SENETAS
Security without compromise

INTERNATIONAL BANK CHOOSES HIGH ASSURANCE ENCRYPTORS TO PROTECT GLOBAL WAN

Application of High-Assurance Network Encryption

Sector:	Financial Services
Use Case:	Encrypting customer financial data
Solution:	High-assurance encryption hardware, enhanced with quantum key technologies to provide long-term data protection.

INTERNATIONAL BANK CHOOSES HIGH-ASSURANCE ENCRYPTORS TO PROTECT GLOBAL WAN

An international bank needed to upgrade its Wide Area Network (WAN) encryption solution to enable secure and instant access to customer data from any of its 30+ locations on three continents. The bank implemented Senetas high-assurance network encryptors, providing it with the maximum data protection necessary to maintain cybersecurity compliance and ensure client privacy, without compromising real time access to sensitive data.

The Business Need

The bank wanted to address its commitment to customer confidentiality and increasing regulatory compliance, whilst addressing the demand for real-time data flow more effectively. To do so it required an agile, high-performance solution that was easy to deploy and manage, and with a cost-effective TCO.

The bank's existing solution was a network protocol specific Layer 2 E1/T1 link that could no longer handle the required data throughput. A Layer 3 IPSec solution had been considered previously, but rejected due to its relatively high cost, complexity of deployment and lower throughput performance.

Moreover, as IPSec encryption adds significant bandwidth overhead, the routers fragmented and reassembled the data packets, resulting in technical problems with packet reassembly.

Low latency was essential, as the bank's critical applications demanded near-zero impact on performance.

The Solution

Working closely with its telecommunications service provider, the bank chose Senetas CN Series high-assurance encryption hardware. The chosen solution was developed in collaboration with ID Quantique - a Senetas technology partner and global leader in quantum cryptography for core network infrastructure.

Senetas CN Series encryption hardware is the best choice for the bank's network and security architecture because it provides:

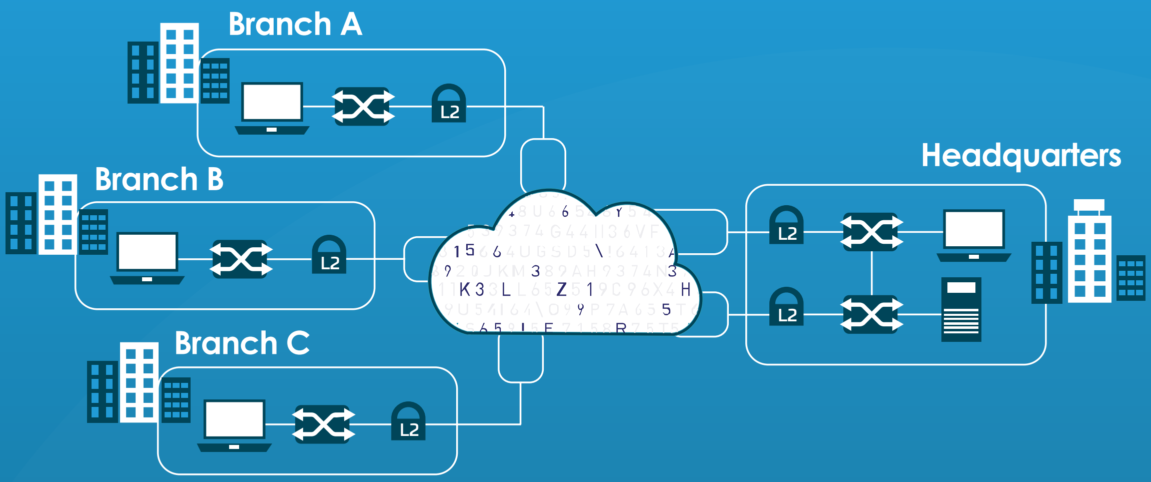
- Efficient, high-performance Field Programmable Gate Array (FPGA) architecture
- Maximum up-time, field-proven and tamper-proof hardware
- Cryptographic agility, including support for both classical and quantum resistant algorithms
- State-of-the-art encryption key management
- Policy based, network independent encryption across Layers 2, 3 and 4.
- Support for point-to-point and multipoint network architectures
- FIPS and Common Criteria security certifications
- True full duplex wire speed encryption up to 10 Gbps
- Low latency under 7.5 microseconds per appliance
- Single, intuitive management interface
- Secure remote management

