IDQ an IonQ company

IONQ

Clavis XG QKD Portfolio

Out-of-band quantum key distribution for enterprise networks —
prevent "harvest now, decrypt later" and protect long-term confidentiality

The long-term security of digital communications can no longer rely solely on conventional asymmetric key exchange mechanisms. Increasing computational power, the risk of undisclosed vulnerabilities, and the anticipated emergence of cryptographically relevant quantum computers undermine the assumption that encrypted data will remain confidential over time.

A critical risk is the ability to harvest encrypted traffic today and decrypt it later when more powerful attack capabilities become available. For governments, financial institutions, and operators of critical infrastructure – where data confidentiality must be preserved for five to ten years or longer – this creates a tangible exposure that cannot be mitigated retroactively.

Quantum Key Distribution (QKD) addresses this challenge by enabling the exchange of cryptographic keys with security rooted in the laws of physics rather than computational assumptions. Any attempt to intercept the key material introduces detectable disturbances, allowing communicating parties to identify compromise in real time.

Clavis XG is purpose-built for seamless deployment in operational networks. It delivers robust, high-rate key distribution over long distances and integrates smoothly with enterprise and carrier environments. Beyond quantum-safe key generation, it incorporates post-quantum cryptography (PQC) to provide a comprehensive, hybrid-secure architecture ensuring forward protection against both current cyber threats and the emerging risks of large-scale quantum computing.

Key Markets

- **Telecom & Data Center Service Providers**
- **Banking & Finance**
- **Government & Defence**
- **Critical Infrastructure**
- **Healthcare Organizations**
- **IP-rich Enterprises**

Key Applications

- **Data center interconnections**
- **Long distance or high throughput backbone optical networks**
- **Hybridized QKD/PQC by design**
- **Key distribution across a complex network**
- **Crypto keys as-a-service**
- **Enterprise-grade Quantum Key Distribution**

IDQ an IonQ company

IONQ

Clavis XG QKD Portfolio

Robust and standard design to be integrated in any data center

The Clavis XG is IDQ's 4th generation of QKD systems, based on 20 years of experience in the development and commercialization of quantum-based products. It supports any kind of network topologies, such as point-to-point, relay, ring, and star networks. Clavis XG systems are designed for uninterrupted and long-term operation by providing high availability services.

System description

Clavis XG systems can be deployed in any network configuration that requires high key throughput or includes long distance links. It is well suited for point-to-point, relay for extended distances, ring or star topologies. At each QKD network node, an embedded Key Management System (KMS) software arbitrates the key distribution between QKD and key consumers as well as performing add/drop or forward functions depending on the recipient's location.

Clavis XG systems operate at standard telecommunication wavelengths (in the O and/or C bands) and can be easily retrofitted onto existing fiber optic network. **Clavis XG meets all requirements for a simple and easy integration in any data center**. Its compact 19'' rackmount 1U size offers the highest integration of QKD technology available in the market today. All the necessary key management, monitoring and administration functions are embedded in the chassis to perform quantum key generation and distribution over a quantum channel with a transmitter (Alice) on one end and a receiver (Bob) on the other end. High availably features like redundant power supplies, hot swap battery and fans module are supported.

Quantum communication is performed over standard optical fiber, enabling easy installation and maintenance while minimizing total cost of ownership.

All optical channels are compatible with the ITU recommendation for Dense-Wavelength-Division-Multiplexing (DWDM). To maximize the distance between nodes, operation of the quantum channel over a dark fiber is recommended. However, channel multiplexing over a single core can be performed with quantum channel around 1310 nm (O-band) whenever fiber resources are scarce.

In practice, QKD is often combined with conventional key distribution techniques, such as RSA or ECC, to generate a dual key agreement. The resulting key is always at least as secure as the strongest of the two original keys and provides proven quantum-safe security. Importantly, the dual key agreement retains the existing certifications of the conventional system.

How does Clavis XG scale through Clarion KX integrated management and monitoring

Entreprise Q-KMS platform

Clarion KX Platform

- Key relaying
- Interoperability with key consumers
- Hybrid key agreement leveraging QKD, ECC and/or PQC (ML-KEM)
- Crypto agility
- High availability and scalability
- Central management and monitoring*

Clarion KX is embedded in our QKD product line and network appliance. It is provided as a yearly licence.

