# INTERNATIONAL BANKING CN8000 MULTI-LINK ENCRYPTION

## CASE STUDY

| Application of High-Assurance Network Encryption | |
|---|---|
| **Sector:** | Financial Services |
| **Use Case:** | Multi-link WAN security |
| **Solution:** | Securing global banking WAN with multi-link encryption featuring QKD |

SENETAS
Security without compromise

# Senetas CN8000 multi-link 10x10Gbps encryptors protect global bank's Ethernet WAN.

## OVERVIEW

A global bank was seeking to address its commitment to customer confidentiality, regulatory compliance and an increasing dependence upon real-time, big data applications.

The bank serviced an international clientele from a network of 30+ offices across 3 continents, all connected via an Ethernet WAN.

To meet its stated objectives, the bank needed to upgrade its network data encryption solution. Above all, it was looking for a high-performance solution that was easy to deploy and manage without "breaking the bank".

## OUT WITH THE OLD

The bank's existing solution was a Layer 2 E1/T1 link. As the bank grew, the old system was no longer able to cope with the increased volume of data and was beginning to impact on network performance.

While assessing alternative solutions, the bank investigated a Layer 3 IPSec solution. This was rejected due to the relatively high cost, complexity of installation and lower throughput.

IPSec encryption adds significant overhead to the data packets. In addition, because the routers fragment and reassemble the packets, there were technical issues with packet reassembly; resulting in higher latency.

## IN WITH THE NEW

Working in partnership with its multinational telecommunications service provider, the bank evaluated several solutions before choosing Senetas certified high-assurance encryptors.

Senetas provides a range of Layer 2 Ethernet encryptors, operating at line speeds from 10Mbps to 10Gbps.

Given the high-performance and security credentials demanded by the financial services industry, it was determined that the CN8000 would be the best solution.

## SENETAS CN8000 MULTI-LINK ENCRYPTOR

The CN8000 was designed and developed in partnership with Swiss Quantum-Cryptography experts, ID Quantique.

IDQ is the world leader in quantum-safe cryptography solutions, designed to provide long-term data protection in a post-quantum world.

IDQ provides a variety of quantum random number generators, quantum key generators and quantum key distribution solutions. Its clients include financial services, government and defence agencies worldwide.

## KEY BENEFITS

Senetas CN8000 certified high-assurance encryptors were the solution of choice as they provide:

> Reliable, field-proven hardware

> Support for AES 256bit encryption keys

> Support for all Layer 2 Ethernet network topologies

> Full duplex wire speed encryption up to 10Gbps

> Ultra-low latency (< 7.5 microseconds per appliance)

> A single GUI and management platform for multiple protocols

> Secure remote management and upgrade

> Secure remote management & upgrade

In addition, the CN8000 series is certified as suitable for government and defence use by both FIPS and Common Criteria.

Senetas CN8000 Multilink Encryptor

## DEPLOYMENT

Following a successful pilot project, the bank rolled out the encryption platform to their global WAN, incorporating over thirty branches on three continents.

Redundant multilink CN8000 devices were used for the hub at the bank's head office; securing 10Gbps links.

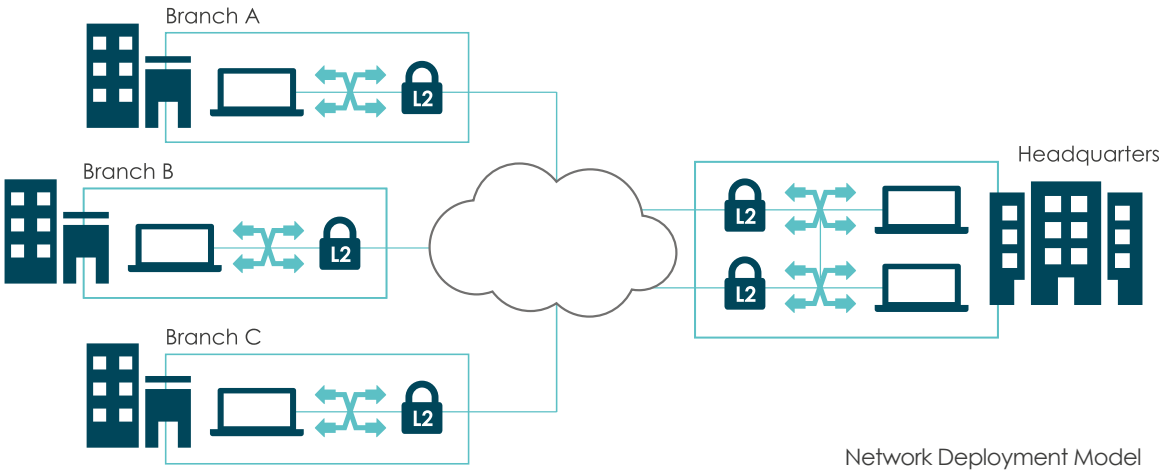
Other high-assurance CN series encryptors were used to secure the end points in the WAN, depending on the bandwidth requirements and space available in the branch offices.

