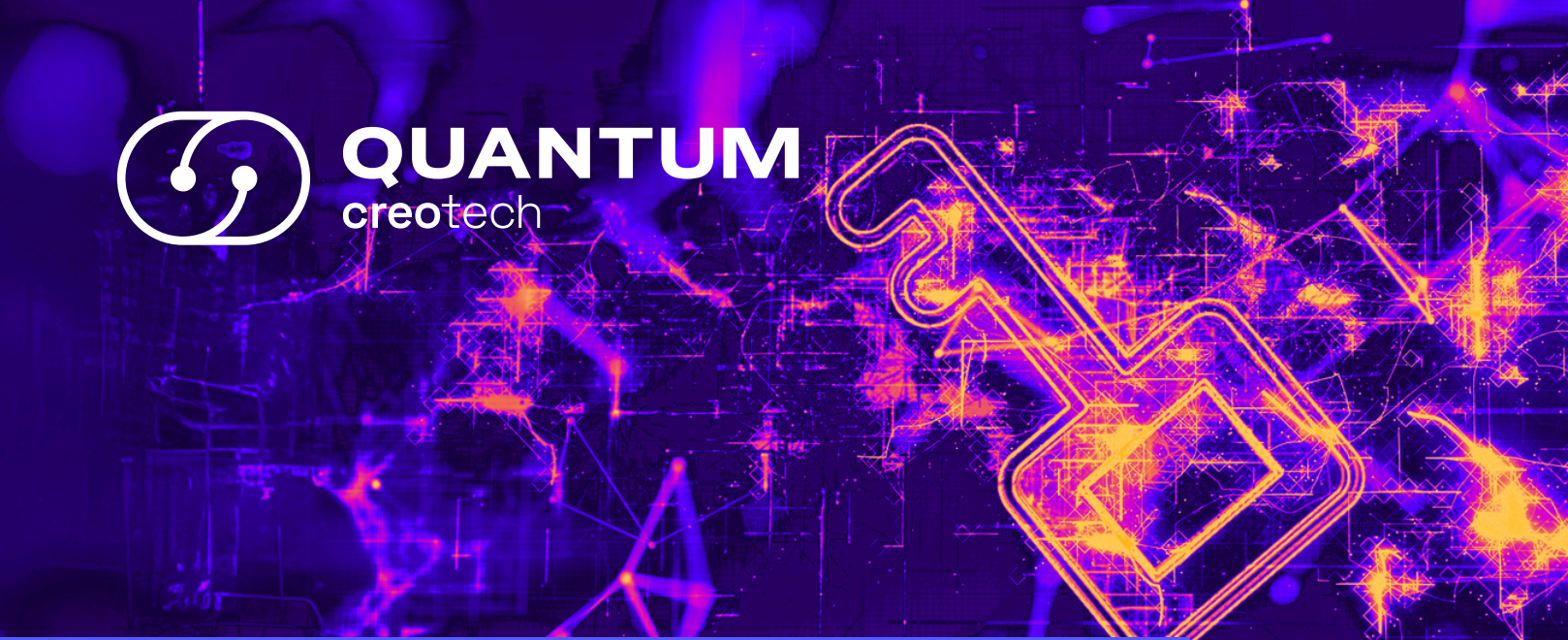


Unlock Unbreakable Security:

The Power of Quantum Key Distribution

The Ultimate Communication Security

Quantum Key Distribution (QKD) System

We use encryption algorithms every day, often without even noticing — whether exchanging information vital to organisational or national security, or simply browsing the web and sending messages. To encrypt and decrypt data, both parties need a shared key: a sequence of characters known only to them. Because these keys must be exchanged securely and frequently, we rely on a variety of algorithms to make it possible.

These algorithms are based on what is known as computational complexity (the idea that breaking the algorithm would take an impractically long time). But once quantum computers become operational, this assumption will no longer hold true. Even those considered resistant still depend on secure key exchange. This is already a concern today, given the "store now, decrypt later" strategy employed by some adversaries.

Critical Infrastructure Protection

QKD is being explored to secure communications in critical infrastructure sectors, such as energy and telecommunications.

Satellite-Based QKD

Free-space and satellite QKD experiments have demonstrated secure key exchange over long distances — including a record 12,900 km between South Africa and China, achieved with a microsatellite in low Earth orbit.

