



QUANTUM OPTICS
JENA

AI- & Quantum-Safe Communications

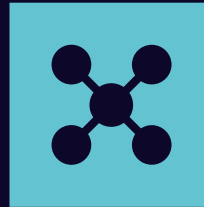
ELVIS Enterprise Quantum Key Distribution System

Secure

Reliable

Scalable





→ Why bother?

When confidential data is communicated, a leak can be devastating and costly: regulatory fines for the institution, personal liability for executives, lasting reputational damage, and lost customers and revenue. While symmetric AES encryption is deemed long-term secure, it requires the same key at both endpoints. Today's computational methods for distributing those keys are not long-term secure: they are threatened by AI-assisted attacks and by upcoming quantum computers. Even new post-quantum cryptography (PQC) methods are not immune – they can be broken through implementation weaknesses today, or by attacks

against their mathematical hardness in the future. For data that must stay secure for years, the attacks are already running: attackers copy the key exchange and encrypted communication today and store them. Later, once they can break the key-exchange method, they decrypt and misuse what was revealed. These are „harvest now, decrypt later“ attacks. AI-assisted attacks on cryptographic implementations are already happening, and quantum computers, powerful enough to break today's classical key exchange, are expected very soon (2030–2033). The threat is here, today.

→ Why QKD?

Quantum key distribution (QKD) uses the quantum-physical properties of photons to distribute keys. This distribution cannot be manipulated or eavesdropped without immediate detection. Its security rests on physical laws, not on a computational algorithm that could be broken. As NASA puts it, breaking a quantum protocol would require violating fundamental physical principles – so that even an adversary with immense computational power, quantum or classical, cannot break it.

QKD guarantees what computational key exchange cannot: keeping your communication secure forever.

→ Why Quantum Optics Jena?

Quantum Optics Jena's ELVIS Enterprise QKD systems are based on entangled photons, where security depends only on the receivers. With this source-independent QKD protocol, an attacker gains nothing by compromising the source. Built on the fundamental laws of physics from the ground up: the system generates entangled photons in a superposition state, distributes them over fiber-optic infrastructure with no restrictive assumptions on the quantum channel, and completes the process with the measurement of the individual photons.

When it comes to security, choose true quantum. ELVIS Enterprise is highly reliable for continuous operation in data centers, backed by responsive service, with redundant configurations for uninterrupted operation. It is cost efficient, integrate easily with existing infrastructure, and offer comprehensive configuration and monitoring tools for the operator. From two-node links to large multi-node networks over long distances, our systems support all kinds of infrastructure – and grow with your requirements. We deliver on our promise: **Secure. Reliable. Scalable.**



