QUANTUM-SAFE SECURITY FOR ENTERPRISE

Quantum technology enables unhackable communications.

Marc Nikles

13/10/2023

ID Quantique - Pioneer in Quantum Technology

20 YEARS QUANTUM INNOVATION

IDQ

Founded in 2001
By 4 quantum physicists from the University of Geneva

Offices in Geneva, Switzerland
Seoul, South Korea
Boston, USA

120+ employees, including 50 engineers/scientists

SK telecom T··

Investments in 2018 by SK Telecom & Deutsche Telekom

Strong IP – 175+ patents & trade secrets
Swiss Made quality label

Develops technologies and products based on quantum physics within 2 business units:

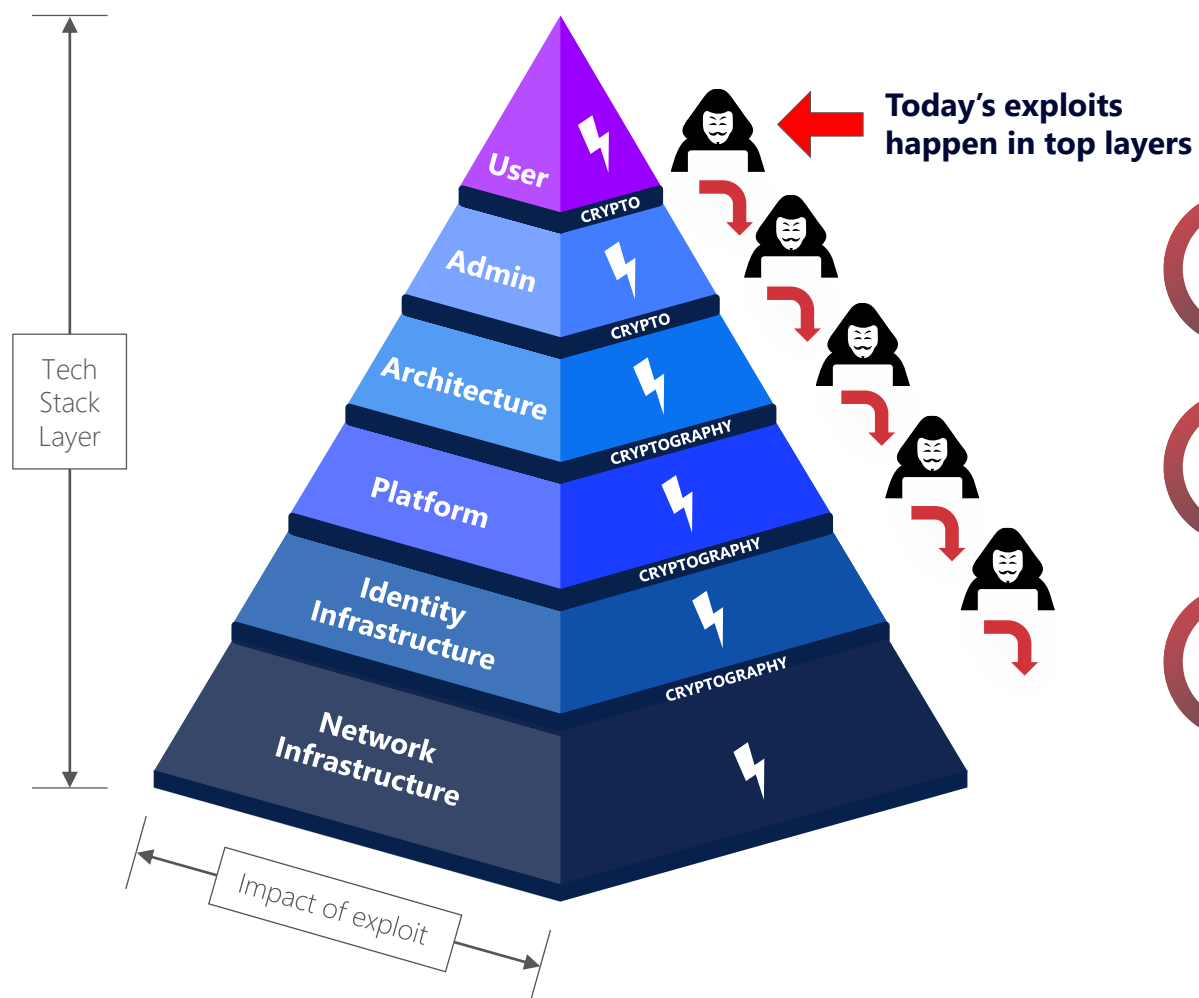Quantum-Safe Security

Quantum Photonic Sensing

Performs R&D, production, professional services, integration, support

Clients: Governments / Banks / Gaming Industry / Universities / IT Security

Today's Threat Vs Looming Quantum Threat

Today's exploits happen in top layers

Tech Stack Layer

User
Admin — CRYPTO
Architecture — CRYPTO
Platform — CRYPTOGRAPHY
Identity Infrastructure — CRYPTOGRAPHY
Network Infrastructure — CRYPTOGRAPHY
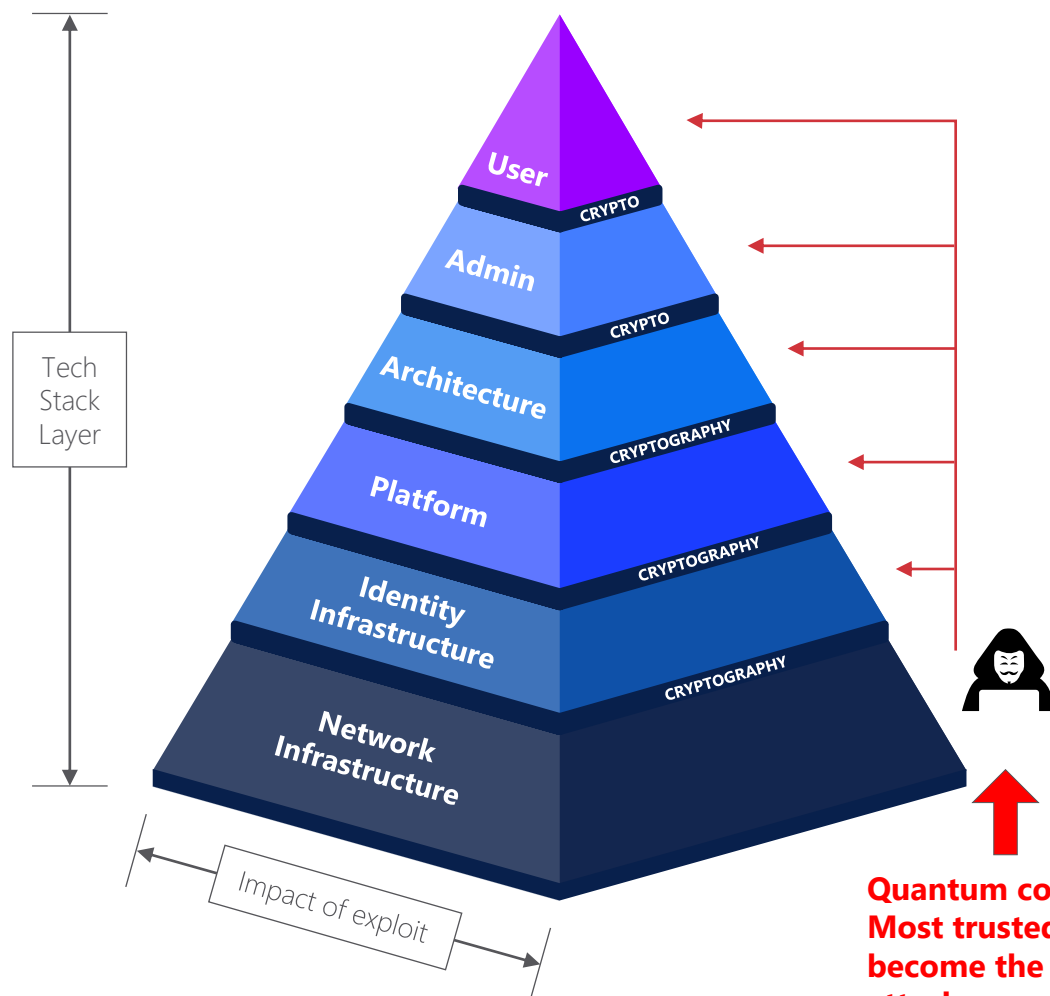
Impact of exploit