Communication Networks

For telecom clients, QKD provides encryption that prevents unauthorised access. By integrating QKD, providers can offer their customers a higher level of security, strengthening both trust and reliability. Several cities and research organisations have already deployed QKD-protected networks:

- DARPA Quantum Network (USA) – a 10-node QKD network that operated continuously for four years.
- SECOQC Network (Vienna) – interconnected multiple locations using QKD across 200 km of fiber-optic cable.
- Swiss Quantum Network (Geneva) – validated the reliability of QKD in real-world conditions.

This is where Quantum Key Distribution (QKD) comes into play. It enables the secure exchange of cryptographic keys by leveraging the fundamental laws of quantum physics, rather than depending on computational complexity.

Creotech Quantum is developing its own QKD system to provide quantum-safe communication for users most exposed to current and future cyber threats, including public authorities, defence agencies, and financial organisations. The system enables the distribution of quantum-secure cryptographic keys over existing terrestrial infrastructure, such as optical fiber networks, to connect headquarters, branch offices, and remote facilities. The system has been available since 2026.

Healthcare Data Protection

QKD has been demonstrated as a means of establishing secure communication for human genome sequences and protecting medical records.

Government and Election Security

QKD was used in the Swiss canton of Geneva to enable the secure transmission of ballot results during national elections.

Securing Financial Transactions

QKD has been used to protect bank transfers and inter-bank communications. For example, the world's first bank transfer using QKD took place in Vienna, Austria. Financial institutions also employ QKD to securely replicate sensitive data between sites.

Our QKD Solution

Exploring the Details

QKD module, 2U design

Technical Description

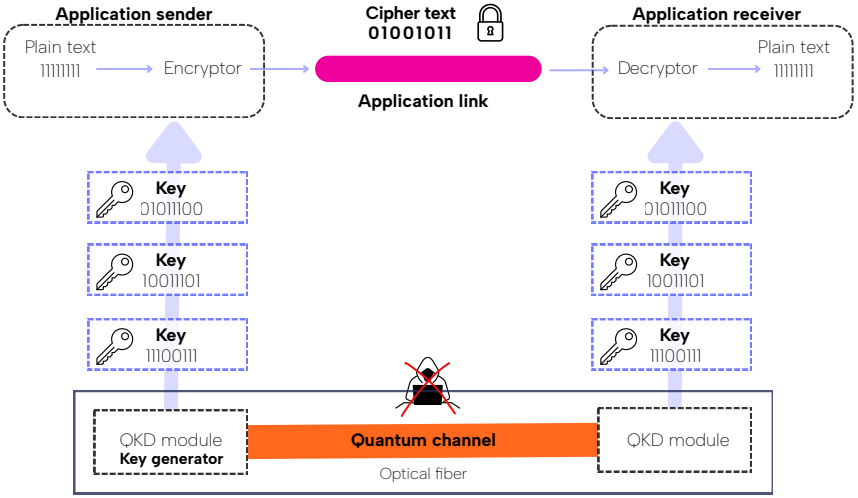
Protocol	BB84, time-bin & phase
Operating wavelength	O-band operation
Attenuation range	0 – 25 dB
Secret key rate	32 – 2 kbps
Dimensions	19" 2U rack mounted or PCIe card
Operating conditions	Temperature range of 18 to 27ºC Humidity range of 40-60%

Other features

- LDPC error correction protocol
- Security parameter: $\varepsilon < 10^{-10}$
- Built-in KMS (optionally)
- Based on ETSI ISG QKD and ITU-T Y.38xx recommendations
- Designed according to ISO 23837-1
- Supports synchronization with White Rabbit for sub-nanosecond timing precision

How It Works

The Value of Our Solution



QKD implementation

Compatibility

- Product development is carried out in close collaboration with ETSI
- Designed to be compatible with other network components, including management systems, encryptors, and more

Manufacturing Quality

- Industry-level electronics and integrated optoelectronics
- Reliable supply chain and manufacturing capabilities

Security

- Designed for Common Criteria evaluation

European QKD Ecosystem

Creotech Quantum collaborates with leading academic partners as well as research and technology organisations to develop cutting-edge QKD solutions, contributing to the broader ecosystem and strengthening the European supply and value chains for QKD. We are leading a EuroQCI project focused on the design and development of industry-grade, ground-based QKD systems.