How it works

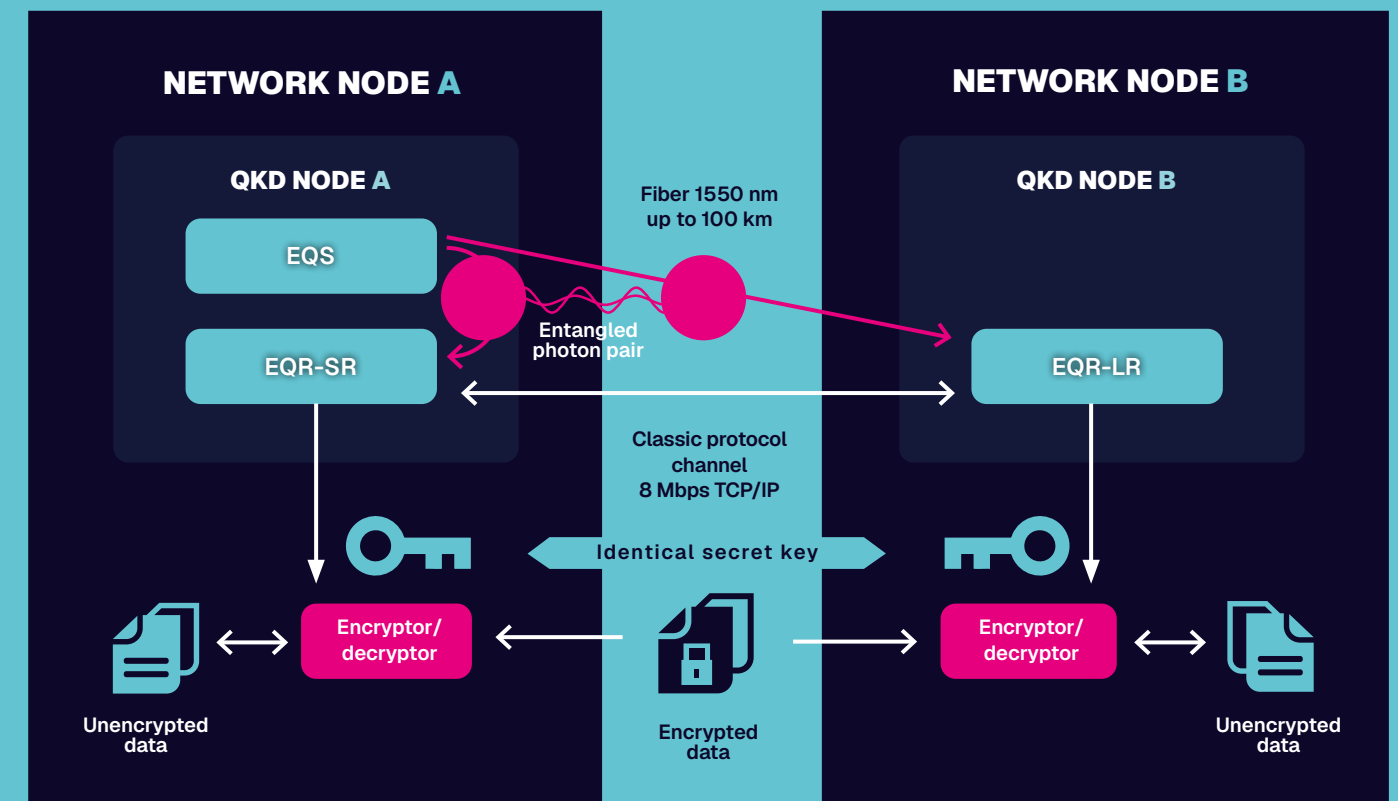
The ELVIS Enterprise QKD system consists of three devices to supply secure keys to two communication endpoints – or network nodes.

- + The **ELVIS Quantum Source EQS** generates pairs of entangled photons which are sent via optical fiber to two ELVIS Quantum Receivers.
- + The **ELVIS Short-Range Quantum Receiver EQR-SR** is best located next to the quantum source but could be located up to 4 km away.
- + The **ELVIS Long-Range Quantum Receiver EQR-LR** is located at the remote network node B, up to approximately 100 km away from the EQR-SR.

The ELVIS Enterprise system requires just a single standard 1550 nm telecom fiber from the quantum source to each receiver. It also uses a standard, non-confidential, 8 Mbps (or lower) TCP/IP connection between the two receivers to run the quantum protocol.

The two ELVIS Quantum Receivers generate secret keys that they supply to their node's data encryptor.

The encryptors are not part of the ELVIS Enterprise system, they are chosen by the customer. The ELVIS Quantum Receivers support standard key interface protocols, making them compatible with market leading key management systems (KMS), hardware security modules (HSM), key combiners, encryptors/decryptors and even end-to-end-encrypting software applications.



→ The properties of quantum physics:

- + Both nodes receive **highly random** and **identical symmetric** keys.
- + **Any attempt of an attacker** to manipulate the Quantum Source or the transmitted photons, or to eavesdrop on the photons, **will be immediately detected**. This detection will be recorded and reported, and the suspect photons will not be used to generate keys.
- + Unlike most other technologies, including PQC as well as non-entanglement-based QKD, no quantum random number generator (QRNG) is required. The **ELVIS Enterprise** system is a distributed QRNG, delivering identical random keys to both nodes.

→ Operational Readiness

QKD is the only scalable key distribution technology that offers complete immunity to „harvest now, decrypt later“ attacks – keeping your data secure today, tomorrow, and forever. And it is no longer experimental: QKD is already deployed and operational in nationwide and international networks.

10.000+ km: China's CN-QCN

An operational QKD network already securing banks an critical infrastructure across the country



Chinese example of continental QKD initiatives

EU-wide: Europe's EuroQCI

The EU is building the same quantum secure capability across all member states



European example of continental QKD initiatives

The ELVIS Enterprise QKD system has been designed and tested for 24/7 operation in data centers. Its compact devices use semiconductor-based single-photon

detectors, which require no cryogenics or maintenance, making the system truly data-center ready.

