

# Cerberis

The best of classical and quantum worlds  
Symmetric encryption and quantum key distribution

Ethernet ATM  
SONET / SDH  
Fibre Channel



## Unprotected optical fiber networks are at risk

Most organizations rely on optical links to connect their disaster recovery sites, data centers or branch offices, often over a semi-private network supplied by a telecom company. These links are often left unprotected with sensitive data being sent in clear. This constitutes a security breach since optical fibers can be tapped easily using cheap optical taps. It is now standard practice to protect mission-critical data traveling outside secure perimeters of companies using encryption.

## A fast and secure solution: high-speed encryption combined with quantum key distribution

id Quantique's Cerberis solution offers a radically new approach to network security, combining the sheer power of high-speed layer 2 encryption appliance with the unconditional security of quantum key distribution (QKD) technology.

Dedicated appliances perform high-speed encryption based on the proven Advanced Encryption Standard (AES). Point-to-point wire-speed encryption with low latency and no packet expansion is made possible by operating at the layer 2 of the OSI model. Four protocols are supported, namely Ethernet (up to 10Gbps), Fibre Channel (up to 4Gbps), SONET/SDH (up to 10Gbps) and ATM (up to 622Mbps).

The exchange of secret encryption keys, the Achilles heel of classical cryptography products, is performed in a separate appliance, called the QKD server. A fundamental principle of quantum physics - observation causes perturbation - is exploited to exchange secret keys between two remote parties over an optical fiber with unprecedented security. The QKD server autonomously produces, manages and distributes secret keys to one or more encryption appliances.

## A scalable solution that grows with your needs

The Cerberis solution is cost-effective as it evolves with the network. Additional encryption appliances can be added to a QKD server at any time, without network interruption. This allows for a scalable deployment, adding more encryption appliances whenever necessary to increase the bandwidth or to add additional protocols, without upgrading the QKD server. With the Cerberis solution, your infrastructure investments last longer and your total cost of ownership is reduced.

## Installation and management is a breeze

The Cerberis solution integrates seamlessly into existing fiber-optic network infrastructures. A simple installation procedure ensures rapid deployment. Top-notch management tools, such as on-line single-point monitoring via Simple Network Management Protocol (SNMP) and off-line web-based applications, give network administrators the capability to centrally monitor and manage the appliances of the Cerberis solution within an enterprise network.

## Regulatory compliances? Get peace of mind with the most technologically advanced solution

Regulations, such as BASEL II, SOX, HIPAA and GLBA, are mandating companies to protect their private data. The scope of threats in today's information society is vast and growing. Companies securing their fiber-optic network with the Cerberis solution effectively raise, to an unprecedented level, the security of communications between their remote sites. It gives them the peace of mind of knowing that they are using the latest in cryptographic technology, and allows them to focus on other threats.

### Why Quantum Cryptography?

**Intrinsic secrecy of cryptographic keys**  
Guaranteed by quantum physics

**Reveals eavesdropper's presence**  
Observation causes perturbation

**Future-proof data confidentiality and integrity**

**High key-refresh rate**  
Automated

### Main Features

**High speed full duplex encryption**  
Ethernet: 10 / 100 Mbps, 1 Gbps, 10 Gbps  
Fibre Channel: 1, 2, 4 Gbps  
SONET/SDH: OC-3, OC-12, OC-48, OC-192  
ATM: OC-3, OC-12