Enterprise has a cryptographic **RISK BLIND SPOT**

Discovery, cataloging and triaging is **DIFFICULT, MANUAL AND ERROR PRONE**

Migration to Quantum-Safe is the **LARGEST CRYPTOGRAPHIC MIGRATION EVER**

Today's Threat Vs Looming Quantum Threat

Tech Stack Layer

User — CRYPTO
Admin — CRYPTO
Architecture — CRYPTOGRAPHY
Platform — CRYPTOGRAPHY
Identity Infrastructure — CRYPTOGRAPHY
Network Infrastructure

Impact of exploit

Quantum computing = Most trusted elements become the easiest to attack

Enterprise has a cryptographic **RISK BLIND SPOT**

Discovery, cataloging and triaging is **DIFFICULT, MANUAL AND ERROR PRONE**

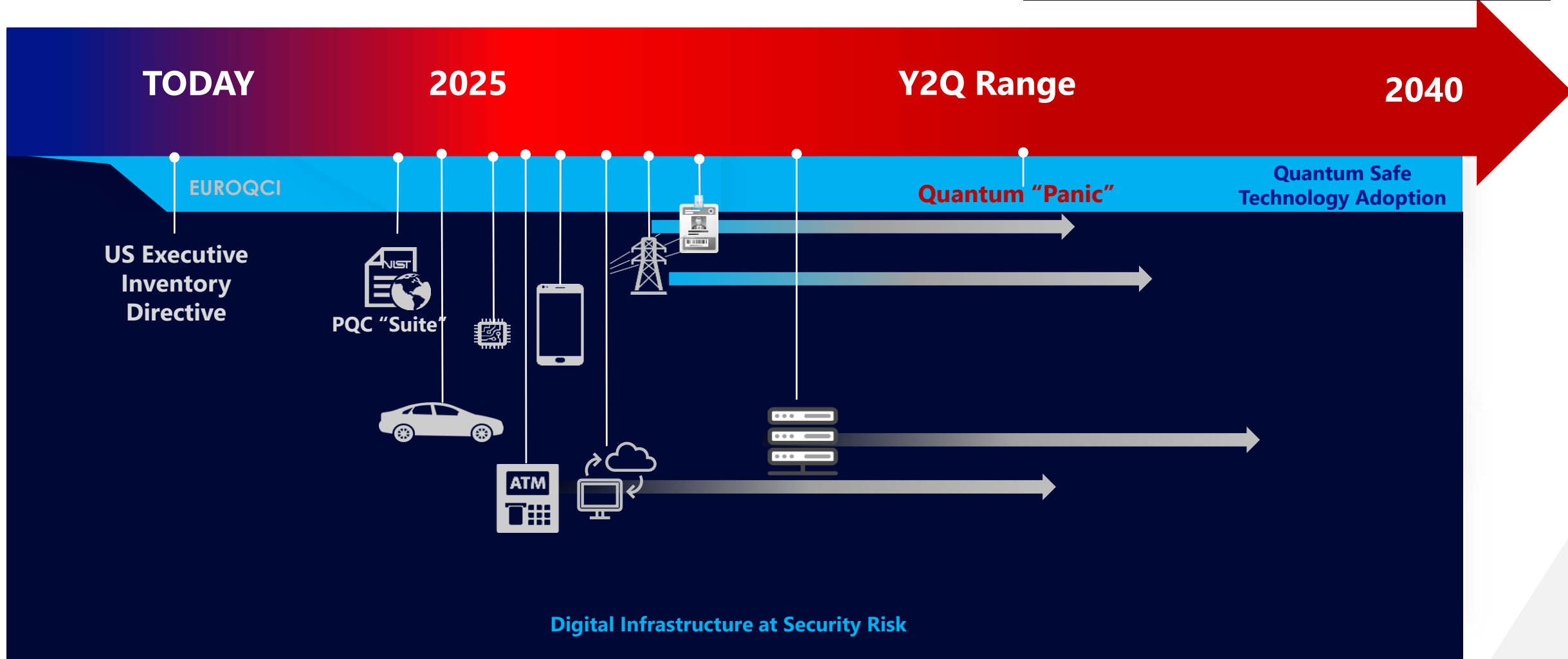Migration to Quantum-Safe is the **LARGEST CRYPTOGRAPHIC MIGRATION EVER**

