



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



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



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 availability 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

Enterprise 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.



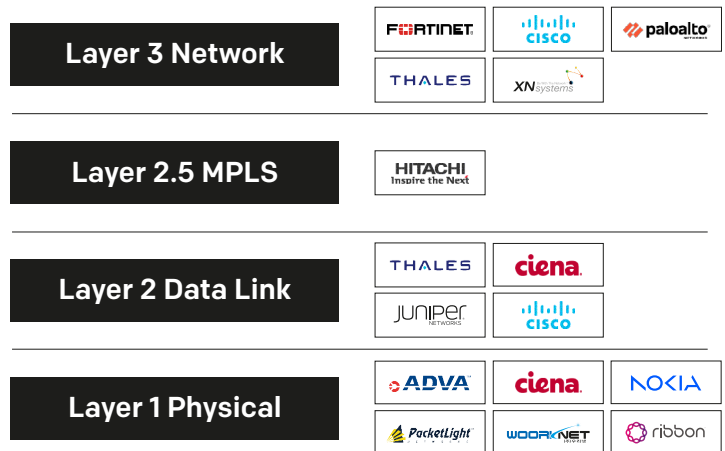
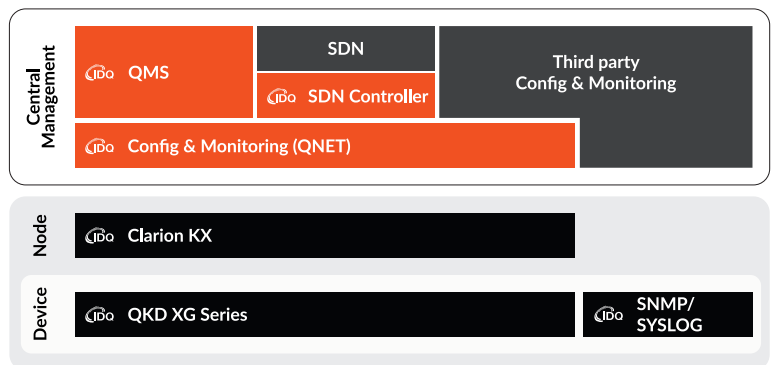
Interoperability with third-party security systems

The Clavis XG portfolio can interface and communicate with major encryptor vendors. 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).

Key management and monitoring

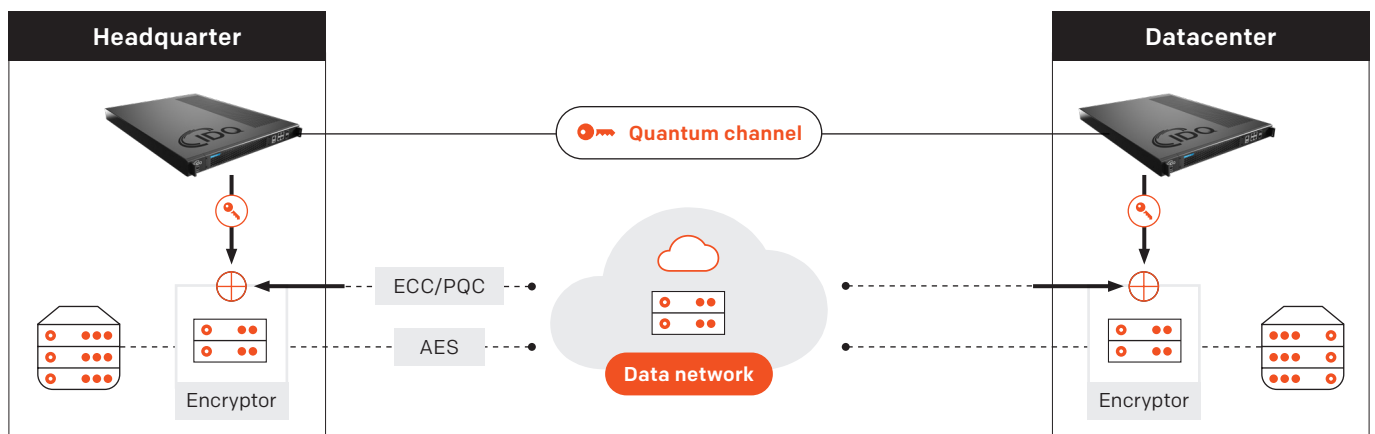
Clavis XG systems integrate enhanced trusted security components, like tamper detection, a secure memory module, as well as IDQ's QRNG chips which provide proven randomness for all related crypto functions. These features guarantee the highest security standards throughout the whole key management process,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