**Encryption algorithms**  
AES 256-bit

**Automated key management**  
Secret keys exchanged via quantum physics  
"Set and forget" operation

**Point-to-point Layer 2 encryption**  
For LAN / MAN / SAN networks

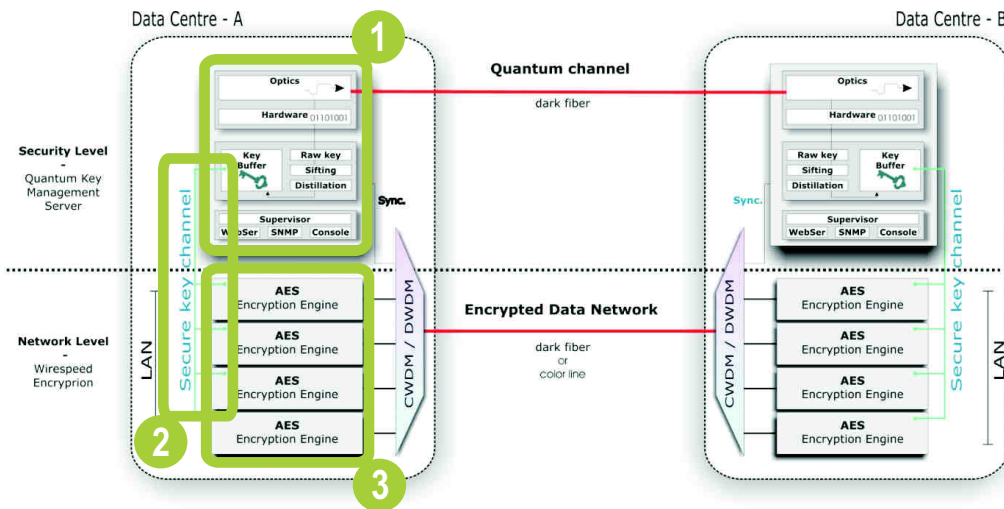
**No impact on network performance**  
Latency below 15µs  
Total bandwidth availability, wire speed

**Simple and secure device management**  
On-line monitoring via SNMP v3  
Off-line management via web server and  
Touch panel display user interface  
Identity-based authentication

**Scalable, stackable**  
Up to 12 encryption appliances in parallel

# Quantum Cryptography

The key to future-proof confidentiality



## QKD Server Performance 1

- ▶ Plug&Play Optical Platform
- ▶ BB84/SARG Protocol
- ▶ Range: < 50km (> 50 Km on request)
- ▶ Secret key rate: > 1'000 bps over 25 km
- ▶ One Quantum Key Server can:
  - ▶ serve up to 12 encryptors
  - ▶ serve encryptors for different protocols

## Key Channel (idQ3P) 2

- ▶ Serial link
- ▶ Encrypted (AES-256)
- ▶ Authenticated (HMAC-SHA-1)
- ▶ Key Exchange rate: 1/minute

## Encryption Appliance 3

- ▶ Up to 10 Gbps
- ▶ Multiprotocol
  - ▶ Ethernet
  - ▶ SONET/SDH
  - ▶ Fibre Channel (FC)
  - ▶ ATM
- ▶ Accredited (FIPS, Common Criteria)

## Technical specifications

<b>Protocols</b>	Ethernet: 10 Mbps, 100Mbps, 1Gbps and 10Gbps Fibre Channel: FC-1G, FC-2G and FC-4G SONET/SDH: OC-3, OC-12, OC-48 and OC-192 ATM: OC-3, OC-12
<b>Cryptography</b>	AES 256-bit
<b>Key Management</b>	QKD protocols: BB84 and SARG QKD server with automated key creation and exchange Secret keys exchanged between QKD server and encryption appliances through secure key channel
<b>Authentication</b>	HMAC-SHA-1 (classical link) Wegmann Carter (QKD link) RSA public key X.509 certificates
<b>Performance</b>	Key refresh rate: 1 key/min up to 12 encryption appliances Quantum link channel length up to 50km on single mode dark fiber (longuer distance on request)
<b>Access Control</b>	Identity based identification Rule based
<b>Audit Trail</b>	Event log, audit log, date and time of secure connexion Configuration changes Interface Status Alarms
<b>Secure Management</b>	<i>QKD Server</i> SNMPv3, Ethernet 10/100 Rj45, touch panel <i>Cryptographic appliance</i> SNMPv1, v2 and v3, Ethernet 10/100 Rj45, browser TLS or IPsec trusted path In-band on local and network interfaces
<b>Indicators</b>	Blue touch panel, 240x180 pixels (QKD server) Two line 20 characters LCD display (encryption appliances) LED indicating status of local interface, network interface, temperature, battery status, system operation and secure status, power
<b>Physical Security</b>	Tamper proof storage of encryption keys and users passwords Tamper resistant metal case
<b>Environmental</b>	Operating temperature 5° to 30° C Non-operating temperature -10° to 60° C Operating humidity 0 to 80% RH @ 40° C Non-operating humidity 95% RH @ 40° C

### Disclaimer

The information and specification set forth in this document are subject to change at any time by id Quantique without prior notice.  
Copyright© 2007 id Quantique SA. All rights reserved.