Bridging the gap

Current Public Key Cryptography

Hybrid Cryptography

Current + Quantum-Safe

Quantum-Safe
PQC + QKD

Today

Quantum Safe Technology Adoption Timeline

Countdown to Y2Q

06 Years 199 Days 07 Hours 32 Minutes 45 Seconds

TODAY

2025

Y2Q Range

2040

EUROQCI

Quantum "Panic"

Quantum Safe Technology Adoption

US Executive Inventory Directive

PQC "Suite"

ATM

Digital Infrastructure at Security Risk

Quantum Key Distribution (QKD)

QKD ensures a provably secure key exchange, alerting to any potential eavesdropping, as well as providing forward secrecy of the encryption keys.

QKD provides the ultimate in quantum-safe security for long-term data protection.
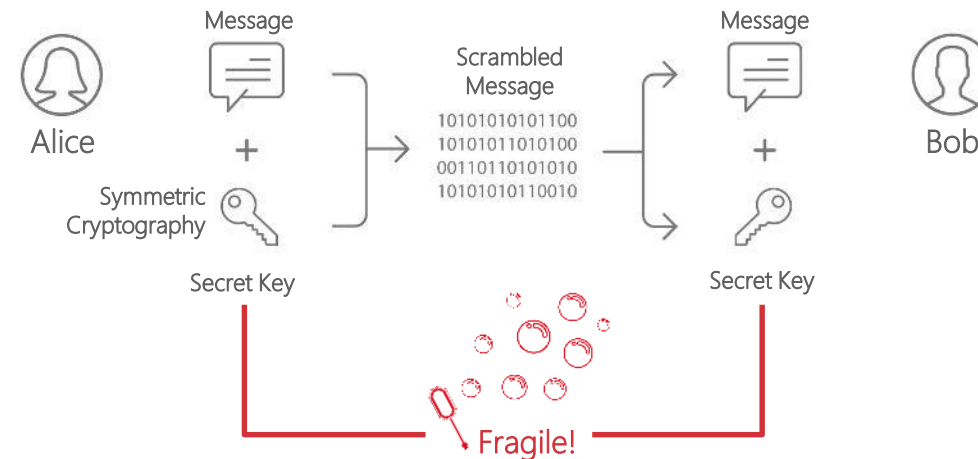
Quantum-Safe Security

Quantum Cyber Security tools to enable unbreakable communications

QRNG

Quantum Random Number Generation

- USB
- PCIe card
- Appliance
- Chips

QKD

Quantum Key Distribution

- For commercial production environments
- For academia, research institutes & innovation labs

Selected Case Studies

- Samsung Galaxy Quantum phones QRNG-Powered 5G smartphones

  NIST Entropy Source Validation (ESV) certified

- First nation-wide QKD network in Korea, linking 48 government organizations Total of 2000 km of QKD link installed

Key Management System – QNET & KMS Software

XG Series' systems can be deployed in any network configurations:

- Point to Point with Key Relay
- Ring
- Star
- Mesh

At each QKD node, an embedded **Key Management System (KMS)** software arbitrates the key distribution between QKD and manages key requests and key transfers between QKD optical systems and external encryptors.

