SENETAS
Security without compromise

CN9000 SERIES ENCRYPTION HARDWARE

Multi-Certified. High-Assurance. Crypto-Agile

SENETAS
Security without compromise

SENETAS CN9000 SERIES ENCRYPTORS

ULTRA-FAST, MISSION CRITICAL, 100GBPS ENCRYPTION

The evolution of 100Gbps links and networks reflect the exponential growth in volume and types of data generated by business applications and the Internet of Things. Big Data is rapidly becoming 'Mega Data' and high-speed networks are becoming ultra-fast.

The CN9100 is the world's first commercially available certified high-assurance 100Gbps Ethernet network encryptor that supports all Layer 2 network topologies.

Why Senetas CN9000 Encryptors

Certified, best 100Gbps network performance and data protection with ultra-low latency of <2 micro-seconds:

- the only defence-grade >100Gbps Ethernet encryption that supports all topolgies
- secure data transmission across Layer 2 Ethernet networks
- FIPS and Common Criteria Certified
- excellent total cost of ownership and ROI
- near-zero latency (at <1.5 microseconds in customer environments)
- zero network impact
- maximum bandwidth
- minimum overheads
- scalable and interoperable
- simple to manage
- maximum availability (99.999% up time)
- store and forward data transmission mode

Field Programmable Gate Array (FPGA) benefits:

- flexibility of FPGA chip tech
- crypto-agile
- advanced customisation
- hardware flexibility not enabled by ASICs

Senetas high-assurance Layer 2 Metro Area and Carrier Ethernet network encryptors protect much of the world's most sensitive data.

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 35 countries.

It is often assumed that data networks are inherently safe. They are not. Data networks are vulnerable to security breaches.

To be protected from a data network breach, cyber-attack, innocent error, or technical failure, your data must be encrypted. Only when encrypted, can data be safe – rendering it useless to unauthorised parties.

Senetas high-assurance network data encryptors are certified by international, independent testing authorities to protect your data when transmitted.

Senetas trusted high speed encryption technology now puts certified defence-grade encryption within easy reach of organisations with entry-level and "encrypt everywhere" requirements. The CN6010 provides all the CN9000 series platform benefits in a cost effective encryptor.

*Refer to detailed certification information at www.senetas.com

Ethernet services

Our CN9000 series platform uniquely provides highly secure, full line rate transparent encryption for data moving across both dark fibre and metro, or wide area Ethernet networks in point-to-point, hub & spoke, or any meshed environment.

The intrinsic key generation and distribution capability in our CN9000 Encryptors removes reliance on external key servers, providing a robust, fault-tolerant security architecture.

The rugged tamper-resistant chassis also gives uncompromising protection to key material held in the encryptor.

Full interoperability with the Senetas CN series encryptors means customers may standardise on one platform to protect transmitted data across large hub and spoke or meshed networks, among locations.

Network and management

Senetas CM7 management software provides simple, secure remote management either out-of-band – using a dedicated Ethernet management interface – or in-band, using the encrypted Ethernet port.

Local management using a command line interface is available via a serial console connector.

Optical interfaces allow operation over single mode fibre, multi-mode fibre or over WDM services by choosing an appropriate wavelength.

Senetas CN platform

The CN9000 series leads Senetas's commitment to robust and multi-certified high-assurance encryption.

For customers with more modest data network and transmission requirements, the CN4000 and CN6000 series provide solutions for 10Mbps to 1Gbps and 10Gbps; based on the same, trusted CN Series platform.

Certifications

Government and commercial customers benefit from the Senetas CN9000 series international, independent testing authority certifications.

- Common Criteria EAL 2+ / 4+
- FIPS 140-2 Level 3

Optical Interfaces

Extensive network interface testing, including customer PoCs, have been conducted to ensure the optimal CN9100 and CN9120 100Gbps performance.

Each test involved network interfaces to encrypt at full line rates of 100Gbps across WANs (up to 40km) and MANs (up to 80km) using optical CFP4 and QSFP28 interfaces respectively. Senetas has adopted the Inphi ColorZ interface for longer range use (up to 80km) due to its tested performance capabilities and features.

Customers with longer range MAN requirements (up to 80km) should note that additional network items may be required. For more information please contact Senetas or an approved, qualified service provider.

CN9100 Rack Mounted 1u Carrier Grade 1000Gbps Certified Encryptor

WHAT MAKES CN SERIES ENCRYPTORS STAND OUT?

Performance

High Speed

Market-leading performance. Operating anywhere from 10Mbps or 100Gbps, Senetas encryptors consistently win competitive performance test.

Low Latency

Operating in full duplex mode, at full line speed, without packet loss. Latency is as low as 2 microseconds per unit at 100Gbps.

Zero Impact

The zero impact of Senetas encryptors is not limited to network bandwidth and latency; it extends to network operations and management.