Initially, the branch locations opted for rate-limited encryptors, with bandwidths from 100Mbps to 1Gbps.

This enabled the bank to just pay for the bandwidth used, helping them to meet their Capex budget requirements.

However, it also provided the bank with the flexibility to upgrade the branches as bandwidth demands increase, without changing the hardware.

All Senetas CN Series encryptors are fully interoperable and share a common management platform.




Network Deployment Model

## KEY BENEFITS

**High performance** - Senetas CN8000 encryptors provide high-throughput encryption on the telco's MPLS network, using 100% of the bandwidth with no packet loss in transport mode.

**Low Latency** - The CN8000 provides the ultra-low latency necessary for real-time communication (under 7.5 microseconds per encryptor)

**Multicast Support** - For VLAN-based multicast traffic, Senetas' intelligent group key system utilizes one encryption key per secured connection.

This means, for example, that the head office could securely video conference with branch A and branch C, without branch B being able to access the communication.

**Certified Secure** - Senetas CN8000 encryptors are based on the leading 256-bit AES cipher in CTR/CFB mode and are certified by both FIPS and CC.

**Scalable architecture** - The CN8000 encryption platform provides both security and versatility in a point-to-multipoint architecture.

Senetas encryptors support different types of traffic across a range of applications, including unicast, multicast (finance information to traders, secure video conferencing) and broadcast (automated equipment info exchange).

**Intelligent Key Management** - The Intelligent Group Key system provides a higher level of security in case of partial network failure – essential for global banking operations in countries with variable SLAs.

Here, the keys are generated per secured connection and are renewed up to every 60 seconds, providing much greater resilience to common network problems.

In the event of a partial network outage or loss of connectivity between two network areas, the keys are still renewed and continue to function as required in each separate part of the remaining network

**Management** - The CM7 graphic management platform user interface facilitates the everyday remote management of the network, the keys and the encryptors through a secure SNMPv3 connection.

The bank can monitor real-time status and configuration changes easily. Different levels of user rights within CM7 allow for separation of duty between the network and security teams, with mission critical functions reserved for the administrator role.

In addition, the topology of the network and the addition or deletion of encryptors can be managed while the encryptors are still functioning, either in manual or in auto discovery mode.

## SPECIFICATIONS

### Cryptography

> AES 128-bit or 256-bit key X.509 certificates

> CTR, GCM modes

### Performance

> 10 Gbps full-duplex Ethernet encryption per card - (< 8µs latency) up to 100 Gbps total bandwidth

### Encryptor management

> Dedicated management interface (outof-band)

> Or via the encrypted interface (in-band)

> SNMPv3 remote management

> SNMPv2c traps

> SNMPv1 read only monitoring

> IPv4 & IPv6 capable

> Supports Syslog, NTP

> Alarm, event, and audit logs

> Command line serial interface

### Installation

> Size: (4U), 430,460,175mm / 17.2, 18.1, 6.9 inches (Wx-HxD)

> Rack mountable

> Maximum Weight: 22kg / 49lbs.