**Physical or virtual server not provided*

Clavis XG Product Line

Enterprise grade plug and play BB84 QKD for any fiber deployment up to 150 km

Solteris Network Appliance

Enhanced enterprise QKD deployment capabilities & performance to go beyond the QKD network

The Clavis XG QKD System

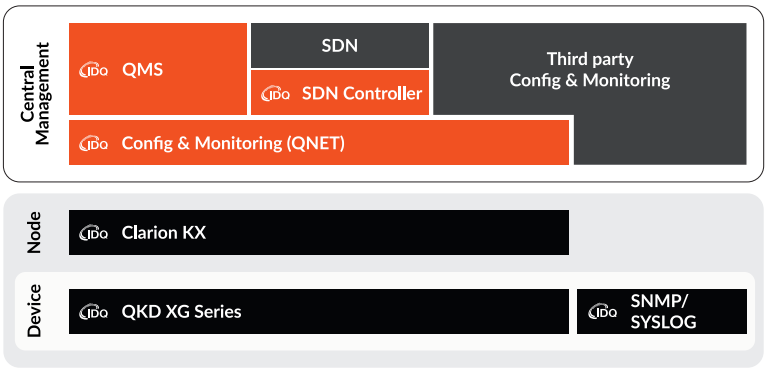
Interoperability is key

The Clavis XG portfolio is the next generation commercial QKD system that can interface with link encryptors from major vendors. It answers high availability requirements thanks to dual redundant power supply, hot swap battery and fans module, key buffering, and alerting and monitoring functions.

Key management and monitoring

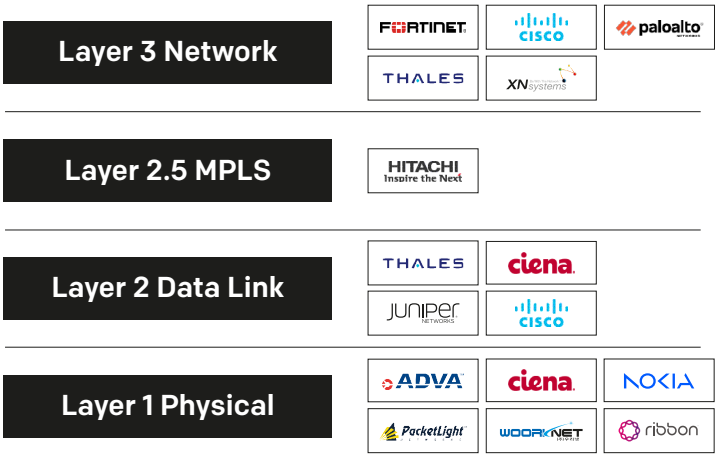
Clavis XG systems integrate enhanced trusted security components, like tamper detection, a secure memory module, as well as IDQ's QRNG chips which provide proven randomness for all related crypto functions. These features guarantee the highest security standards throughout the whole key management process, from key generation to key delivery, and including key storage.

The Clavis XG portfolio is compatible with IDQ's QKD management and monitoring framework. It consists of an Extensive Network and Key Management software suite: Clarion KX. This framework integrates current Software-Defined Network (SDN) QKD ETSI standards as well as IDQ's Quantum Management System (QNET QMS) to facilitate all large QKD deployments. It ensures a seamless integration in existing infrastructure.



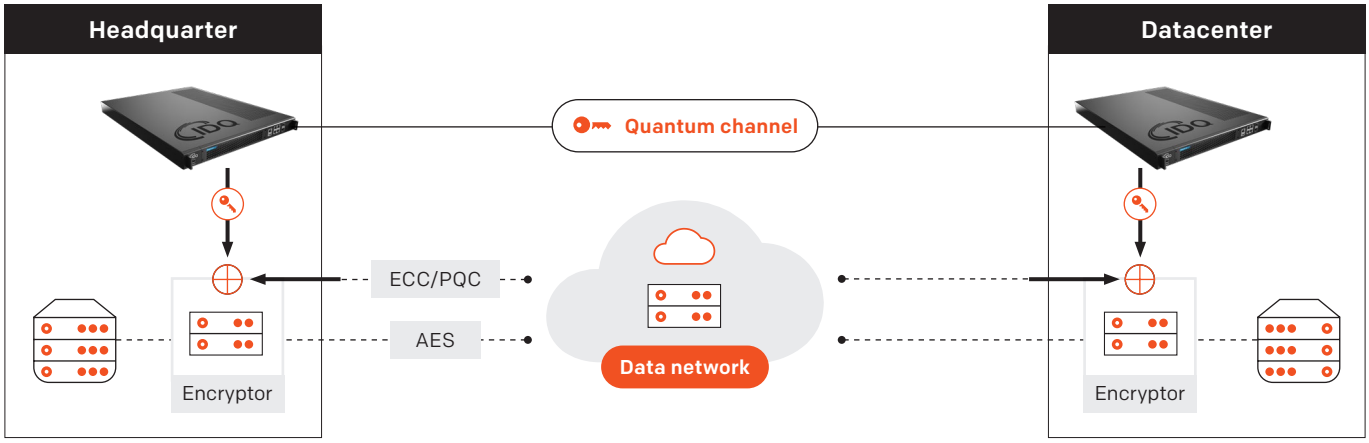
Interoperability with third-party security systems

The Clavis XG portfolio can interface and communicate with major encryptor vendors. It supports standard and proprietary interfaces. ID Quantique is actively taking part in the standardization processes, particularly at ITU and ETSI, to boost interoperability of QKD and other security systems. Leading Optical Transport Network (OTN) vendors offer this QKD-ready interface in their encryption's appliances (OSI Layer 1/2/3 and MPLS).

