SENETAS

Security without compromise

SENETAS CN SERIES HIGH-ASSURANCE ENCRYPTORS

FEATURES AND SPECFICATION GUIDE

AN INTRODUCTION TO SENETAS CERTIFIED HIGH-ASSURANCE CN SERIES ENCRYPTORS

Since the turn of the millennium, data breaches have become increasingly commonplace, with an average of 4.5 million records lost or stolen every day.

Recent increases in high-profile data breaches and the emergence of new, tougher, data protection legislation have brought the need to encrypt data in motion to everyone's attention.

However, Senetas encryptors have been used to secure much of the world's most sensitive data for more than 20 years.

Senetas high-assurance encryptors are certified by the leading independent certification authorities (Common Criteria, FIPS and NATO) as suitable for government and defence use.

They are trusted to protect network-transmitted data in more than 40 countries. Applications include: cloud and data centre services, government information and secrets, commercially sensitive data, intellectual property, defence and military information, business and financial data, banking transactions, CCTV networks and more.

Not all encryption is the same. Truly robust network data encryption solutions feature high-assurance credentials, are independently certified and are crypto-agile by design.

Multi-certified

Independent security certification provides government and non-government customers with full confidence in their chosen solution. Senetas CN Series encryptors are certified by multiple testing authorities as suitable for government and defence use.

- FIPS 140-2 level 3
- Common Criteria EAL 2+/4+
- NATO Restricted Green

As governments typically mandate the use of certified security solutions, commercial organisations seeking to work with them must meet the same exacting standards.

High-Assurance

High-assurance network data encryption features four key elements:

Dedicated encryption hardware

Secure, tamper-proof hardware, dedicated to encryption only.

State-of-the-art encryption key management

Encryption keys themselves should be encrypted, stored in a secure device and accessible only to the customer; regardless of data and key storage methods.

Authenticated, end-to-end data encryption

The encryption process must start and end behind the network itself, to ensure that no unencrypted data is exposed during transit.

Standards-based encryption

The encryption model must be based on validated standards (e.g. AES 256) and the encryption process must include authentication.

Crypto-Agile

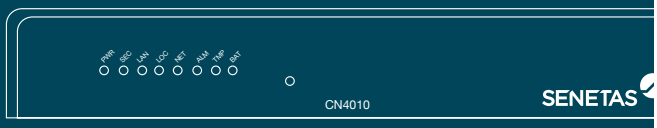
Cryptographic protocols and algorithms evolve over time to counter new security threats. That's why Senetas encryptors are designed to be "crypto-agile" out of the box. They provide extra assurance that your investment keeps pace with cryptographic advances.

Key components of agility include support for:

- AES 128 and 256bit algorithms
- Custom curves and BYO entropy
- Quantum Key Distribution (QKD)
- CFB, CTR and GCM encryption modes
- Network Independent Encryption
- Self-Healing Key Management