Security

Certification

For over 20 years, Senetas R&D has remained committed to the principle of certification in depth. Senetas CN Series encryptors are certified by: FIPS, Common Criteria and NATO.

Key Management

All CN Series encryptors feature state-of-the-art encryption key management. Keys are securely stored and encrypted, and only accessible by you.

Solution Integrity

Senetas high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption.

Versatility

Crypto Agility

All Senetas encryptors are 'crypto-agile'; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility.

Topology Support

Senetas CN encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies.

Flexible Management

Configuration may be performed locally or remotely through the intuitive Senetas CM7 management software.

Efficiency

Cost Effectiveness

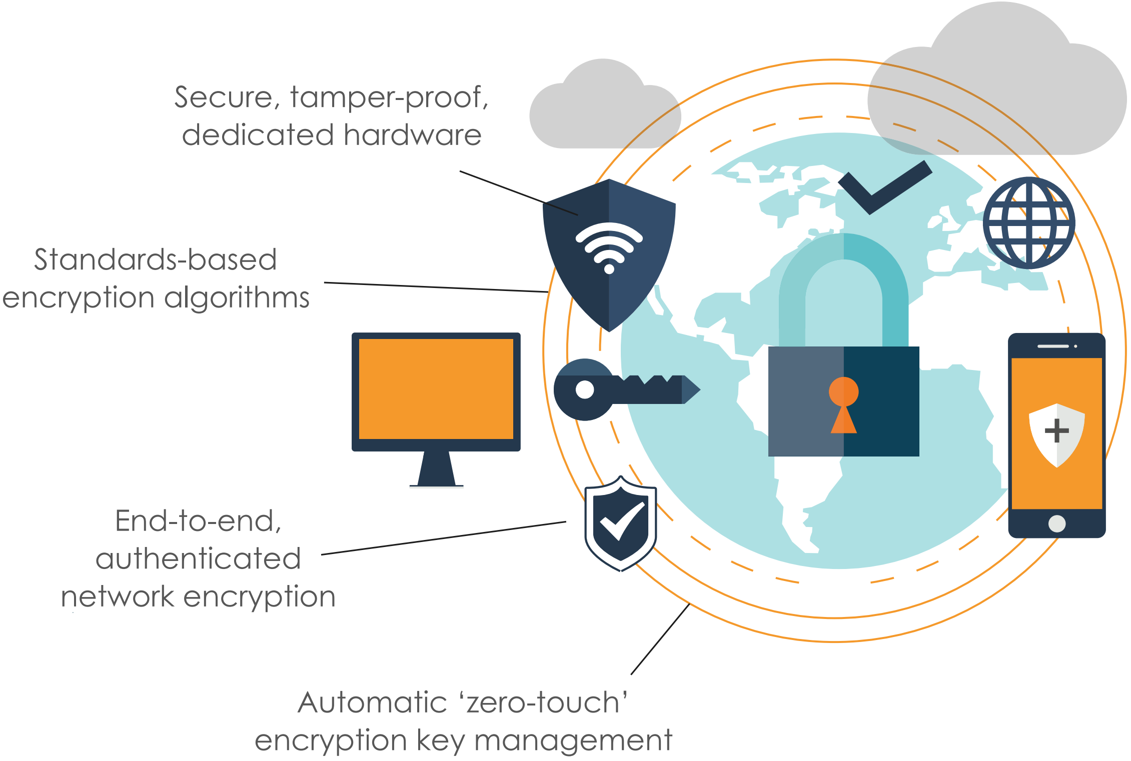
Senetas encryptors provide excellent TCO through a mix of network bandwidth savings, ease of management and longevity.

Reliability

All carrier-grade Senetas encryptors are hot-swappable, feature dual redundancy and deliver 99.999% uptime.

Flexibility

Use of FPGA technology enables maximum operational flexibility, including use of custom encryption and in-field upgradability.


Secure, tamper-proof, dedicated hardware
Standards-based encryption algorithms
End-to-end, authenticated network encryption
Automatic 'zero-touch' encryption key management

High-Assurance Encryption

As recommended by leading data security and encryption analysts; for a network encryption solution to be truly robust, and provide long-term data protection (well beyond the useful life of the data), it must be a high-assurance solution.

Not all encryption solutions are created equal. So-called 'hybrid' encryption devices – such as network routers/switches with embedded encryption or those using MACSec or similar standards (not originally intended for WAN and MAN security) provide low assurance data protection.

By contrast, Senetas CN Series encryption solutions are certified by the world's leading independent testing authorities as suitable for government and defence applications. They are purpose-engineered for dedicated, high-assurance network data security.