The Benefits

Following a successful pilot project, the bank deployed the CN Series encryption platform across its global WAN, including over thirty branches on three continents. Redundant devices were used for the hub at the bank headquarters, and other Senetas CN series encryptors were used at the end points in the WAN.

Currently, the branches are using variable speed encryptors, with bandwidths from 100 Mbps to 1 Gbps. This allows the bank flexibility to pay only for the bandwidth used, with the option to upgrade in the future without changing the hardware. The links at the headquarters are 10 Gbps.

THALES IDQ



Customer Requirements

- **High performance** - The Ethernet (Layer 2) network platform provided maximium throughput encryption on the telco's MPLS network, using 100% of the bandwidth with no packet loss in transport mode. Meeting network standards (IEEE 802.1Q) the VLAN was left transparent for the carrier.
- **Near-Zero Latency -** The Senetas CN Series encryption solution provided the low latency crucial for the bank's real time communications and banking applications (Latency was tested at below 7.5 microseconds per encryptor.
- **Designed for security -** Senetas CN Series encryptors are purpose-built security devices. Based on an FPGA platform they are cryptographically agile and certified to Common Criteria and FIPS standards.
- **Multicast -** For VLAN-based multicast traffic, the intelligent group key system uses one encryption key per secured connection. This enables the bank's headquarters to securely videoconference with Branch A and Branch C, without Branch B being able to access the communication.
- **Scalable architecture -** The encryption platform provided enables both security and versatility in a point-to-multipoint architecture. The products support different traffic for varied applications - for example, unicast (standard), multicast (finance information to traders, secure videoconferencing, etc.) or broadcast (automated equipment info exchange, etc.).
- **Intelligent key management –** The architecture of the Intelligent Group Key system also provided a higher level of security in case of partial network failure – essential for global banking operations in countries with variable service level agreements. Providing much greater resilience to common network problems, the keys are generated per secured connection and are renewed up to every 60 seconds. 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.

Challenge

Evolving data network architecture, protocols and bandwidth demands meant the existing encryption solution was no longer fit for purpose. It lacked both the performance and agility necessary to meet the bank's needs.

Solution

Having established the bank's specific performance and security requirements, the joint Senetas / ID Quantique solution was chosen to secure its global WAN (supported in all locations by Thales, Senetas' global distributor).

Benefit

The bank now has state-of-the-art network data encryption security, without compromising the high-performance benefits of its new network architecture. The solution is crypto-agile, ensuring a future-proof, quantum-resistant platform.

- **Management -** The Senetas CM7 encryptor management system provides centralised remote management through a user-friendly graphical user interface using a secure SNMPv3 connection. The bank is now able to monitor real-time status and configuration changes easily. Different levels of user rights within CM7 allow separation of responsibilities between network and security teams, with mission critical functions reserved for the administrator role. The network topology, plus the addition or deletion of encryptors can be managed while the encryptors are still functioning, either in manual or in auto-discovery mode.

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas CN and CV Series encryption solutions are sold by Thales as part of its Cloud Protection and Licensing portfolio.

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers. Visit our **ANZ Partner Page** for full details.

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file-sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** info@senetas-europe.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal encryption solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has an encryption solution to suit. Our certified high-assurance encryptors protect data across networks operating at speeds from 10Mbps to 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 5Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

SECURE FILE SHARING

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Secure File Gateway extension.

DISARM MALICIOUS CONTENT

Votiro leverages patented anti-malware technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.

SENETAS