Point-to-point (with relay)

Ring

Star

Key Consumer Layer (Encryptors)

KMS Layer

QMS

Key Provider Layer (QKDs)
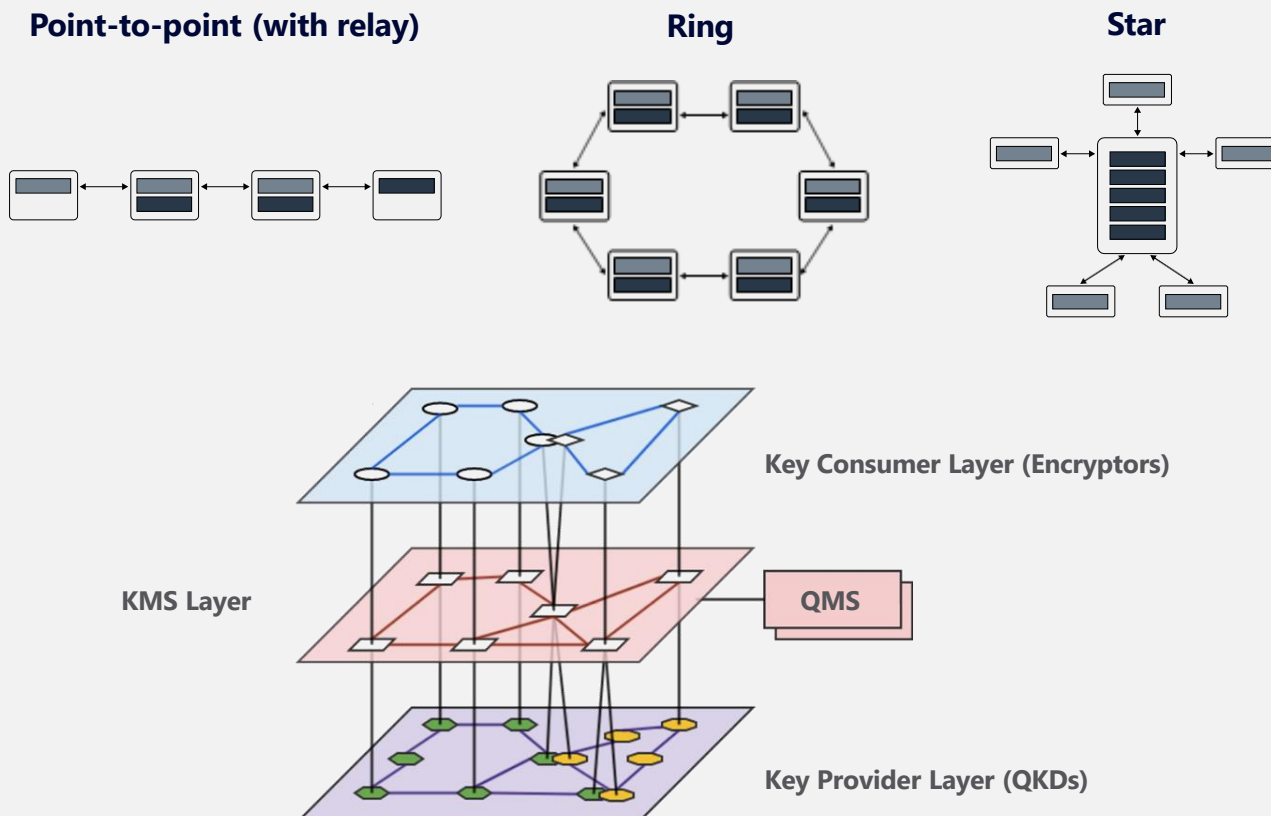
Quantum Safe PaaS

