

▶ Quantum Security: a strategic imperative for banks and financial institutions



Overcoming the largest cryptographic migration ever

Quantum computers are expected to break today's public-key cryptography as early as the 2030s – potentially sooner – a risk confirmed by NIST, national authorities, and cybersecurity experts worldwide. “Harvest now, decrypt later” (HNDL) is an immediate threat, not an active breach; it is a large-scale data exfiltration that may be happening now. Adversaries can capture your traffic now and decrypt it as soon as a Cryptographically Relevant Quantum Computer is available.

A dual strategy – Post-Quantum Cryptography (PQC) + Quantum Key Distribution (QKD) – provides immediate risk reduction, a predictable and efficient migration path, and a durable foundation for long-term resilience.

Why finance is uniquely exposed ?

- ▶ Long data-retention and high confidentiality needs
- ▶ High liabilities & reputational costs for breaches
- ▶ Complex, heterogeneous cryptographic inventory that makes mass migration slow and error-prone

What's at stake ?

- ▶ Loss of customer trust, legal exposure and regulatory penalties
- ▶ Cost of emergency re-migrations and system downtime
- ▶ Exposure of archived, legally sensitive records

A practical, defense-in-depth approach: PQC + QKD

The leading global financials have embraced a comprehensive approach towards quantum-safe, which leverages both PQC and QKD, providing for a defense-in-depth approach to minimize the risk early and gain flexibility and cost-efficiency in the migration process.



- ▶ **PQC:** software-only algorithms designed to resist quantum attacks. Fast to deploy in new solutions, including IDQ's, but requires re-engineering, updates and hardware refresh across the infrastructure, with more potential future standards and repeated migrations.
- ▶ **QKD:** physics-based, provably secure key exchange for protecting keys in transit today and tomorrow. Fast to retrofit to provides a stable security backbone for core network keying.






Why combine them ?

PQC addresses most cases via software updates or re-engineering, albeit with a long and tedious implementation cycle. QKD reduces the attack surface for key network segments, lowers tail-risk from future PQC flaws, and minimizes high-impact emergency migrations.





Key benefits

 <p>Rapidly strengthens security for high-value inter-datacenter traffic</p>	 <p>Exchanges keys out-of-band with long-term security, fully mitigating HNDL exposure</p>	 <p>Provides a stable key layer that lowers pressure for urgent PQC migrations</p>	 <p>Maintains operational continuity with minimal impact on existing applications</p>	 <p>Delivers product-level certified key transport for sensitive and regulated environments</p>
---	---	---	--	--

Deployment blueprint (phased, low-disruption)

- 1 Assess & prioritize:** inventory cryptographic assets; classify links & archived data that are highest risk.
- 2 Protect the crown jewels:** deploy QKD at core DCI (data center interconnect) and clearing/settlement networks first.
- 3 Hybrid keying:** use QKD-derived keys as additional key material combined with PQC or symmetric keys (no rip-and-replace of apps).
- 4 Widen & operationalize:** use QKD-derived keys as additional key material combined with PQC or symmetric keys.
- 5 Maintain PQC roadmap:** layer PQC for endpoints and long-term archival encryption as NIST standards settle.



Cost & ROI drivers

- ▶ **Capex:** limited CAPEX due to retrofit of existing infrastructure with QKD, typically amortized over several years.
- ▶ **Opex:** service, monitoring, and minimal incremental management overhead.
- ▶ **ROI:** reduces probability and cost of emergency cryptographic migrations, avoids potential compliance fines and remediation costs, and protects high-value archives.

WHY ID QUANTIQUE

With IDQ's quantum-safe products, you can build an end-to-end and out-of-band key distribution infrastructure that is quantum-safe and future-proof. It's a complete, standards-based, and third-party certified solution for network encryption applications.

PROOF & CREDENTIALS

- ▶ Production deployments with tier-1 financials (references available on request)
- ▶ Third-party certifications and standards compliance
- ▶ 24/7 support, SLAs, and seamless solution integration



Take the first step toward quantum resilience

>> Book a 30-min briefing

ID Quantique, an IonQ company
www.idquantique.com | info@idquantique.com

