Ekate

Ekate combines in a single platform the most **advanced cryptographic key distribution solutions** to improve the resilience of existing telecommunication networks, enabling **quantum-resistant security**.

Ekate integrates advanced cryptographic solutions, both physical, **Quantum Key Distribution** (QKD), and mathematical, **Post-Quantum Cryptography** (PQC), offering a high, adaptable level of protection against **emerging quantum-related cyber threats**.

- Ensures secure storage of keys and their distribution, following the latest standards in the field of QKD.
- Combines the intrinsic randomness provided by the Quantum Random Number Generator (**QRNG**) integrated into the system, together with PQC algorithms, to securely distribute cryptographic keys over long distances or across any network configuration.

Ekate

Ekate is a **scalable solution**, able to integrate cryptographic material from heterogeneous sources **according to the customer's needs** (QKD, PQC, classical cryptography), to guarantee **multi-layer protection**. This approach makes it possible to mitigate any as-yet-unknown vulnerabilities of individual cryptographic algorithms and to **dynamically adapt security strategies** according to the assets and specific applications of the end user.

- Enables extending quantum-resistant protection to network nodes lacking adequate infrastructure for implementing QKD technology (e.g., optical fiber or free-space links)
- Implements a **Software-Defined Networking** (SDN) framework for centralized management, operational monitoring, and path orchestration, supporting redundancy and business continuity.

Key management is unified and controlled by the organisation itself: Ekate ensures a **logical separation between key management and the application layer**.

Ekate can be **fully integrated with QTI's QKD systems** (Quell-X/XR) and is an essential component of the **QSDN solution**.

Key Features

Crypto-agile solution

Modular solution:

Module (add-on)	Description
QRNG	Generation of certified quantum entropy
PQC	Post-Quantum key distribution and digital signature
QSDN (Agent/ Controller)	Centralized management and monitoring of Quantum networks
HSM	Secure key storage on dedicated hardware via PKCS#11

- Distribution of symmetric keys over **any distance** and **independently of the communication channel** (radio, fiber, acoustic) or logical network (Internet) using a physical transmission channelLogical separation of key generation/ distribution from applications
- L2/L3 switch function
- Compatible with the latest version of the standards:
    - ETSI GS QKD 014
    - ETSI GS QKD 014 Nokia Extension
    - ETSI GS QKD 004
    - Cisco SKS SKIP
    - ETSI GS QKD 015 (QSDN)
    - ETSI GS QKD 018 (QSDN)
- Integrated PKI management
- Scalable and **easy-to-deploy**
- Supports **complex configurations** such as those based on trusted nodes (multi-peer architecture, optical switch)

Advantages

- Interoperability with all **ISO/OSI layers**
- Logical separation of key generation and propagation from the application
- Integration into **existing telecommunications infrastructure**
- Compact redundant hardware - **1U**
- User-friendly **Graphic User Interface** (GUI) and **Command Line Interface** (CLI)
- Compatible with SNMPv3

Certifications

CE marking (EU)
FIPS 140-3 (expected Q4 2026)

info@qticompany.com