HIGH-PERFORMANCE IN-FIELD ENCRYPTION FOR A NATIONAL DEFENCE AGENCY

CASE STUDY

Application of High-Assurance Network Encryption	
Sector:	Government & Defence
Use Case:	Securing Layer 2 communications between head office & in-field locations
Solution:	Compact, high-assurance encryptors providing in-field encryption of secure communications across a bespoke platform.

SENETAS

Security without compromise

“Originally a Layer 3 solution, we wanted to eliminate as much encryption overhead and latency as possible. We required a very high-performance solution.”

CUSTOMER CHALLENGE

Our client is a government department responsible for delivering a national defence policy. With offices all over the world, it employs over 60,000 people.

The organisation utilises a custom platform for secure communications between head office and hundreds of in-field locations. The maximum data bandwidth required among the locations is 1Gbps.

With an incumbent Layer 3 (Internet Protocol) encryption solution nearing end-of-life, our client was seeking to upgrade to a Layer 2 (Ethernet) solution to maximise available bandwidth and efficiency and reduce the latency evident in Layer 3 encryption.

SENETAS SOLUTION

Senetas CN4010 (x202) compact, high-assurance encryptors to provide in-field encryption of secure communications across a bespoke platform.

Security Management Centre (SMC) was used to provide centralised encryptor management.

“The Security Management Centre was a significant step forward in terms of centralised network encryption management for us.”

DEPLOYING HIGH-ASSURANCE ENCRYPTION

Having mandated an upgrade from Layer 3 to Layer 2 communications, our client was seeking to make the most of all available bandwidth by significantly reducing encryption latency and data overheads.

The nature of the organisation, its operations and its encrypted network communications objectives emphasised the importance of the solution’s performance, simplicity, ease of integration and even physical size.

A compact form factor was required to facilitate the encryption of secure in-field communications. The encryptors would not necessarily be located in conventional server racks.

Our client required a high-assurance solution. New encryption hardware needed to be tamper-proof and had to work with the custom platform “out of the box” (vendor agnostic).

Due to the nature of the data transported among the network links, end-to-end encryption and secure key management were essential requirements.

Importantly, the new solution required FIPS certification to meet government and defence use security requirements.

Having met all the client’s security and hardware requirements, proven near-zero latency and data overheads performance requirements were validated.

The FIPS, Common Criteria and NATO certified Senetas CN4000 Series small form factor encryptors were an obvious client choice, meeting all requirements, straight out of the box.

“FIPS certification was an absolute must. The nature of our communications mandates validation by a recognised third-party testing authority.”

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales and within government & defence sectors by Thales Defense & Security Inc.

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas products are sold by Thales under its SafeNet brand.

THALES

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; including:

ADVA Optical Networking	AUCLOUD	Data#3
DATACOM	dimension data	DXC
IBM	macquarie GOVERNMENT	VOCUS communications

© SENETAS CORPORATION LIMITED

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 35 countries.

From certified high-assurance hardware and virtualised encryption, to secure file sharing 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 modest 10Mbps to ultra-fast 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 Disarmer extension.

DISARM MALICIOUS CONTENT

Votiro Disarmer leverages patented Content Disarm & Reconstruction (CDR) 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