

▶ Quantum Security: a strategic imperative & growth opportunity for telecom operators



Benefit from 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.

Telecom has an opportunity to create **Quantum-Safe as a Service (QSaaS) offerings**. By embedding Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) into managed services, telecom operators can protect their own infrastructure while monetizing secure connectivity for enterprises and governments.

Why telecom is uniquely exposed ?

- ▶ Transports the world's most sensitive data
- ▶ Decades-long data and infrastructure lifecycles
- ▶ Massive, complex, heterogeneous networks
- ▶ Systemic risk from inter-carrier trust

What's at stake ?

- ▶ Retroactive exposure of sovereign traffic
- ▶ Loss of secure-connectivity leadership
- ▶ Forced, high-cost network migrations
- ▶ Regulatory and contract failure

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

The leading global telecom operators 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>Delivers product-level certified key transport for sensitive and regulated environments</p>	 <p>Maintains operational continuity with minimal impact on existing applications</p>	 <p>Enhance brand trust as a leader in next-generation secure networking</p>
---	---	--	--	---

Business opportunity: Quantum-Safe as a Service

Telecoms are ideally positioned to monetize quantum-safe capabilities:

- 
Enterprise & government upsell: premium, quantum-resilient connectivity services for sectors with high security needs.
- 
Turnkey quantum security: remove adoption barriers, the need for upfront investment and customer-operated infrastructure.
- 
Managed cryptographic lifecycle: bundle PQC migration roadmaps and QKD into managed security services.
- 
Compliance-driven adoption: position as the default provider meeting anticipated quantum-security mandates.



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:** avoid costly emergency migrations, capture premium service revenue, comply with emerging mandates, and protect national-level trust.

WHY ID QUANTIQUE

With IDQ's quantum-safe solutions, telecoms can both protect their own networks and launch revenue-generating, quantum-resilient services. Our technology is standards-based, third-party certified, and proven in carrier-scale environments.

- ▶ [Read our case study with Singtel](#)

PROOF & CREDENTIALS

- ▶ Production deployments with tier-1 carriers
- ▶ Proven expertise in knowledge transfer, GTM support and customer pilot programs
- ▶ Third-party certifications and standards compliance
- ▶ 24/7 support, SLAs, and seamless solution integration



Take the first step toward quantum resilience

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

>> [Book a 30-min briefing](#)

