Redefining Security

Cerberis XG QKD System

Quantum Key Distribution for production environments requiring standard key transmission rate and medium range interconnection

Safety of current encryption methods, and especially of the key exchange mechanisms based on asymmetric cryptography, is a major concern today. Possible back-doors in current systems combined with massive computing power already put high-value sensitive data at risk of being decrypted by malevolent actors. Moreover, the arrival of quantum computers is imminent and will render arithmetic asymmetric key exchanges unsafe: encrypted data can be stored now and easily decrypted later. Governments or enterprises, which must protect data for five to ten years or more, need to move to new crypto solutions now.

As a leading security solution provider, IDQ has developed Quantum Key Distribution (QKD) systems that generate and distribute cryptographic keys across a provably secure communication network, to safely encrypt or authenticate data. Cerberis XG is the 4th generation of our Cerberis Series. QKD exploits a fundamental principle of quantum physics – observation causes perturbation – to exchange cryptographic keys over fiber optic networks with provable security: an eavesdropper intercepting keys transmitted on the QKD quantum channel will necessarily translate into a perturbation that can be detected by the sender and recipient.

In contrast to conventional key distribution algorithms, QKD is the only known cryptographic technique which offers 100% forward security, resilience to new attack algorithms from current and upcoming quantum computers.

Key Markets

- Telecom and Data Center Service Providers
- Financial Services Companies
- Governments and Defense
- Healthcare Organizations
- Critical Infrastructure
- IP-rich Enterprises

Key Applications

- Data center interconnections
- Metropolitan backbone optical networks
- Long distance distribution using relay nodes
- Key distribution across a complex network (ring, hub and spoke, meshed)
- Crypto keys as-a-service
- Validation of QKD and encryption pilot networks

Cerberis XG QKD System

Robust and standard design to be integrated in any Data Center

The Cerberis 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. The XG Series is designed for uninterrupted and long-term operation by providing high availability services.

SYSTEM DESCRIPTION

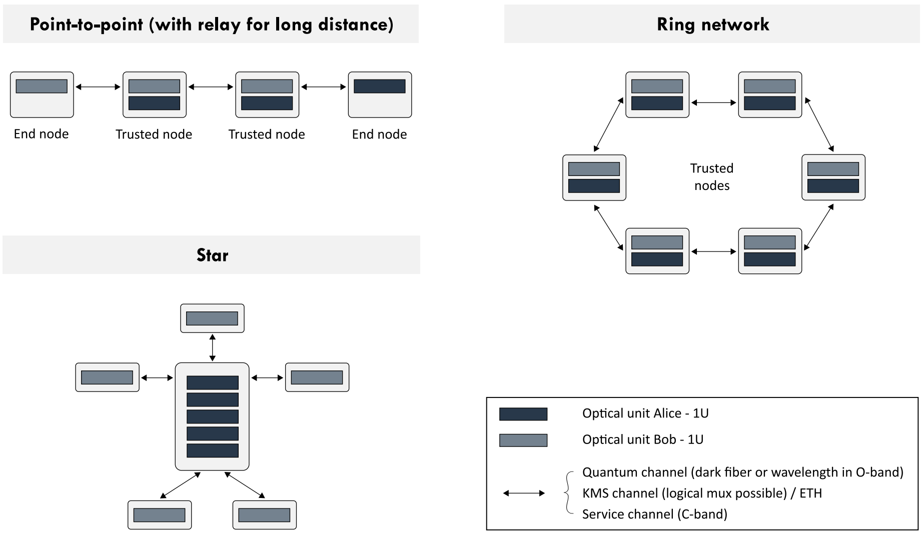
Cerberis XG systems can be deployed in any network configurations including point-to-point, relay for longer distances, ring or star topologies. At each QKD network node, an embedded Key Management System (KMS) software arbitrates the key distribution between QKD and key consumers as well as performing add/drop or forward functions depending on the recipient's location.

The Cerberis XG QKD System

IDQ XG Series of products operates at standard telecommunication wavelengths (in the O and/or C bands) and can be easily retrofitted onto existing fiber optic network. The XG Series 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 a standard optical fiber leading to easy installation and maintenance, and minimized 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 1310nm (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.