### Interfaces

> SFP+

> Front panel network connections

> Front panel LED display status

### Indications

> Color backlit LCD display

> RS-232 serial console for CLI connection

> USB port

> RJ45 SNMP management port

> RS-232 serial console for quantum key channel

### Power Requirements

> Input: 100 to 240V AC;1.5A; 60/50Hz

> Power: 300 watts for 10 links

### Physical security

> Active/passive tamper detection and key erasure

> Tamper-evident markings

> Anti-probing barriers

### Regulatory Safety

> EN 60950-1 (CE)

> IEC 60950-1 Second Edition

> AS/NZS 60950.1

> UL Listed

> EMC (Emission and Immunity)

> ICES-003 (Canada)

> EN 55022 (CE)

> AS/NZS CISPR 22 (C-Tick)

> EN 61000-3-2 (CE)

> EN 61000-3-3 (CE)

> EN 55024 (CE)

> EN 61000-3-3 (CE)

> EN 55024 (CE)

### Environmental

> RoHS compliant

> Max operating temperature: 40°C/104°F

> 0 to 80% RH at 40°C/104°F operating

All specifications are accurate as of the time of publishing and are subject to change without notice to meet the ongoing requirements of Senetas and its customers.

## CN8000 AT-A-GLANCE

| Model | CN8000 |
|---|---|
| Protocol | Ethernet |
| Maximum port speed | 10 Gbps |
| Maximum chassis throughput | 100 Gbps |
| Support for jumbo frames | ✓ |
| **Security** | |
| Tamper resistant and evident enclosure | ✓ |
| Flexible encryption policy engine | ✓ |
| Per packet confidentiality and integrity with AES-GCM | ✓ |
| **Encryption policy** | |
| AES 128-bit or 256-bit keys | 128/256-bit keys |
| Quantum random generator | ✓ |
| Supports optional 3rd party quantum key distribution (QKD) | ✓ |
| Policy based on MAC address or VLAN ID | ✓ |
| Self-healing key management | ✓ |
| **Performance** | |
| Low overhead full duplex line rate encryption | ✓ |
| Latency (microseconds per link) | <8 |
| FPGA based cut-through architecture | ✓ |
| **Management** | |
| Centralized configuration and management using CM7/SMC* and SNMPv3 | ✓ |
| Support for external (X.509v3) CAs | ✓ |
| Remote management using SNMPv3 (inband and out-of-band) | ✓ |
| NTP (time server) support | ✓ |
| CRL and OCSP (certificate) server support | ✓ |
| **Maintainability / interoperatibility** | |
| In-field firmware upgrades | ✓ |
| Dual hot swappable AC power supplies | ✓ |
| User replaceable fans | ✓ |
| Fully interoperable with related CN models | ✓ |
| **Physical and installation** | |
| Front panel access for all interfaces | ✓ |
| Chassis airflow | Front to rear |

## GLOBAL SUPPORT AND DISTRIBUTION

Senetas high-assurance encryptors are supported and distributed globally (excl. AUS & NZ) by Gemalto – the world's largest data security company - under its SafeNet Identity and Data Protection Solutions brand.

Gemalto also provides pre-sales technical support to hundreds of accredited partners around the world; including systems integrators, data network providers, cloud and data centre service providers, telecommunications companies and network security specialists.

## TALK TO SENETAS OR OUR PARTNERS

Senetas and Gemalto also work with customers' own data network service providers, systems integrators and information security specialists to specify the optimal high-assurance encryption solution for their needs.

Wherever you are, simply contact Senetas or Gemalto to discuss your needs. Or, if you prefer, your service provider may contact Senetas or Gemalto on your behalf.

## CERTIFIED HIGH-ASSURANCE NETWORK DATA ENCRYPTION

Whatever your Layer 2 Ethernet network security needs, Senetas has a high-assurance solution to suit. They support data network links from modest 10Mbps and 100Mbps to high speed 1Gbps and 10Gbps as well as 10 x 10Gbps and ultra-fast 100Gbps bandwidth.

Certified, scalable, agile and easy to use; Senetas high-assurance encryptors provide maximum data security without compromising network performance.


## SENETAS CORPORATION LIMITED

**E** info@senetas.com
**www.senetas.com**


Senetas manufactures high-assurance Layer 2 Metro Area and Carrier Ethernet network encryptors. They support all Layer 2 protocols and topologies.

Our multi-certified encryptors are used by some of the world's most secure organisations; including governments and defence forces, commercial and industrial enterprises, Cloud, data centre and telecommunications service providers in more than 40 countries.

SafeNet

SafeNet CN Series Ethernet encryptors

www.gemalto.com

### GEMALTO DISTRIBUTION & SUPPORT

Senetas CN Series certified high-assurance network encryptors are distributed and supported internationally by Gemalto (North America, Europe, Asia, Middle East and Africa) as SafeNet CN Ethernet Encryptors.

MULTIL-CS0617