→ Evaluated Security

The core of the ELVIS Enterprise technology – entanglement-based QKD with the BBM92 protocol – and its security assumptions have been studied continuously for over three decades and are mature and well understood. The system builds on the research that won the 2022 Nobel Prize in Physics.

In an evaluation under ISO/IEC 23837-2 “Information security – security requirements, test and evaluation methods for quantum key distribution”, based on a wide range of attack attempts, TÜV Informationstechnik

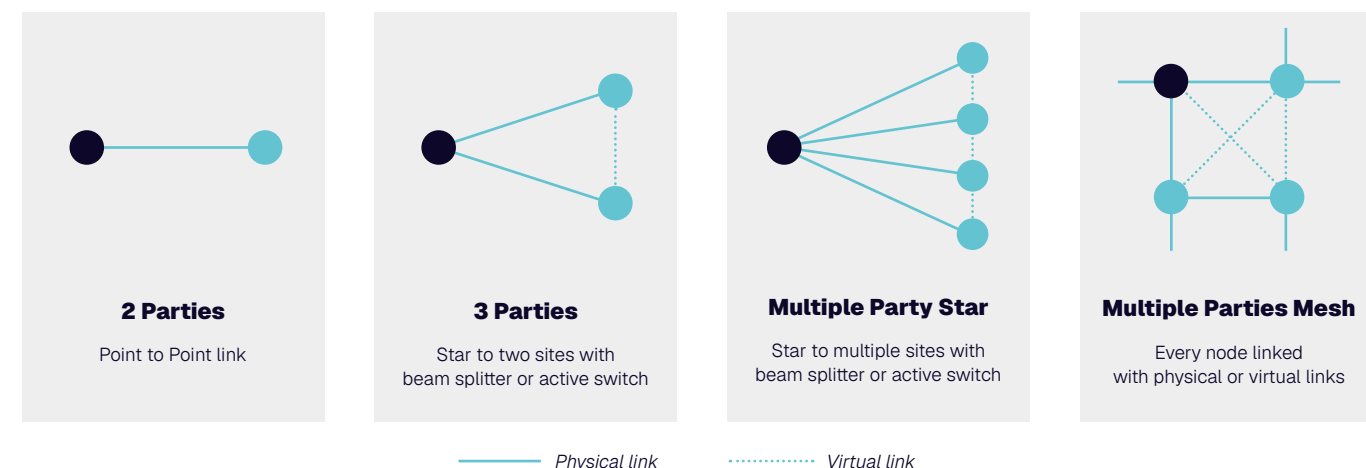
(TÜVIT) confirmed that the ELVIS QKD system withstood targeted attacks on hardware side channels, with no serious weaknesses found.

Entanglement-based QKD depends on the photons being genuinely entangled. The ELVIS Quantum Source has been validated by INRiM, the National Metrology Institute of Italy, to generate high-quality entangled photon pairs.

→ Multi-Link Switching: Unlimited Scalability with Cost Efficiency

For non-entanglement based QKD, the usual approach for building larger QKD networks with multiple nodes is to use separate QKD systems for each connection between nodes. While this works, it can be costly. An entanglement based QKD system overcomes this challenge. The ELVIS Enterprise QKD system allows connecting one ELVIS Quantum Receiver with multiple other nodes via a beam splitter or an active optical switch. This multi-link switching allows the user to:

- + Reduce hardware costs as less receivers are required, or
- + Use two or more redundant fibers for uninterrupted operation even if one fiber is damaged.



Naturally, the total key rate is shared among all connected receivers. The key advantage of ELVIS Enterprise: sharing comes at virtually no cost – aside from a slight signal loss from the beam splitter or switch. Because ELVIS Enterprise switches between nodes almost instantly, key rates stay consistently high.

This enables scaling to metro, national, and international QKD networks.

Quantum Optics Jena also supports its customers with tools for network planning and analysis.

Depending on the key rate required, a single ELVIS fiber connection can reach distances of up to 100 km. Longer distances can be covered using one or more trusted nodes in between – each of which must reside in the operator's secured environment – and can be either a full ELVIS Enterprise system or a receiver equipped with a beam splitter or optical switch. A KMS can relay keys across these trusted nodes, creating virtual QKD connections spanning multiple intermediate nodes.



