

Cerberis

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

Ethernet ATM
SONET / SDH



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 standardized 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. Three protocols are supported, namely Gigabit Ethernet, 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 Kanga 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
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

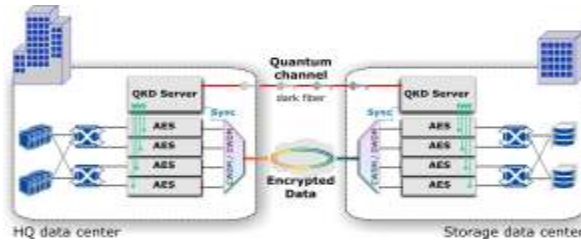
No impact on network performance
Latency below 15µs
Total bandwidth availability, wire speed

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 4 encryption appliances in parallel

Quantum Cryptography

The key to future-proof confidentiality



Technical specifications

Protocols	Ethernet, SONET/SDH, ATM			
Cryptography	AES 256-bit			
Key Management	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			
Authentication	HMAC-SHA-1 (classical link) Wegmann Carter (QKD link) RSA public key X.509 certificates			
Performance	Key refresh rate: 1 key/min up to 4 encryption appliances Quantum link channel length up to 80km on single mode dark fiber			
Access Control	Identity based identification Rule based			
Audit Trail	Event log, audit log, date and time of secure connexion Configuration changes Interface Status Alarms			
Secure Management	<i>QKD Server</i> <i>Cryptographic appliance</i>	SNMPv3, Ethernet 10/100 Rj45, touch panel SNMPv1, v2 and v3, Ethernet 10/100 Rj45 In-band on local and network interfaces		
Indicators	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			
Interfaces	<i>QKD server appliance</i> Quantum link channel: SC connector, single mode fiber Sync link: GBIC module with SC connector, single mode fiber Secure key channel Rs232 10/100BASE-T Rj45 <i>SONET/SDH encryption appliance</i> OC192-c/STM-64 Single mode fiber, 15km and 40km reach. LC connectors 3R interfaces (re-amplify, re-shape, re-time)	<i>Gigabit Ethernet encryption appliance</i> 10/100BASE-T Rj45 1000BASE-T Rj45 1000BASE-SX SFP LC connector 1000BASE-LH SFP LC connector <i>ATM encryption appliance</i> OC12-c/STM-4Single/Multimode fibre 2, 15, 40km reach. SCconnector OC3-c/STM-1 Single/Multimode fibre 2, 15, 40km reach. SC connector E1/E3/T3 - BNC 75 ohm coaxial T1 - RJ45 connector		
Physical Security	Tamper proof storage of encryption keys and users passwords Tamper resistant metal case			
Environmental	Operating temperature Non-operating temperature Operating humidity Non-operating humidity	5° to 40° C -10° to 60° C 0 to 80% RH @ 40° C 95% RH @ 40° C		
Electrical	<i>QKD Server</i> Redundant power supply 110VAC to 250VAC, 50-60HZ	<i>Gigabit Ethernet</i> 90VAC to 250VAC, 47-63HZ 24VDC to 48VDC 25 Watts maximum	<i>SONET/SDH</i> 90VAC to 250VAC, 47-63HZ 48VDC 40 Watts maximum	<i>ATM</i> 90VAC to 250VAC, 47-63HZ 48VDC 30 Watts maximum
Mechanical	<i>QKD Server</i> Height – 177mm (4RU) Width – 428mm-19” rack mount. Depth – 466mm Weight – 16kg	<i>Gigabit Ethernet</i> Height – 41mm (1RU) Width – 435mm-19” rack mount. Depth – 285mm Weight – 4kg	<i>SONET/SDH</i> Height – 123mm (3RU) Width – 435mm-19” rack mount. Depth – 285mm Weight – 5kg	<i>ATM</i> Height – 41mm (1RU) Width – 435mm-19” rack mount. Depth – 285mm Weight – 4.5kg

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.

Cerberis v.1.0 - Specifications as of March 2007



Senetas Corporation
Level 1, 11 Queens Road
Melbourne, 3004 Australia
Tel + 61 3 9868 4555
Fax + 61 3 9821 4899
www.senetas.com

id Quantique SA
ch. de la Marbrerie 3
1227 Carouge, Switzerland
Tel + 41 (0)22 301 83 71
Fax + 41 (0)22 301 83 79
www.idquantique.com

