SENETAS

Security without compromise

CERTIFIED HIGH-ASSURANCE NETWORK ENCRYPTION

TECHNICAL PAPER

A COMMITMENT TO INDEPENDENT CERTIFICATION; IF FURTHER ASSURANCE WERE NEEDED

Why is product certification Important?

Certification by internationally recognised testing authorities provides both government and commercial customers with additional peace of mind. Expert, independent validation that Senetas encryptors provide maximum data protection is another key component of Senetas certified high-assurance security.

Compliance with these international certification standards is a strict requirement for many governments and defence agencies when it comes to the protection of sensitive data. The need to comply with high assurance standards often also extends to third parties wishing to provide services to government and defence agencies.

Security product certifications involve rigorous testing procedures, which often take years to be completed. It is not a one-time process; but typically an on-going assessment, where even the smallest change to the product requires a process of 're-certification'.

These certifications ensure that products are "suitable for government and defence use". Classification within the certification process determines the level of data sensitivity for which the product is suitable – including "confidential" and "secret" information.

Many commercial enterprises reference these government standards for their own encryption solutions, especially if they are part of the government supply chain. Products without the appropriate certifications are not permitted to be installed in government or government service provider networks.

Independent certification is a valuable indicator of both security and performance. That's why Senetas has always ben 100% committed to certification.

Certification in-depth

Since developing the first CN encryptor, Senetas has chosen to differentiate its products through certifications. Multiple certifications form a key part of the 'certified high-assurance' promise you get from Senetas CN series encryptors.

We call this commitment 'certification in-depth'. Having developed R&D expertise in the security standards and testing requirements, certifications are a cornerstone of Senetas hardware encryption design and development.

Senetas encryptors are certified by not one, but three leading testing authorities:

- Common Criteria (International)
    - EAL2+ EAL4+
- FIPS (USA)
- Theft of intellectual property
    - 140-2 Level 3
- NATO (Member States)
    - Restricted/Green

Network independent encryption

Senetas hardware has set the standard for secure Layer 2 encryption for many years. However, as networks have evolved to become increasingly virtualised and borderless, there is greater demand to add encryption security at Layers 3 and 4.

Senetas provides a range of end-to-end encryption solutions that are interoperable and support all topologies; providing organisation-wide data protection.

In 2018 Senetas introduced the concept of concurrent, policy-based Network Independent Encryption to meet the evolving needs of today's multi-Layer networks.

AN EVOLVING THREAT LANDSCAPE HIGHLIGHTS THE NEED FOR HIGH-ASSURANCE ENCRYPTION

The controversial revelations of multiple, high-profile network data breaches have brought the need to encrypt data in motion to everyone's attention.

However, not all encryption solutions are the same. The most robust network data encryption solutions are referred to as high-assurance. Those that fail to meet this standard are referred to as low-assurance (or no-assurance).

What does high-assurance look like?

There are four key criteria that need to be met if a solution is to be classed as high-assurance:

Dedicated encryption hardware

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

State-of-the-art encryption key management

Encryption Key Management must be 'client-side', in that the keys are encrypted, stored in a secure device and only accessible to the customer; regardless of the data storage and key storage methods.

Gapless, end-to-end data encryption

The encryption process/methodology must start and end behind the network itself, to ensure that no unencrypted data has begun or ended its journey.

This is also essential to protect data from vulnerable devices such as routers and switches

Authenticated, standards based encryption

The encryption model must be based on validated standards (e.g. AES256) and the encryption process must include authentication.

Traps for the trusting

Customers seeking maximum data security and maximum network performance are well advised to examine alternative solutions' level of assurance.

Weaknesses in any of the high-assurance criteria expose the data to successful cyber-attack.

Analysts warn that in this information era of Big Data, Cloud Computing and data centre connectivity; there is no room for under investment in data security or the adoption of a simple tick-box approach.

The transmission of high data volumes is what first gets cyber-criminals' and cyber-terrorists' attention. They adopt a business-like Return on Investment (ROI) approach to their attacks.

Senetas encryptors are certified by not one, but three leading testing authorities.

- Common Criteria (international)
- FIPS (USA)
- NATO (all member states)

Certification. Your assurance, our commitment.

Independent certification involves years of rigorous testing by the testing authorities' own labs. Senetas CN encryptors are certified as "suitable for government and defence use".

Products without these certifications are unable to be installed in the respective government and government service provider data networks.

Senetas encryptors provide our customers with the best assurance that their transmitted data is protected according the rigorous, defence-grade standards required.

Despite our encryptors' certifications, some government, defence and commercial customers have undertaken their own "proof of concept" and benchmarking testing. In every case, Senetas encryptors have excelled.

Encryption without compromise

Senetas customers are seeking to protect data transmitted across Layer 2 network links for a wide range of applications: Cloud computing, remote data centre services, information-rich Big Data, CCTV traffic or infrastructure and industrial process and control systems.

Independent testing authorities' certifications are valuable security and performance assurance. That is why Senetas has always been 100% committed to testing authorities' certifications.

Senetas encryptors' leading features and benefits (combined with our commitment to research development and independent testing authority certification) provide organisations and their stakeholders with long-term peace of mind.

WHAT MAKES SENETAS STAND OUT?

Best Performance

High-speed

The designed-in, market-leading performance capabilities of Senetas encryption solutions are what make them stand out from the crowd.

Whether operating at 10Mbps, 100Mbps, 1Gbps, 10Gbps or 100Gbps; time after time, they consistently win competitive performance tests.

Their encryption speeds, near-zero data overhead and near-zero latency make Senetas encryption solutions ideally suited to the most demanding network environments.

