Redefining Security

Cerberis³ 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. QKD exploits a fundamental principle of quantum physics – observation causes perturbation – to exchange cryptographic keys over optical fibre 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 Organisations
- 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)
- Crypto keys as-a-service
- Validation of QKD and encryption pilot networks

Cerberis³ QKD System

Robust and standard design to be integrated in any Data Centre

The Cerberis³ is the latest generation of QKD systems at ID Quantique, based on 16 years of experience in the development and commercialisation of quantum-based products. It now supports any kind of network topologies, such as point-to-point, relay, ring and hub and spoke networks.

SYSTEM DESCRIPTION

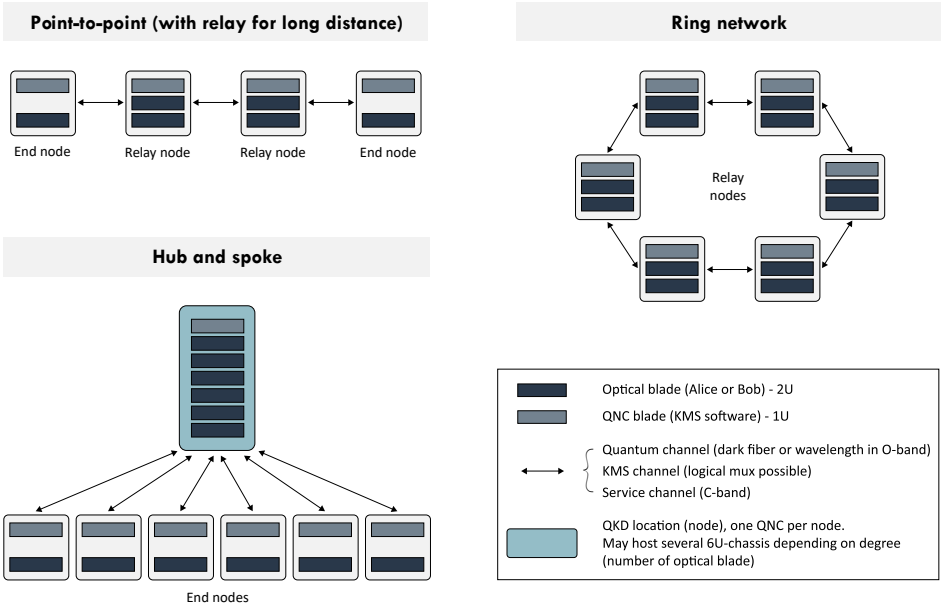
Cerberis³ system meets all requirements for an easy integration in any data centre. Its 19" rackmount 6U ATCA chassis presents high performance integrated Switch and Shelf Manager, and redundant power supplies. It can host a QNC blade for key management, monitoring, and administration and 1 or 2 QKD Cerberis optical blades that perform the quantum key generation and distribution over a quantum channel with a transmitter (Alice) on one end and a receiver (Bob) on the other end.

The Cerberis³ QKD System, in ATCA chassis

Quantum communications are done over a standard optical fibre leading to easy installation and maintenance and minimised total cost-of-ownership. All optical channels are compatible with the ITU recommendation for Dense-Wavelength-Division-Multiplexing (DWDM). To maximise the distance between nodes, operation of the quantum channel over a dark fibre is recommended. However, channel multiplexing over a single core can be performed with quantum channel around 1310nm (O-band) whenever fibre resources are scarce.

Cerberis³ systems can now be deployed in any network configurations including point-to-point, relay for longer distances, ring or hub and spoke topologies. At each QKD network node, a KMS software hosted on the Quantum Node Controller (QNC) blade arbitrates the key distribution between QKD and key consumers and performs add/drop or forward functions depending on the recipient's location. QKD blades can be housed in same chassis for point-to-point or relay topologies, or add-on chassis connected to the QNC, in case of complex network topologies.

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.



Cerberis³ QKD System

Interoperability is key

The Cerberis³ is the first commercial QKD system that can interface with link encryptors from major vendors. It answers high availability requirements thanks to dual redundant power supply, 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), which interface with Cerberis³ through standard and proprietary interfaces. ID Quantique is actively taking part in the standardisation 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 Cerberis³ with Centauris high-speed Ethernet encryptors.

KEY MANAGEMENT AND MONITORING

Cerberis³ performs standard key management functions between nodes, including key generation, key storage and key life cycle management.

QKD administrators can configure QKD network 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.

QKD administration can continuously monitor centrally via SNMP critical parameters such as temperature, fan and power supply, CPU load, Quantum key rate and Quantum Bit Error Rate (QBER). Syslog alerts are also generated in case some thresholds are reached: in particular, an alarm is sent when QBER becomes too high showing there is an intruder on the QKD quantum channel. With Cerberis³, the probability that an eavesdropper knows at least one bit of a 256-bits AES key is about 10^{-12}.

Cerberis³ answers high availability requirements with redundant power supplies 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 fibre
- Easy integration in any data centre
- Interoperability with major Ethernet and OTN encryption vendors
- Resilient to mechanical vibrations and thermal changes in fiber optics (polarisation-independent scheme)
- Centrally monitored solution
- Non-intrusive to data communication channels

Cerberis^3 QKD System at a glance

Model	Cerberis^3
KEY FEATURES	
Key generation rate	1.25 GHz pulse repetition rate
High speed hardware-based key processing, to distill the secret keys	✓
Key security parameter[1]	$\varepsilon_{QKD} = 4.\ 10^{-9}$
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	1.4 kb/s (12 dB)
PHYSICAL PARAMETERS	
Dimensions[2]	19'' rackmount 6U ATCA chassis; 13'' depth
Switching Shelf Manager (SSM)	Full status LEDs, 10GbE SFP+, GbE ports, RS-232 de-bug ports, and Telco alarm
Power supply	Up to 4x swappable 1300 W AC power supplies or 2x 90 Amp DC Power Entry Modules. The input voltage is from 100 to 240 VAC or -36 to-72 VDC
Weight for one node[2]	30 kg
Operating conditions	
Temperature	10 to 30°C
Max relative humidity (@30°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	Temperature (high and low), fan failure, power supply failure, low key rate, high QBER (intruder alarm), service and key channel failure, key buffer
Continuous monitoring	Temperature, fan and power supply operations, system uptime, firmware version, CPU load, memory usage, actual quantum key rate, QBER, compression rate (due to key processing)

[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

[2] For a typical installation with the ATCA chassis, the QNC and one QKD blade

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 organisations globally.

IDQ also commercialises 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.