CN4000 SERIES ENCRYPTORS

- Compact, encrypt anywhere device
- 10Mbps to 1Gbps

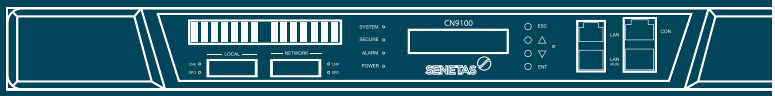


CN6000 SERIES ENCRYPTORS

- Rack mounted, carrier-grade device
- 1GBps to 10Gbps

CN9000 SERIES ENCRYPTORS

- Supports big data applications across all topologies
- Ultra-fast 100Gbps



THE SENETAS CN SERIES PLATFORM

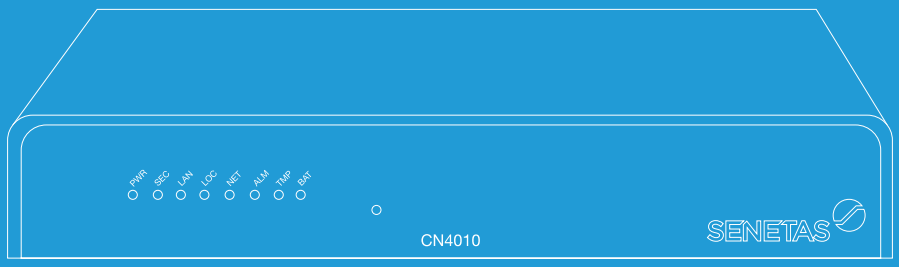
High-Assurance

Multi-Certified

Crypto-Agile

SENETAS CN4000 SERIES

MULTI-CERTIFIED | HIGH-ASSURANCE | CRYPTO-AGILE



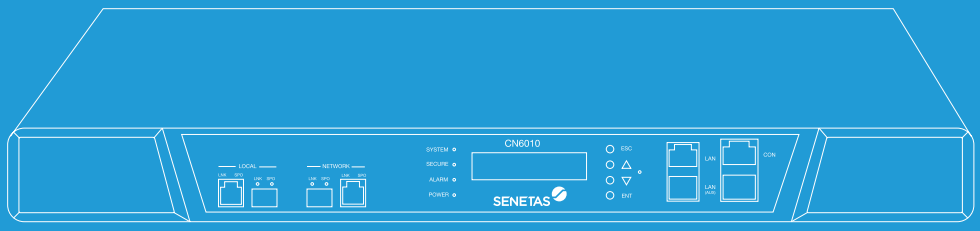
Compact, Cost-Effective 10Mbps-1Gbps Encryption

Model	CN4010	CN4020
Network Protocols Supported	**ETHERNET**	**ETHERNET**
Protocols and Connectivity		
Support for all Ethernet network topologies	✓	✓
Physical encryption channels	1	1
Maximum speed	1Gbps	1Gbps
Link/rate limiting	✓	✓
Support for jumbo frames	✓	✓
Protocol and application transparent	✓	✓
Encrypts unicast, multicast and broadcast traffic	✓	✓
Automatic network discovery and connection establishment	✓	✓
Network interfaces (optional SFP to RJ45 adapter available)	RJ45	SFP, SFP+
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	✓	✓
Traffic flow analysis protection (TRANSEC)	✓	✓
Encryption and Policy		
AES 128 or 256 bit keys	128/256	128/256
Policy based on MAC address or VLAN ID	✓	✓
Encryption modes	CFB, CTR, GCM	CFB, CTR, GCM
Self-healing key management	✓	✓

Model	CN4010	CN4020
Network Protocols Supported	**ETHERNET**	**ETHERNET**
Certifications		
Common Criteria	✓	✓
FIPS	✓	✓
NATO	✓	✓
Performance		
Low overhead full duplex line-rate encryption	✓	✓
FPGA based cut-through architecture	✓	✓
Ultra low-latency for high performance	✓	✓
Latency (µs per encryptor) - microseconds	<10 @ 1Gbps <50 @ 100Mbps <650 @ 10Mbps	<10 @ 1Gbps <50 @ 100Mbps <650 @ 10Mbps
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 (inband and out-of-band)	✓	✓
NTP (time server) support	✓	✓
CRL and OCSP(certificate) server support	✓	✓
Maintainability/ Interoperability		
In-field firmware upgrades	✓	✓
Fan cooled	-	✓
Fully interoperable with all CN models	✓	✓
Physical and Installation		
Form factor (optional rack-mount kit available)	Desktop	Desktop
Physical dimensions (mm) W / D / H	180 / 126 / 32	180 / 126 / 32
Weight	500g	500g
Power source	AC plug pack	AC plug pack
Power input rating	9-15V DC, 1.0A (DC input) 100-240V AC, 0.7A (AC input)	12V DC, 1.0A (DC input) 100-240V AC, 0.7A (AC input)
Power consumption at highest data rate	6W at DC input 10W at AC input	7W at DC input 11W at AC input
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) UL / IEC 60950-1 AS/NZS 60950.1	EN 60950-1 (CE) UL / IEC 60950-1 AS/NZS 60950.1
UL listed	✓	✓
FCC Part 15 / CISPR 32 / EN 55032 Emissions	Class B	Class B

SENETAS CN6000 SERIES

MULTI-CERTIFIED | HIGH-ASSURANCE | CRYPTO-AGILE



Rack-Mounted, Carrier-Grade 1-10Gbps Encryption

Model	CN6010	CN6100	CN6140	
Network Protocols Supported	**ETHERNET**	**ETHERNET**	**ETHERNET (SINGLE)**	**ETHERNET (MULTI)**
Protocols and Connectivity				
Support for all Ethernet network topologies	✓	✓	✓	✓
Maximum speed	1Gbps	10Gbps	10Gbps	4 x 10Gbps
Link/rate limiting	✓	✓	✓	✓
Support for jumbo frames	✓	✓	✓	✓
Protocol and application transparent	✓	✓	✓	✓
Encrypts unicast, multicast and broadcast traffic	✓	✓	✓	✓
Automatic network discovery and connection establishment	✓	✓	✓	✓
Network interfaces	RJ45, SFP	XFP	SFP, SFP+	SFP, SFP+
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	✓	✓	✓	@1Gbps only
Automatic, zero-touch key management	✓	✓	✓	✓
Traffic flow security (TRANSEC)	✓	✓	✓	✓
Encryption and Policy				
AES 128 or 256 bit keys	128/256	128/256	128/256	128/256
Policy based on MAC address or VLAN ID	✓	✓	✓	✓
Encryption modes	GCM, CFB, CTR	GCM, CFB, CTR	GCM, CFB, CTR	GCM, CFB, CTR
Self-healing key management	✓	✓	✓	✓