- European design and production of key integrated photonics
- Testing QKD solutions under operational conditions within EuroQCI infrastructures
- Supply chain and manufacturing capabilities, including Common Criteria certification

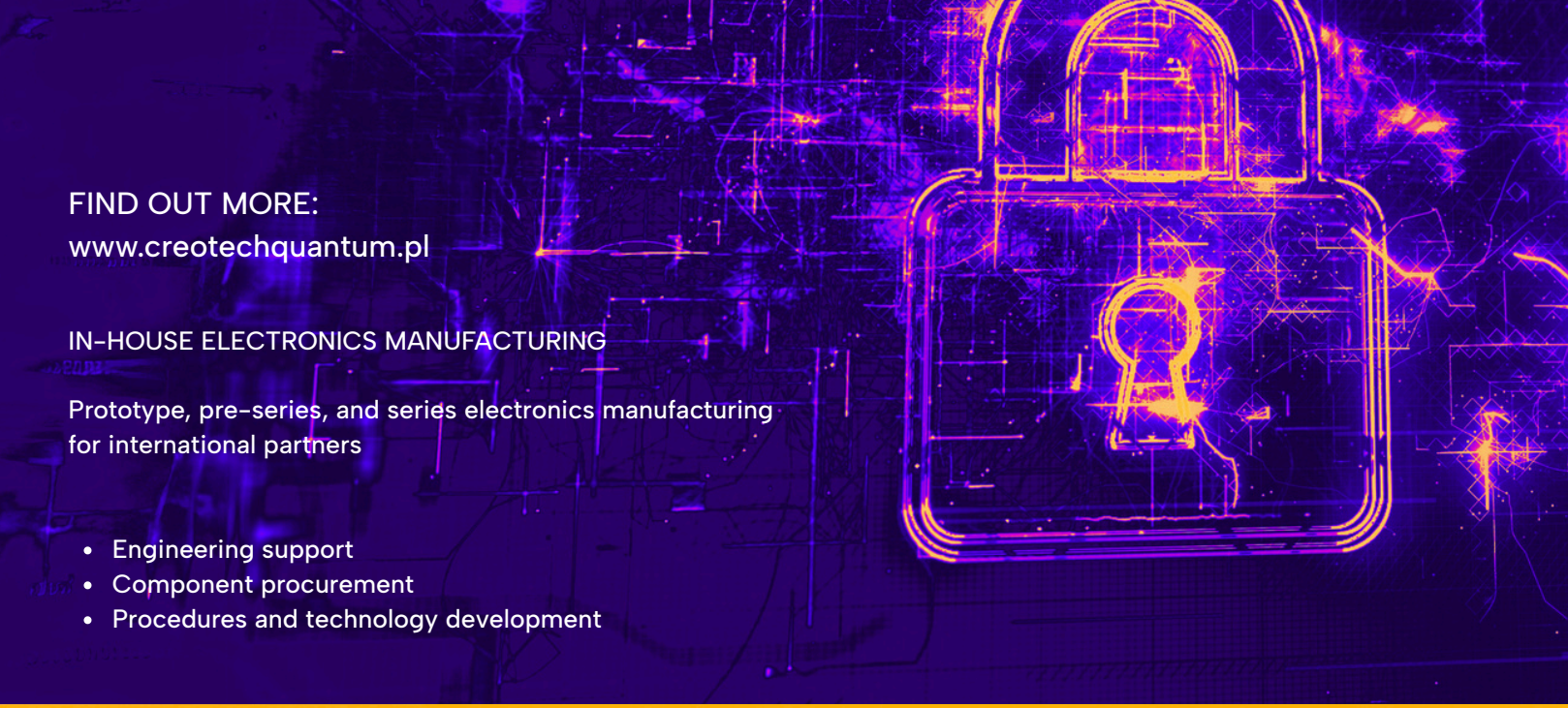
The QKD prototype system – Creotech Quantum lab

Our solution is 100% European. Both our company and our technical expertise — including electronics — are Polish.

EUROPEAN CERTIFICABLE AFFORDABLE USER-ORIENTED SECURE INTEGRATION-ABLE SCALABLE

Project consortium

Notes



FIND OUT MORE:
www.creotechquantum.pl

IN-HOUSE ELECTRONICS MANUFACTURING

Prototype, pre-series, and series electronics manufacturing for international partners

- Engineering support
- Component procurement
- Procedures and technology development

QUANTUM creotech

Creotech Quantum S.A.
sales@creotechquantum.pl

Co-funded by the European Union