Technologies Flagship.	Citation: European Commission. (various years).

#	Publisher	Source title	Citation and full URL
			Quantum Technologies Flagship. Evidence quote: Full source URL listed below. Full URL: https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship
33	UK NQCC / UK Government	National Quantum Strategy.	Citation: UK NQCC / UK Government. (various years). National Quantum Strategy. Evidence quote: Full source URL listed below. Full URL: https://www.nqcc.ac.uk/about-us/national-quantum-strategy/
34	International Monetary Fund	Quantum Computing's Possibilities and Perils.	Citation: International Monetary Fund. (various years). Quantum Computing's Possibilities and Perils. Evidence quote: Full source URL listed below. Full URL: https://www.imf.org/en/publications/fandd/issues/2021/09/quantum-computings-possibilitiesand-perils-deodoro
35	JPMorgan	Quantum Computing and the Future of Encryption.	Citation: JPMorgan. (various years). Quantum Computing and the Future of Encryption. Evidence quote: Full source URL listed below. Full URL: https://www.jpmorgan.com/payments/payments-unbound/volume-2/quantum-computers-will-redefine-encryption
36	Goldman Sachs	Can Europe beat China and the US in quantum computing?	Citation: Goldman Sachs. (various years). Can Europe beat China and the US in quantum computing? Evidence quote: Full source URL listed below. Full URL: https://www.goldmansachs.com/insights/articles/can-europe-beat-china-and-the-us-in-quantum-computing
37	BlackRock	iShares Quantum Computing UCITS ETF.	Citation: BlackRock. (various years). iShares Quantum Computing UCITS ETF. Evidence quote: Full source URL listed below. Full URL: https://www.blackrock.com/se/individual/products/345953/ishares-quantum-computing-ucits-etf
38	World Bank	Digital identity / PKI materials.	Citation: World Bank. (various years). Digital identity / PKI materials. Evidence quote: Full source URL listed below. Full URL: https://documents1.worldbank.org/curated/en/099090425092038437/pdf/P507040-56c0ebfb-4d44-4670-bc35-1b7c8b810935.pdf

AI Disclosure

HINWEIS ZUR KI-NUTZUNG · EU AI ACT ART. 50

This content was created with the assistance of AI systems (large language models). It has been reviewed for accuracy by Spherity staff prior to publication. Spherity is responsible for the content.

The cover imagery used in this document was generated using an AI image-generation tool. It is decorative and illustrative only — it does not depict real infrastructure, data, or any Spherity system.

This disclosure is provided in accordance with Article 50 of Regulation (EU) 2024/1689 (the EU AI Act) and Spherity's internal policy POL-0047 (AI Content Disclosure).