Ultra-low latency

Senetas high-speed encryption solutions operate in full duplex mode at full line speed 99.99% without loss of packets.

Latency is not affected by packet size (<2 microseconds per unit at 100Gbps) meaning maximum throughput with near zero protocol overhead.

Importantly, by using Field Programmable Gate Array (FPGA) technology, this outstanding performance is predictable and dependable.

Zero impact

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

They simply fit in within the user network. They don't require changes to other devices or network reorganisation; making them a favourite among network engineers.

High-Assurance

Certification in-depth

Senetas CN Series encryptors include the only multi-certified products of their types, as a result they are trusted by governments and defence forces around the world.

Rigorous testing is carried out over many years and provides our government and commercial customers with maximum confidence. Senetas CN Series encryption solutions are certified by: FIPS, Common Criteria and NATO.

For over 20 years, Senetas R&D has included a commitment to 'certification in depth'. Customers value the benefits of exhaustive and ongoing testing authorities' product evaluation.

Best encryption key management

All Senetas products adopt state-of-the-art encryption key management. Your encryption keys are only ever held by and accessible to you, on your premises; securely stored and encrypted.

Solution integrity

Senetas encryptors provide maximum solution integrity; unlike 'low assurance' solutions, such as router-based network data encryption or multi-function devices with embedded encryption.

Senetas high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption with standards-based (AES256) encryption algorithms.

* As surveyed in 2014 and 2015, Senetas hardware was on-site engineers' preferred hardware.

Versatile & Simple

Crypto-agility

All Senetas encryption solutions are agile by design; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility.

Selected Senetas encryptors also support Quantum Key Distribution (Quantum Cryptography) and Quantum Random Number Generation, for long-term data security.

Support for all topologies

Senetas CN series encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies. Senetas CN9000 encryptors are the only 100Gbps encryptors that support multipoint-to-multipoint topologies.

Custom encryption

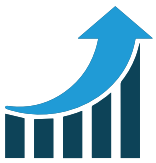
In addition to the standards-based AES256 and 128-bit algorithms, Senetas CN series encryptors support the use of customer-requested algorithms, custom curves (BYOC) and entropy (BYOE).

Ease of use

Set and forget simplicity and network transparency are underlying Senetas design themes. They ensure ease of implementation, operation and management. All Senetas encryption solutions feature automatic zero-touch key management. They also feature automatic network discovery and connection.

Local or centralised management

Configuration may be performed locally or remotely through the intuitive Senetas CM7 management software; which acts as the Certificate Authority in a network of encryptors by signing and distributing X.509 certificates.



Low Cost, High Efficiency

Suitability

All Senetas CN Series solutions operate at full line speed; enable maximum network performance and deliver 'set and forget' management simplicity.

The business investment case out-performs even 'cheap and cheerful' low-assurance solutions that prove very costly over time.

It is not necessary, nor beneficial, to opt for low-cost, low-assurance solutions to meet the toughest business case and TCO requirements.

Cost-efficiency

Senetas encryption solutions provide excellent TCO through a mix of network bandwidth savings, ease of management and reliability.

Longevity, interoperability, backward compatibility, minimal installation and management costs and solution flexibility all contribute to a rapid ROI.

Other cost benefits include, low power consumption minimal rack space use and combined rack space/ power utilisation efficiency.

Reliability

All Senetas hardware encryption solutions boast 99.999% uptime. Carrier-grade, rack mounted devices are hot-swappable and provide further network operations uptime benefits thanks to dual redundancy of consumables, such as fans and power supplies.

Flexibility

The use of FPGA technology enables maximum operational flexibility. This enables on-going operational simplicity, such as infield upgradability, as customers' requirements change; helping to protect their investment in technology.

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

SENETAS CN6000 SERIES

Model	CN6010	CN6100	CN6140	
Network Protocols Supported	**ETHERNET**	**ETHERNET**	**ETHERNET (SINGLE)**	**ETHERNET (MULTI)**
Protocols and Connectivity				
Network topologies	All	All	All	All
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 256bit 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)**
Management				
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	35/329/43	35/329/43
Weight	8.5kg	8.5kg	8.5kg	8.5kg
Power source	Mains	Mains	Mains	Mains
Power input rating	100-240 VAC, 50/60 Hz, 0.6 A or 40.5-60 VDC, 1.0 A	100-240V AC, 50/60 Hz, 1.5A or 40.5-60V DC, 2A	100-240 VAC, 50/60 Hz, 1.5 A or 40.5-60 VDC, 2.0 A	100-240 VAC, 50/60 Hz, 1.5 A or 40.5-60 VDC, 2.0 A
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 CN4000 SERIES

Model	CN4010	CN4020
Network Protocols Supported	**ETHERNET**	**ETHERNET**
Protocols and Connectivity		
Ethernet all 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 256bit 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	✓	✓

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)	<10 @ 1Gbps <50 @ 100Mbps <650 @ 10Mbps	<10 @ 1Gbps <50 @ 100Mbps <650 @ 10Mbps

Model	CN4010	CN4020
Network Protocols Supported	**ETHERNET**	**ETHERNET**
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	9-15 VDC, 1.0 A at DC input 100-240 VAC, 0.7 at AC input	12 VDC, 1.0 A at DC input 100-240 VAC, 0.7 at 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

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 or secure file sharing and collaboration 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 cybersecurity 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.

NETWORK DATA SECURITY WITHOUT COMPROMISE

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

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 15Gbps. 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.

They are trusted to protect much of the world's most sensitive government, defence and commercial data.

SECURE COLLABORATION

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 Secure File Gateway 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