Model & service

Platform-aaS
for all networks

Quantum-Safe Bandwidth

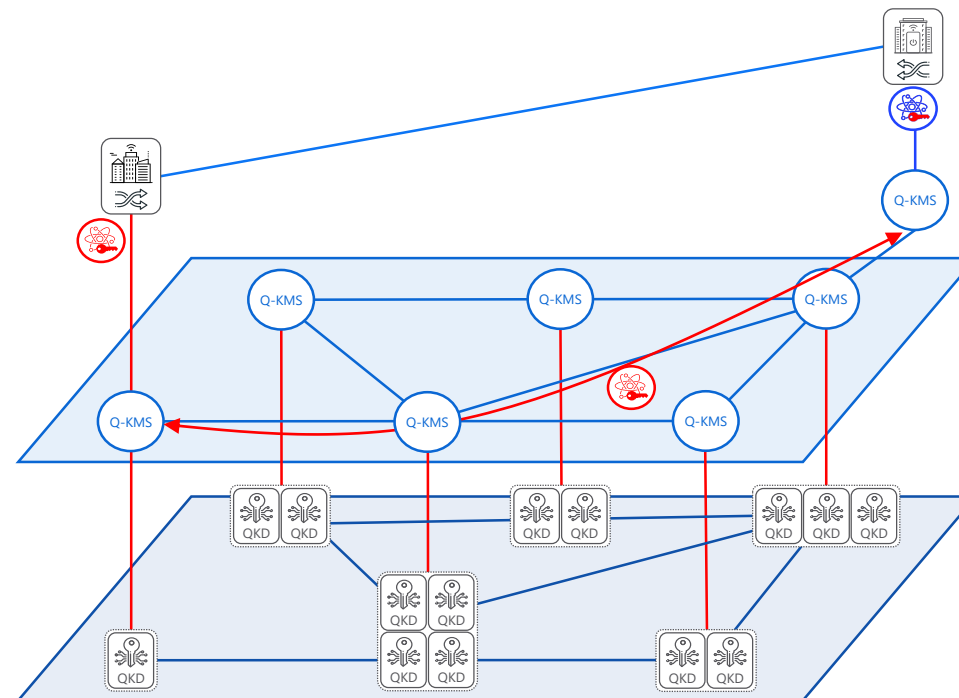**Enterprise client**

Quantum-Safe bandwidth Layer 1-3

Encryption

Telecom operator

Quantum Enhanced KMS

Open ETSI interface

Any network

Fiber

QKD

Secure Application Layer

Quantum Key Management System Layer

IDQ - **Clarion KX**

Quantum Key Distribution Layer

IDQ - **QKD XG Series**

Key takeaways

1 — Do not delay

(Crypto)
Winter is coming!

It will take time to implement solutions.

Start now!

2 — Know Your Data

Where are your vulnerabilities?

What needs to be protected?

For how long?

3 — Improve key generation

Use QRNG as a first, easy step to instantly strengthen your crypto systems

4 — Pursue crypto-agility

Be prepared to switch to alternative crypto primitives and algorithms

Protect any kind of investment you made so far by overlaying QKD to your existing infrastructure

5 — One size does not fit all

Adapt the solution to the case.

Hybrid systems can improve security.

Use QKD on mission-critical links & data center interconnect

ID Quantique

Quantum.
Trust enabled for the future

Q & A

info@idquantique.com | www.idquantique.com

ID Quantique

Founded in 2001

3 Product lines:
1. Quantum Random Number Generation
2. Quantum-Safe Security
3. Quantum Sensing

High-quality engineering

Best-in-class performance

Trust

Operational simplicity