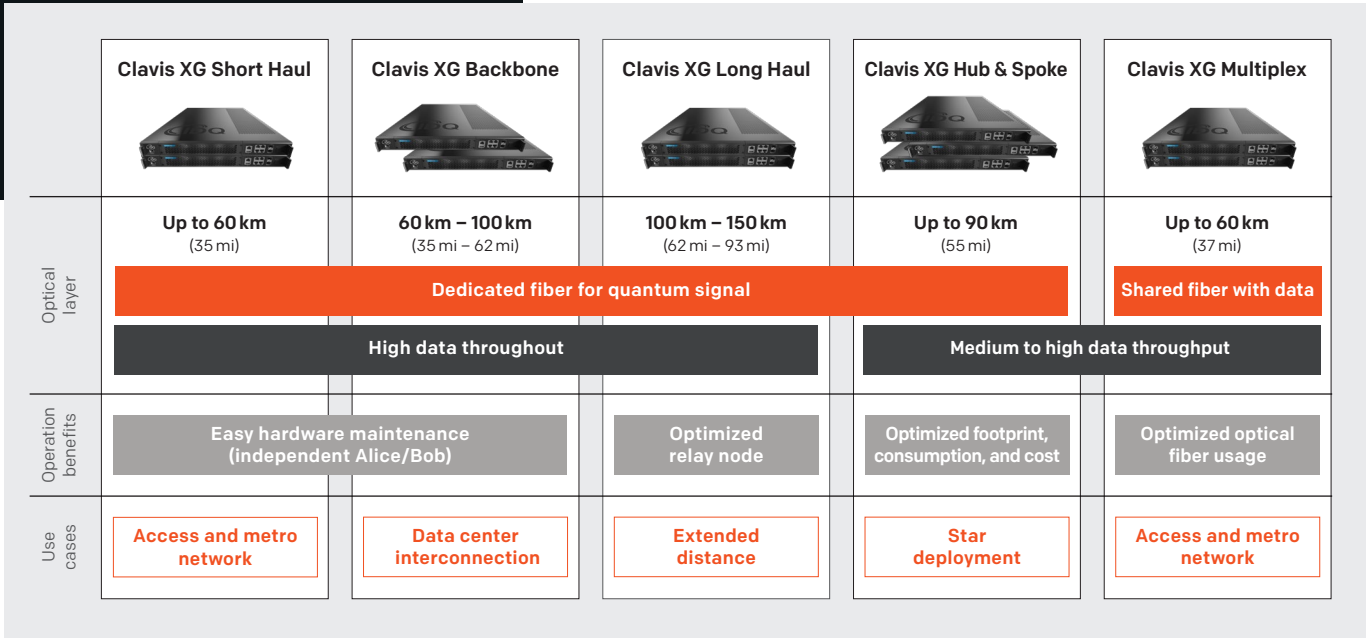


Integration with other suppliers available upon request

"Out-of-band" offering high availability & security



Product portfolio & use cases



The Clavis XG portfolio enables secure long-distance **quantum-safe communications** for critical infrastructure operators and government agencies requiring unhackable encryption over fiber networks, with models ranging from **short-haul** (60 km) to **long-haul** (150 km) dark fiber deployments for maximum data protection. Organizations can deploy these systems to protect sensitive **telecommunications, enterprise networks, financial institutions, and government** communications against both current cyber threats and future quantum computing attacks, leveraging IDQ's optimized architecture for either **simple point-to-point connections** (Backbone, Hub & Spoke) or **complex multi-site networks** (Multiplex).

The Hub & Spoke and Multiplex variants specifically address enterprise and telecom provider needs for scalable, quantum-secure network infrastructure, enabling secure key distribution across distributed sites while minimizing hardware maintenance requirements and infrastructure complexity.

Main advantages

- \+ Out-of-band key distribution and instantaneous intrusion detection
- \+ True Quantum random key generation
- \+ Single core for metropolitan area, through multiplexing of all channels on the same fiber
- \+ Interoperability with major Ethernet and OTN encryption vendors
- \+ Easy installation and remote support
- \+ Resilient to mechanical vibrations and thermal changes in fiber optics (polarization-independent scheme)
- \+ Centrally monitored solution available with QNET software
- \+ Non-intrusive to data communication channels
- \+ Small form factor: 1U compact chassis (Alice or Bob)
- \+ Trusted Security (Tamper Detection, Secure Memory Module, IDQ20MC1 QRNG chip)

IDQ an IonQ company

ID QUANTIQUE
www.idquantique.com | info@idquantique.com

IONQ

IonQ
www.ionq.com | info@ionq.com