Quantum Optics Jena network planning tool depicting a complex multi-node infrastructure

Integration and Interfaces

The ELVIS Quantum Source EQS provides:

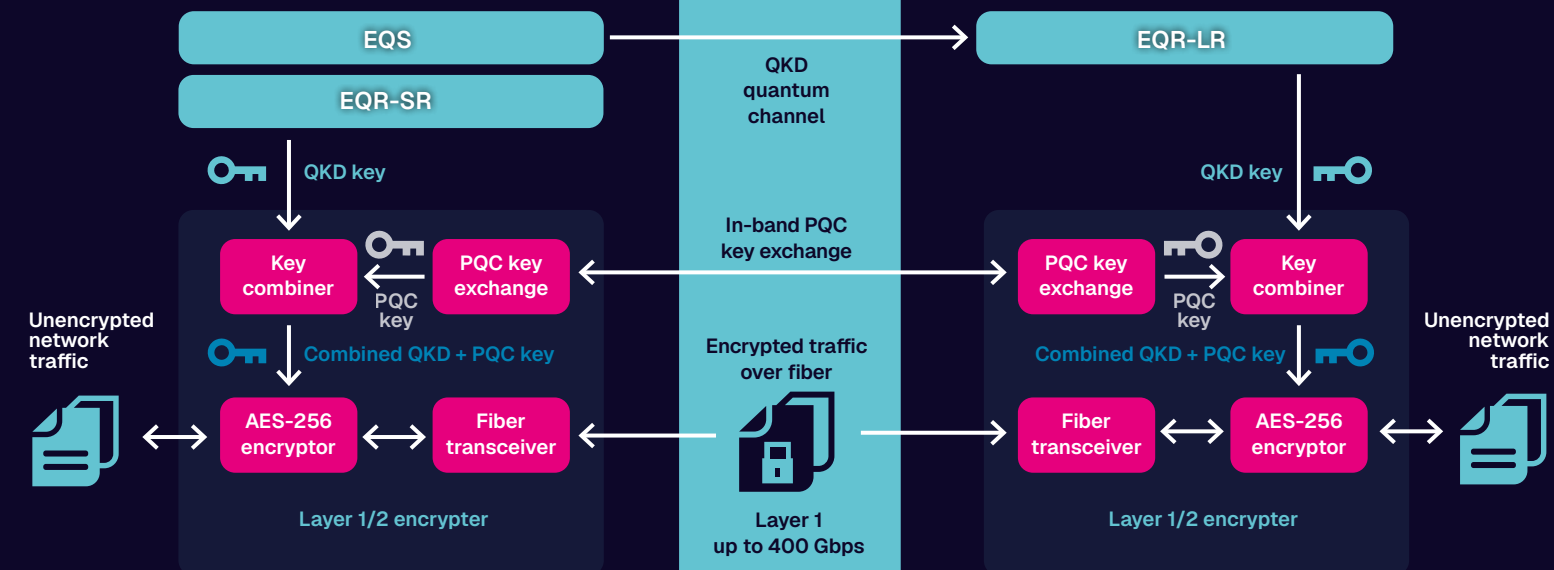
- + Two optical fiber connectors, one to each receiver.
- + A copper Ethernet connector for TCP/IP for the monitoring interface.

The ELVIS Quantum Receivers EQR-SR and EQR-LR each provide:

- + An optical fiber connector. The long-distance connection to EQR-LR uses a standard 1550 nm telecom fiber that must not be used by any other communication (dark fiber).
- + Four copper Ethernet connectors for TCP/IP, configurable for:
 - + The > 8 Mbps classical protocol channel between the two receivers. This communication has no confidentiality requirements.
 - + The key interface(s) to the key consumers, supporting multiple key pools with configurable properties and ETSI GS QKD 014 or Cisco SKS v4 SKIP.
 - + The configuration interface.
 - + The monitoring interface, supporting SNMP, Syslog, and Prometheus. It provides real-time information as well as comprehensive log data, including link status, key rate, and eavesdropping warning.

ELVIS Enterprise systems are easy to install, configure and work out of the box with a wide range of HMS, KMS, key combiners, and encryptors from ADVA, Ciena, Cisco, Futurex, Nokia, Rohde & Schwarz, secunet, Utimaco, WireGuard, and others. If the device is ETSI 014 or SKIP compliant, it will be interoperable with ELVIS Enterprise. With an appropriate interface layer,

ELVIS Enterprise can also supply quantum keys to applications and TLS, including OpenSSL. As an integration example, the following illustration shows how easily quantum keys from an ELVIS Enterprise system can increase the security of an existing PQC-based layer 1/2:



Use cases examples

→ Legal compliance for Banking & Finance

European regulations such as GDPR, NIS2, and DORA require security measures appropriate to the risk, with encryption a central example. For financial data, the relevant risk is its confidentiality lifetime – often 7 to 15+ years. Against the combined threats of AI, upcoming quantum computers, and “harvest now, decrypt later” attacks, computational encryption is increasingly hard to defend as „risk-appropriate“ over such long confidentiality periods.