Model	CN6010	CN6100	CN6140	
Network Protocols Supported	**ETHERNET**	**ETHERNET**	**ETHERNET (SINGLE)**	**ETHERNET (MULTI)**
Certifications				
Common Criteria EAL2+ EAL4+	✓	✓	✓	✓
FIPS 140-2 Level 3	✓	✓	✓	✓
NATO	✓	✓	✓	✓
Performance				
Low-overhead full duplex line-rate encryption	✓	✓	✓	✓
FPGA-based cut-through architecture	✓	✓	✓	✓
Ultra low latency for high performance	✓	✓	✓	✓
Latency (µs per encryptor)	< 10 @ 1Gbps	< 5 @ 10Gbps	< 5 @ 10Gbps	< 5 @ 10Gbps
Management				
Config & management via CM7 and SNMPv3	✓	✓	✓	✓
SNMPv1/2 monitoring (read-only)	✓	✓	✓	✓
Certificate signing	RSA, EC	RSA, EC	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	✓	✓	✓	✓
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	1U rack mount	1U rack mount
Physical dimensions (mm) W / D / H	435/329/43	435/329/43	435/329/43	435/329/43
Weight	8.5kg	8.5kg	8.5kg	8.5kg
Power source	Mains	Mains	Mains	Mains
Power input rating	100-240V AC, 50/60Hz, 0.6A or 40.5-60V DC, 1A	100-240V AC, 50/60Hz, 1.5A or 40.5-60V DC, 2A	100-240V AC, 50/60Hz, 1.5A or 40.5-60V DC, 2A	100-240V AC, 50/60Hz, 1.5A or 40.5-60V DC, 2A
Power consumption at highest data rate	18W	50W	22W	49W
Environment, Regulatory and Safety				
RoHS compliant	✓	✓	✓	✓
Maximum operating temperature	0-80% RH at 50°C	0-80% RH at 50°C	0-80% RH at 40°C	0-80% RH at 40°C
Safety standards	EN 60950-1 (CE) UL / IEC 60950-1 AS/NZS 60950.1	EN 60950-1 (CE) UL / IEC 60950-1 AS/NZS 60950.1	N 60950-1 (CE) IEC 60950-1 AS/ NZS 60950.1	N 60950-1 (CE) IEC 60950-1 AS/ NZS 60950.1
UL listed	✓	✓	✓	✓

SENETAS CN9000 SERIES

MULTI-CERTIFIED | HIGH-ASSURANCE | CRYPTO-AGILE

Ultra-Fast, Mission-Critical, 100Gbps Encryption

Model	CN9120
Network Protocols Supported	**ETHERNET**
Protocols and Connectivity	
Support for all Ethernet network topologies	✓
Maximum speed	100Gbps
Support for jumbo frames	✓
Protocol and application transparent	✓
Encrypts Unicast, Multicast and Broadcast traffic	✓
Automatic network discovery and connection establishment	✓
Network interface	QSFP28
Link distance of available optical transceiver	up to 80km
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
Policy based on VLAN ID	✓
Encryption modes	GCM*, CTR
Self-healing key management	✓

*Firmware upgrade pending

Model	CN9120
Network Protocols Supported	**ETHERNET**
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 encryption channel) - microseconds	< 2
Management	
Central config. and management using CM7 and SNMPv3	✓
SNMPv1/2 monitoring (read-only)	✓
Certificate signing	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	✓
Maintainability/ Interoperability	
In-field firmware upgrades	✓
Dual swappable AC and/or DC power supply	✓
Fan cooled	✓
User-replaceable fans	✓
Fully interoperable with all CN models	✓
Physical and Installation	
Form factor	1U rack mount
Physical dimensions (mm) W / D / H	435 / 480 / 43
Weight	8kg
Power source	AC/DC
Power input rating	100-240V AC, 50/60Hz, 2A or 40.5-60V DC, 4.5A
Power consumption at highest data rate	80W
Environment, Regulatory and Safety	
RoHS compliant	✓
Maximum operating temperature	0-80% RH at 40°C
Safety standards	EN 60950-1 (CE) IEC 60950-1 AS/NZS 60950.1
UL listed	✓
FCC Part 15 / CISPR 32 / EN 55032 Emissions	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.

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.

HSE-BR0121

SENETAS