Senetas CN Series encryptors' security credentials include all four essential high-assurance features:

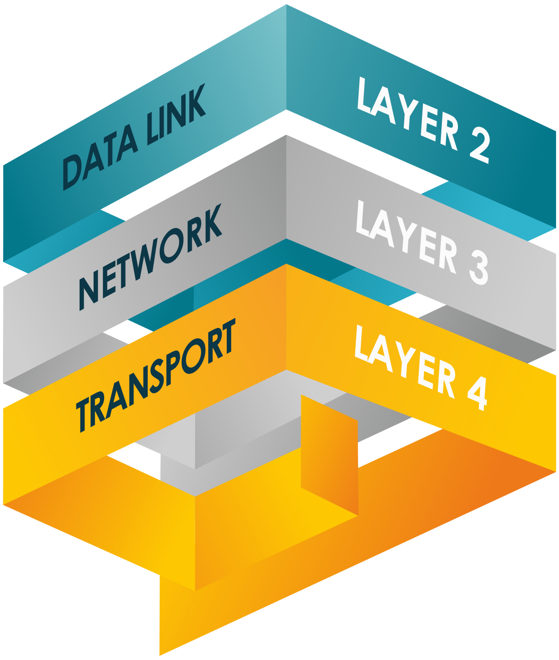
- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art, client-side, zero-touch encryption key management
- End-to-end, authenticated encryption
- Use of standards-based encryption algorithms

Network Independent Encryption

Many organisations utilise multiple data network Layer protocols (Layer 2, 3 and 4) to help deliver their business applications and communications services. Recognising this, Senetas has designed-in Network Independent Encryption.

This advanced, network Layer agnostic encryption technology enables destination policy-based, concurrent multi-Layer encryption.

Significantly, customers are still assured of strong, end-to-end encryption as the protected data traverses the various network Layers, for example: from Layer 2 Ethernet to Layer 3 IP network destination.



SENETAS CN9000 SERIES

Model	CN9100	CN9120
Network Protocols Supported	**ETHERNET**	**ETHERNET**
Protocols and Connectivity		
Support for all Ethernet network topologies	✓	✓
Maximum speed	100Gbps	100Gbps
Support for jumbo frames	✓	✓
Protocol and application transparent	✓	✓
Encrypts Unicast, Multicast and Broadcast traffic	✓	✓
Automatic network discovery and connection establishment	✓	✓
Network and Local Interface – SR4, LR4, ER4(lite) links (up to 40km)	CFP4	QSFP28
Network Interface MAN – Inphi ColorZ - links (up to 80km)^	-	QSFP28
Security		
Tamper resistant and evident enclosure	✓	✓
Anti-probing barriers	✓	✓
Flexible encryption policy engine	✓	✓
Robust AES encryption algorithm	✓	✓
Per packet confidentiality and integrity with AES-GCM encryption	✓	✓
Automatic, zero-touch key management	✓	✓
Encryption and Policy		
AES 128 or 256 bit keys	128/256	128/256
Policy based on VLAN ID	✓	✓
Encryption modes	GCM*, CTR	GCM*, CTR
Self healing key management	✓	✓
Certifications		
Common Criteria EAL 2+	✓	✓
FIPS 140-2 Level 3	✓	✓
Performance		
Low overhead full duplex line-rate encryption	✓	✓
FPGA based cut-through architecture	✓	✓
'Store and forward' data transmission mode support	-	-
Ultra low latency for high performance	✓	✓
Latency (μs per encryptor)	< 2	< 2
Management		
Central config. and management using CM7 and SNMPv3	✓	✓
SNMPv1/2 monitoring (read-only)	✓	✓
Certificate signing	RSA, EC	RSA, EC
Support for external (X.509v3) CAs	✓	✓
Remote management using SNMPv3 (in-band and out-of-band)	✓	✓
NTP (time server) support	✓	✓
CRL and OCSP (certificate) server support	✓	✓

Model	CN9100	CN9120
Network Protocols Supported	**ETHERNET**	**ETHERNET**
Maintainability/ Interoperability		
In-field firmware upgrades	✓	✓
Dual swappable AC and/or DC power supply	✓	✓
Fan cooled	✓	✓
User replaceable fans and batteries	✓	✓
Fully interoperable with all CN models	✓	✓
Physical and Installation		
Form factor	1U rack mount	1U rack mount
Physical dimensions (mm) W / D / H	435 / 480 / 43	435 / 480 / 43
Weight	8kg	8kg
Power source	AC/DC	AC/DC
Power input rating	100-240V AC, 50/60Hz, 2A or 40.5-60V DC 4A	100-240V AC, 50/60Hz, 2A or 40.5-60V DC 4A
Power consumption at highest data rate	80W	80W
Environment, Regulatory and Safety		
RoHS compliant	✓	✓
Maximum operating temperature	0-80% RH at 40°C	0-80% RH at 40°C
Safety standards	EN 60950-1 (CE) IEC 60950-1 AS/NZS 60950.1	EN 60950-1 (CE) IEC 60950-1 AS/NZS 60950.1
UL listed	✓	✓
FCC Part 15 / CISPR 32 / EN 55032 Emissions	Class B	Class B

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 products are sold by Thales under its brand.

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.

© 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 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 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.