Integration with other suppliers available upon request

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



Product portfolio & use cases

	Clavis XG Short Haul	Clavis XG Backbone	Clavis XG Long Haul	Clavis XG Hub & Spoke	Clavis XG Multiplex
					
Optical layer	Up to 60 km (35 mi)	60 km – 100 km (35 mi – 62 mi)	100 km – 150 km (62 mi – 93 mi)	Up to 90 km (55 mi)	Up to 60 km (37 mi)
	Dedicated fiber for quantum signal				Shared fiber with data
	High data throughput			Medium to high data throughput	
Operation benefits	Easy hardware maintenance (independent Alice/Bob)		Optimized relay node	Optimized footprint, consumption, and cost	Optimized optical fiber usage
Use cases	Access and metro network	Data center interconnection	Extended distance	Star deployment	Access and metro network

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)



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



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

Disclaimer: The information and specification set forth in this document are subject to change at any time by ID Quantique without prior notice.
Copyright © 2026 ID Quantique SA - All rights reserved - G.192.0121-PB-3.0 - Specifications as of June 2026.

Clavis XG Multiplex



The Clavis XG Multiplex

Why the O-band matters for your network

While the classical C-band (1530–1565 nm) is the industry standard for high-speed data, it is often too “noisy” for delicate quantum signals. By utilizing the O-band (1260–1360 nm), the XG Series ensures your quantum keys travel on a separate wavelength, eliminating interference and allowing for seamless integration into existing fiber infrastructure.



Enterprise grade co-propagating QKD

The Clavis XG Multiplex inherits the proven DNA of the Clavis XG series, delivering the market’s smallest QKD form factor without compromising on power. Engineered for seamless “plug-and-play” deployment, it features an integrated Q-KMS (Clarion KX) for sophisticated key management and optimized power consumption. Built for mission-critical reliability, the system includes redundant power supplies and a 1U chassis designed to fit effortlessly into any high-density data center.

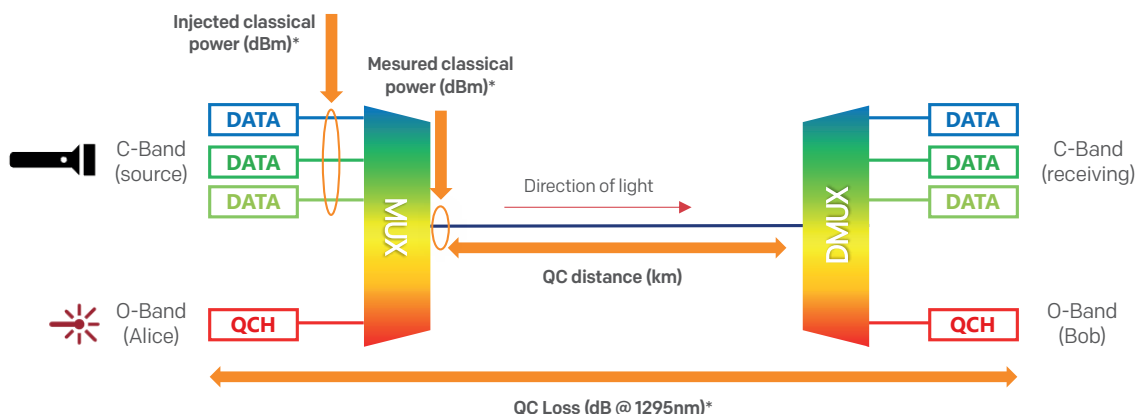
Explore the Ecosystem: For detailed specifications on the Clarion KX management platform and the full Clavis XG portfolio, visit idquantique.com.

Optimized for Coexistence: The O-Band Advantage

The Clavis XG Multiplex utilizes the 1295 nm O-band as the optimal wavelength for Quantum Signal transmission. By operating in “copropagating mode” alongside classical C-band data, the system significantly reduces Stokes-Raman Scattering and provides industry-leading protection against cross-talk.

- **Certified Coexistence:** Field-proven for simultaneous deployment with high-speed C-band data on the same fiber.
- **Enhanced Monitoring:** Supports an Optical Supervisory Channel (OSC) in the S-band (recommended power of -5 dBm, at 1511nm) for robust link management without impacting quantum performance.

