



Redefining Security

Cerberis XG QKD System

Quantum Key Distribution for enterprise, government and telco production environments

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 optical fiber 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 forward security, resilient to new attack algorithms and upcoming quantum computers.

Key Markets

-  Telecom and Data Center Service Providers
-  Financial Services Companies
-  Governments and Defence
-  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

Robust and standard design to be integrated in any Data Center

The Cerberis XG is the 4th generation of QKD systems at ID Quantique, 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.

SYSTEM DESCRIPTION

Cerberis XG system meets all requirements for an 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.

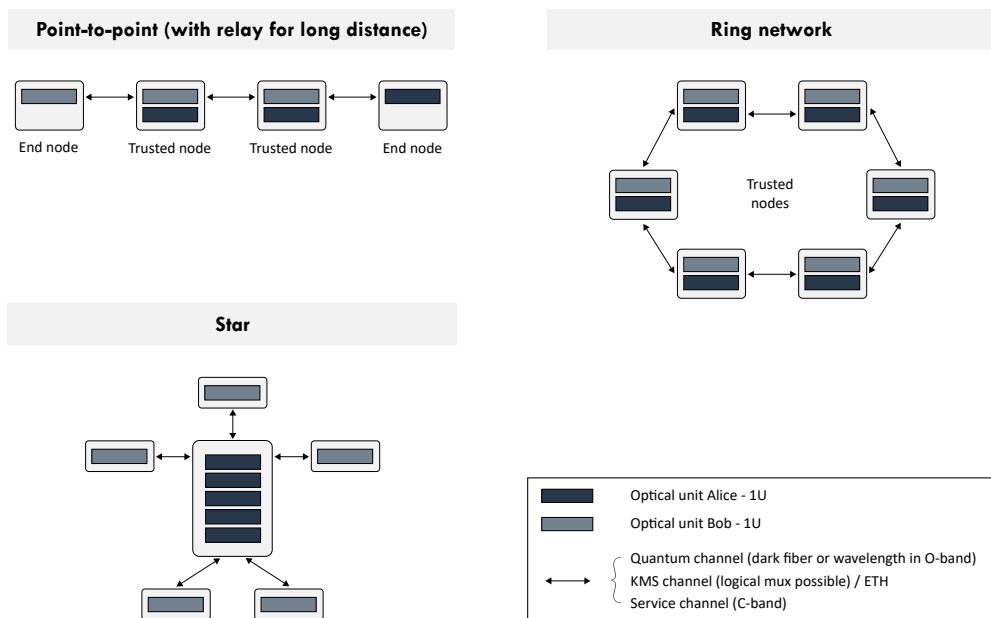


The Cerberis XG QKD System

Quantum communications are done 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.

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 and performs add/drop or forward functions depending on the recipient's location.

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.



Interoperability is key

The Cerberis XG 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

Major encryptor vendors, notably leading Optical Transport Network (OTN) vendors, offer QKD-ready encryption appliances (OSI Layer 1/2/3/4 and MPLS), which interface with Cerberis XG through 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.

ID Quantique can also provide a full cryptographic solution that guarantees long-term protection of data into the quantum era by combining Cerberis XG with Centauris high-speed Ethernet encryptors.



KEY MANAGEMENT AND MONITORING

Cerberis XG performs standard key management functions between nodes, including key generation, key storage and key life cycle management. Cerberis XG embeds enhanced trusted security components, like tamper detection, a secure memory module, as well as an IDQ QRNG chip which provides proven randomness for all the related crypto functions. This

guarantees the highest security standards, throughout the key management process, from key generation to key delivery, and including key storage.

QKD administrators can configure and monitor QKD networks via either an embedded REST WebAPI or via an Element Management System (EMS) web console by setting consumers, providers at each QKD network node, QKD links between nodes and key distribution routes between key consumers.

The WebAPI continuously collects several critical parameters, such as system status, fan, power supply, temper detection, Quantum key rate, QBER (Quantum Bit Error Rate), KMS key buffers, and is able to distribute them to 3rd party monitoring systems, via common protocols like SNMP, syslog, etc. Monitoring events are also generated when QBER becomes too high, warning there might be an intruder on the QKD quantum channel.

In addition, our Quantum Management System (QMS) provides a single Management and Monitoring platform for all QKD products and components. It reduces the time and effort to manage large and complex QKD Network.

Cerberis XG answers high availability requirements with redundant power supplies, hot swap battery and fans module, and key buffering functions that ensure continuous quantum key supply.



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

Embedded KMS and Management Tools

Resilient to mechanical vibrations and thermal changes in fiber optics (polarisation-independent scheme)

Centrally monitored solution

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)

Cerberis XG QKD System at a glance

Model	Cerberis XG
KEY FEATURES	
Key generation rate	1.25GHz pulse repetition rate
High speed hardware-based key processing, to distill the secret keys	✓
Key security parameter ¹	$\epsilon_{\text{QKD}} = 4 \cdot 10^{-9}$
Dynamic range	12 dB (up to 16/18 dB on request)
Maximum length of quantum channel (typ. @ 0.23 dB/km)	50 km (up to 70/80 km on request)
Secret key rate	2 kb/s (12 dB)
PHYSICAL PARAMETERS	
Dimensions	19" rackmount chassis; 22.4"
Dimensions (without front & back handles, and mounting kit)	W 428mm x L 610mm x H 43.6mm
Interfaces	Full Status LEDs, 2x Duplex Fiber SFP (Service Channel, KMS-O), 1x Simplex Fiber (Quantum Channel), 4x 1Gb Ethernet ports (Keys / Encryptors, KMS, Management, Aux), 1x RS-232 Serie (Console), 1x USB 2.0
Power supply	1+1 Redundant power supply consisting of two 300W hot-swappable power modules with input ratings of 100V-240Vac, 47-63Hz, 5-2.5A
Weight for one node	13.5 kg
Operating conditions	
Temperature	10 to 35°C
Max relative humidity (@35°C)	80% (non condensing)
Non-operating conditions	
Temperature	-10 to +60°C
Max relative humidity (@40°C)	90% (non condensing)
MANAGEMENT AND MONITORING	
Alerting functions & continuous monitoring	Cerberis XG can be administrated, configured and monitored via multiples interfaces (QNET REST Web API, QNET CLI Tools, QMS Web Application) allowing users or systems to control, and automatize through scripting, the various QKD services.

¹ The key security parameter characterises quantitatively the quality of the distributed keys. Technically, it is defined as the probability that the key distillation process went wrong, with either an error or at least one bit of the key leaked to the eavesdropper. It is normally calculated over a large block size, to allow an efficient distillation process. 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 for example: <https://doi.org/10.1088/1367-2630/16/1/013047>



ID Quantique

Chemin de la Marbrerie 3,
1227 Carouge/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.