Point-to-point (with relay for long distance)
End node
Trusted node
Trusted node
End node
Ring network
Trusted nodes
Star
Optical unit Alice - 1U
Optical unit Bob - 1U
Quantum channel (dark fiber or wavelength in O-band)
KMS channel (logical mux possible) / ETH
Service channel (C-band)

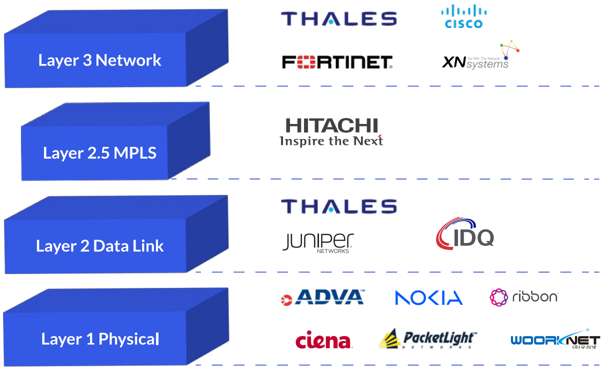
Interoperability is key

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

Supported/PoC vendors

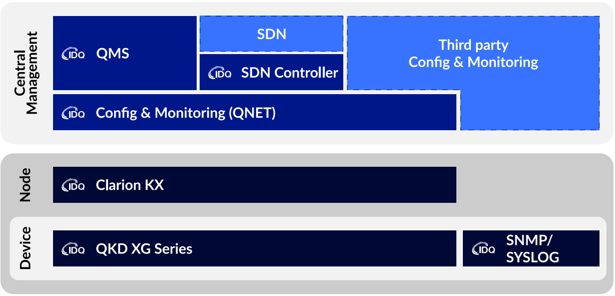


Integration with other suppliers available upon request

KEY MANAGEMENT AND MONITORING

The XG Series integrates 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 XG Series 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.



MAIN ADVANTAGES

- Provably secure 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 (polarisation-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)

XG Series QKD System at a glance

Model	Cerberis XG
KEY FEATURES	
Maximum length of quantum channel (typ. @ 0.2 dB/km)	60 km (@ 12 dB, optional 80/90 km @ 16/18 dB)
Secret key rate	Typical 14’000 AES-256 Keys per hour @ 18 dB Typical 28’000 AES-256 Keys per hour @ 12 dB
Protocol	COW
Key generation source	IDQ QRNG chip
Quantum channel	1 dedicated fiber (Optional WDM: O-Band in a single core)
Service Channel	1 TX/RX DWDM channel (C-Band)
Optical engine	Intrinsically Polarization independent
Key processing	High speed hardware-based
Key security parameter[1]	$\varepsilon_{QKD} = 4.\ 10^{-9}$
Pulse repetition rate	1.25 GHz
ENVIRONMENTAL AND PHYSICAL PARAMETERS (per device)	
Form factor	1U, 19’’ rackmount chassis
Dimensions (without front & back handles, and mounting kit)	W 428 mm x L 610 mm x H 43.6 mm
Interfaces	• Full Status LEDs available on the front panel • 2x Duplex Fiber SFP (Service Channel, KMS-O) • 1x Simplex Fiber (Quantum Channel) • 4x 1Gb Ethernet ports (Keys / Encryptors, KMS, Mgt, Aux) • 1x RS-232 (Console) • 1x USB 2.0
Power supply	1+1 Redundant hot-swappable power supply Each 300 W, 100-240 VAC, 47-63 Hz, 5-2.5 A or 36-72 VDC (optional)
Weight	13.5 kg
Temperature range	Operating +10 to +35°C Non-operating -10 to +60°C
Relative humidity range	Operating 5% to 80% RH, non-condensing Non-operating 5% to 90% RH, non-condensing
MANAGEMENT AND MONITORING	
Alerting functions & continuous monitoring[2]	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 62638-1:2018, IEC 60825-1:2014 **CE EMC:** EN 55032:2015+A11:2020 (Class A) EN 55035:2017+A11:2020

[1] 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.
[2] Provided separately

ID Quantique

Rue Eugène-Marziano 25
1227 Geneva, Switzerland

T +41 22 301 83 71
F +41 22 301 83 79
E info@idquantique.com

www.idquantique.com

ID Quantique (IDQ) is the world leader in quantum-safe security solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and government organizations globally.

IDQ also commercializes a quantum random number generator, which is the reference in the gaming and security industries.

Additionally, IDQ is a leading provider of optical instrumentation products; most notably photon counters and related electronics. The company’s innovative photonic solutions are used in both commercial and research applications.

Disclaimer: The information and specification set forth in this document are subject to change at any time by ID Quantique without prior notice.