Environment specifications - optical setup



*Datasheet classical power (dBm) = Measured classical power (dBm) = Injected classical power (dBm) – MUX Loss (dB)

**Typical loss @ 1295nm = 0.35dB/km

Performance specifications

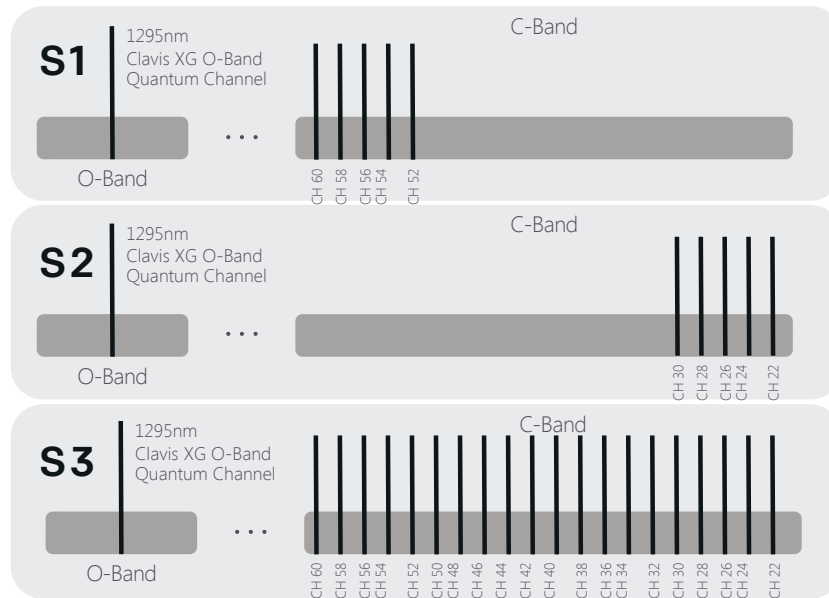
QC length (km)	QC loss (dB)	Min SKR (AES-256/hour)	C-Band Maximum classical power* (dBm)		
			S1 low channels	S3 distributed ch.	S2 high channels
25 (16 mi)	12	14 000	16	17+	17+
25 (16 mi)	21	14 000	13	17+	17+
50 (31 mi)	21	7 000	10	16	17+
50 (31 mi)	24	7 000	8	14	17
60 (37 mi)	25	3 500**	10	16	17

*After the MUX

**Typical SKR

17+: maximum certified power, tested up to 21dBm

Environment specifications - wavelengths distribution



Main advantages

- + Non-intrusive Coexistence with Data:** Operates in the 1295 nm range (O-band) to stay physically separated from classical C-band data traffic, effectively reducing Raman scattering noise and interference.
- + Provably Secure & Real-time Detection:** Provides information-theoretic security with instantaneous detection of any physical intrusion on the fiber link, ensuring keys are never compromised.
- + Enterprise grade QKD O-Band System:** Leverages 25 years at IDQ & IONQ experience designing and manufacturing QKD for the most demanding live operational customer use cases.
- + Intrinsically Stable Optical Engine:** Features a polarization-independent scheme that is highly resilient to the mechanical vibrations and thermal changes common in busy city fiber ducts.
- + Seamless Multi-Vendor Interoperability:** Fully compatible with major Ethernet and OTN encryptors and centrally manageable via QNET software for easy integration into existing SOCs.