Quantum-safe encryption is the state-of-the-art response for high-value links between sites, to data centers and for centralized backup. Usage of QKD and PQC approaches, e.g. combining PQC and QKD keys using a standardized key derivation function, keeps the link secure even if one method is later broken (defense in depth). The integration example on the previous page fits this use case perfectly.

→ Quantum-Secure Keys as a Service (QSKaaS) by Telecommunications Providers

For small and mid-sized enterprises, sharing QKD and fiber-optic infrastructure through a managed service delivers an excellent – and economically highly attractive – level of security for data that must be protected over the long term. Instead of high upfront investments (CAPEX) in their own hardware, customers pay only pre-

dictable, usage-based operating costs (OPEX) – gaining access to the same security class that otherwise only large institutions can afford. QSKaaS can be a profitable new business opportunity for communication service providers and eminently affordable for their enterprise customers.

→ Long-term confidentiality for Government & Defense

Classified government and defense data carries the longest secrecy requirements of any sector – often 25 to 75+ years for intelligence, diplomatic, and strategy-related records. Because command centers, ministries, and national data centers are fixed sites joined by fiber, they are a natural fit for QKD. QKD also supports a sovereign security posture, with key material generated and kept on infrastructure the government physically controls.

As with the banking use case, the state-of-the-art implementation is a hybrid approach – combining QKD and PQC keys through a standardized key-derivation function. This keeps QKD additive to the PQC that national security agencies recommend as a certifiable baseline. For wide-area reach, keys are relayed across trusted nodes within the government's secured environment, scaling protection to metro, national, and allied networks.

Technical Specification

ELVIS Quantum Source EQS

Long-range output center wavelength (to EQR-LR)	1550 nm
Short-range output center wavelength (to EQR-SR)	810 nm
Fiber connectors	FC/PC (easy patching to every other fiber standard possible)
Pair Generation Rate	> 25 MHz
Fidelity / Source Heralding / Spectral bandwidth	> 90 % / > 15 % / 2 nm
Dimensions (L x W x H) / Weight	530 x 485 x 88 mm, 2 U in a 19" server rack / 7.5 kg
Power Consumption	Max. 150 W redundant (nominal 60 W)
Operating temperature	15–30 °C
Monitoring interface	Ethernet (RJ45)

ELVIS Quantum Receiver EQR-LR / EQR-SR

	EQR-LR	EQR-SR
Input wavelength	1550 nm	810 nm
Recommended fiber type / Fiber connectors	Standard 1550 nm / FC/PC	780 nm fiber / FC/PC
Used detector technology	InGaAs SPADs	Si SPADs
Self-calibration	Yes, with polarization compensation	
Typical key rates	> 1500 bps @ 0 dB loss	
	> 500 bps @ 10 dB loss	
	> 10 bps @ 20 dB loss	
Dimensions (L x W x H) / Weight	530 x 485 x 88 mm, 2 U in a 19" server rack / 12 kg	
Power Consumption	Max. 150 W redundant (nominal 70 W)	
Operating temperature	15–35 °C	
Quantum protocol interface	Ethernet (RJ45); BBM92-protocol, protocol data payload between receivers: < 8 Mbps (typically < 3 Mbps at 10 dB loss)	
Control interface	Ethernet (RJ45), SFP+	
Configuration interface	Ethernet (RJ45); SFP+, web server GUI	
Monitoring interface	Ethernet (RJ45); SFP+, SNMP, Syslog, Prometheus	
Key interface	Ethernet (RJ45); SFP+, ETSI GS QKD 014, Cisco SKS v4 SKIP	
Maintenance requirements	None	
Validation & Certifications	CE, ISO 23837-2 by TÜVIT, validation of entangled photon-pair source by INRiM	



QUANTUM OPTICS
JENA

Quantum Optics Jena GmbH
Am Zementwerk 8 | 07745 Jena, Germany
info@qo-jena.com | +49 3641 207470



www.qo-jena.com