



# 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.*
- *SwissQuantum 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 Instruments 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 will enable 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 will be available in 2026.**



#### ***Healthcare Data Protection***

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

#### ***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.*



#### ***Government and Election Security***

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



# Our QKD Solution

## Exploring the Details



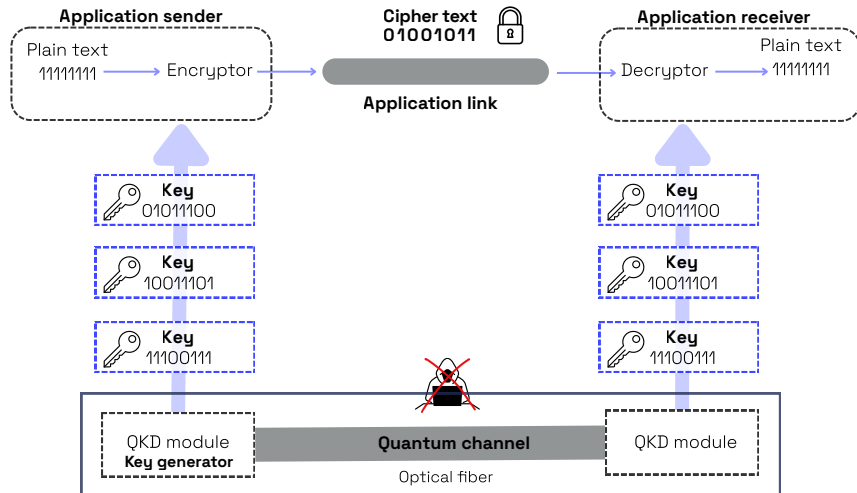
QKD module, 2U design

## Technical Description

<b>Protocol</b>	<ul style="list-style-type: none"><li>• BB84, time bin – phase</li></ul>
<b>Attenuation range</b>	<ul style="list-style-type: none"><li>• 0 – 25 dB</li></ul>
<b>Secret key rate</b>	<ul style="list-style-type: none"><li>• 43 – 3 kbps</li></ul>
<b>Dimensions</b>	<ul style="list-style-type: none"><li>• 19" 2U rack mounted or PCIe card</li></ul>
<b>Operating conditions</b>	<ul style="list-style-type: none"><li>• Temperature range of 18 to 27°C</li><li>• Humidity range of 40-60%</li></ul>
<b>Other features</b>	<ul style="list-style-type: none"><li>• 0-band operation</li><li>• LDPC error correction protocol</li><li>• Security parameter: <math>\epsilon &lt; 10^{-10}</math></li><li>• Built-in KMS (optionally)</li><li>• Based on ETSI GS QKD recommendations</li><li>• Designed according to ISO 23837-1</li><li>• Supports synchronization with White Rabbit for sub-nanosecond timing precision</li></ul>

# 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 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

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



*The QKD prototype system – Creotech lab*



E C A U S I S  
U E F S E N C  
R R F E C T A  
O T O R U E L  
P I R - R G A  
E F D O E R B  
A I A R A L E  
N C B I T E  
A L E I  
B E N O  
L E T N  
E E - A  
B L E



creotech



 **Fraunhofer**  
HHI

*Project consortium*



FIND OUT MORE  
[www.creotech.pl](http://www.creotech.pl)



## IN-HOUSE ELECTRONICS MANUFACTURING

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

- Engineering support
- Component procurement
- Procedures and technology development



Creotech Instruments S.A.  
[sales@creotech.pl](mailto:sales@creotech.pl)



Co-funded by  
the European Union