Clavis XG QKD Portfolio specifications

Specifications	Clavis XG Short Haul (18 dB)	Clavis XG Backbone (24 dB)	Clavis XG Long Haul (30 dB)	Clavis Multiplex (24 dB) ⁽¹⁾	Clavis XG Hub&Spoke (23 dB) ⁽²⁾
Quantum Channel	C-band (1551.72 nm)			O-band (1295.56 nm)	C-band (1551.72 nm)
Service Channel	Standard configuration: one channel on DWDM frequency grid (ITU-T G.694.1) or CWDM BIDI. SFPs provided with the solution.				
Segment Type	Access	Backbone	Extra-Long Distance	Copropagation	Star deployment
Recommended Use	Local secure link for end-users	Regional / national QKD infrastructure	Nationwide / Cross-border	Local / regional	Metropolitan
Max Fiber Distance (@0.22 dB / km)	80 km	110 km	150 km	Refer to Clavis XG Multiplex specs	100 km
Min QKD AES-256 Keys / hour @ max distance	70'000	14'000	2'800	Refer to Clavis XG Multiplex specs	Round robin key exchange averages: - 1'170@ 23 dB w/t 3 spokes - 292 @ 23 dB w/t 12 spokes
Q-KMS AES-256 Keys / hour	7'000'000				
Q-KMS Embedded	Secure key relaying, PQC/ECC Hybrid key exchange, redundant key routing and key buffering (refer to Clarion KX brochure for more info)				
Form Factor	1U				2U hub / 1U spoke
Dimensions	1U, 19" rackmount chassis (easy to install sliding rails provided with the each system) W 428 mm x L 610 mm x H 43.6 mm (without front & back handles, and mounting kit)				
Infrastructure Requirements	Minimal		Need of optimal dark fiber	Dependency on copropagated data	Minimal
Deployment Consideration	Quantum channel: One dark fiber. Service channel: One wavelength configurable at the point.			Unlighted o-band. One wavelength configurable at the point.	Quantum channel: One dark fiber. Service channel: One wavelength configurable at the point.
Benefits	• Cost-effective • No need for extensive infrastructure • Ideal for local or small deployments	• Mid-range scalability with strong security • Balanced performance and cost-efficiency • Ideal for region-wide QKD backbones	• Extra-long range • Suitable for global or country-wide networks • High ROI in environments demanding maximal confidentiality	• Best where no dark fiber available	• Cost-effective for highly connected nodes
Power supply	1+1 Redundant hot-swappable power supply (connector on the back panel) Each 300 W, 100-240 VAC, 47-63 Hz, 5-2.5 A or 36-72 VDC (optional) Typical power consumption 80 W per device at 25°C				Same as other models, but: 100 Watts Hub
Device deployment type	Alice/Bob independent	Alice/Bob independent	By pair (Alice and Bob)		Hub and spoke independent (up to 12 spokes)
Protocol	BB84 with two decoy states, Intrinsically Polarization independent, Key security parameter ³ $\epsilon_{\text{QKD}} = 4. \cdot 10^{-9}$				
Random Number Generator Chip	Quantis Quantum Random Number Generator (QRNG)				
Front panel connectivity	• Full Status LEDs available on the front panel • 2 x Duplex Fiber SFP (Service channel, KMS-O, LC/UPC Connectors) • 1 x Simplex Fiber (Quantum channel, SC/UPC Connectors) • 4 x 1 Gb Ethernet ports (Keys / Encryptors, KMS, Mgt, Aux) • 1 x RS-232 (Console) • 1 x USB 2.0				Spoke: Same as other Clavis XG Hub: • 1 x SFP • 12 x LC/UPC Connectors (Service channel) • 12 x SC/UPC Connectors (Quantum channel)
Weight	< 14 kg per device				
Temperature range	Operating: +5 to +40°C (standard cooling: front to back air flow) Non-operating: -10 to +60°C				
Relative humidity range	Operating: 5% to 85% RH, non-condensing ⁽⁴⁾ Non-operating: 5% to 90% RH, non-condensing ⁽⁴⁾				
Management and monitoring					
Alerting functions & continuous monitoring ⁽⁵⁾	XG Series can be administrated, configured and monitored via multiples interfaces (QNET REST Web API, QNET CLI Tools, QMS Web Application, SNMP, Syslog)				
Applicable standards	FCC: 47 CFR, Part 15 (Class A) Industry Canada: ICES-003, Issue 7 (Class A) RoHS: 2015/863/EU NIST: ESV IID SP 800-90B (IDQ QRNG chip)		CE Safety: IEC 62368-1:2018, IEC 60825-1:2014 CE EMC: EN 55032:2015+A11:2020 (Class A) EN 55035:2017+A11:2020		

⁽¹⁾ Including IDQ embedded filters necessary for multiplex system. Mux/Demux to be provided by third party.

⁽²⁾ Between 1 and 12 spokes supported

⁽³⁾ With the above value, the probability that an eavesdropper knows at least one bit of a 256-bits AES key is about 10^{-12} . See this example.

⁽⁴⁾ As per ETSI-300-019-1-3 Class 3.1

⁽⁵⁾ Provided separately