

CERTIFIED HIGH-ASSURANCE NETWORK ENCRYPTION FOR THE GAMING SECTOR



WHO SHOULD READ THIS DOCUMENT

Layer 2 Data Networks Managers and Support staff, Data Network Architects, Data Security Managers and staff, Chief Information Security Officers, Chief Information Officers and Data Security Procurement Staff.



KEYWORDS

Layer 2 Data Networks, Network Data Encryption Hardware, High Speed Data Networks, Network Data security, Encryption Data Security, Network Data Encryption, Certified Layer 2 Network Encryptors, High-Assurance Network Encryptors, 10Mbps, 100Mbps, 1Gbps, 10Gbps and 100Gbps Data Encryptors. Casino Gaming and Wagering Data Security. CCTV Big Data Cloud and Data Centre Networks Data Security.

Big Data, HD CCTV, Cloud and Data Centre Services have become key technologies within the gaming industry.

OVERVIEW

The gaming industry (including casinos, manufacturers of gaming technology, lottery operators and sports betting companies) has become increasingly dependent upon CCTV, Big Data Applications, Cloud and Data Centre Services.

High speed network-delivered services not only enable the gaming industry to maximise financial and operational efficiencies, they also support regulatory control and compliance.

However, because of the potential for significant financial gain, the gaming industry is a high-risk, high-profile target for cyber-criminals.

In a big-data world, the information exchanged across an organisation's high speed networks is often of a sensitive nature.

The security and integrity of this data is essential, whatever its use:

- > Personal safety
- > Regulatory compliance
- > Operational standards
- > Asset protection
- > Business analytics
- > Financial transactions

Whatever the application, from HD CCTV to big data analytics, networks require high-assurance data encryption security and maximum network performance.

Where the gaming industry differs from other commercial sectors is its dependence upon:

- > Real-time data availability
- > 100% data integrity
- > High-definition video
- > Ultra-high speed network performance
- > Unified data, video and voice



CCTV ENCRYPTION

Robust encryption security and high speed data network performance are both essential to real-time HD CCTV monitoring.

This is where Senetas encryptors excel; delivering robust CCTV encryption without loss of network performance – the most challenging of network security tests.

As CCTV technology advances (EG: real-time HD streaming, face recognition, motion tracking and night-vision) the volume and sensitivity of data transmitted across an organisation's high speed networks increases.

Video content is tightly regulated in many countries. This not only impacts on the streaming of video content, but also on the storage, sharing and archiving of data.

The last, best line of defence is to ensure the data itself is protected. This means, when a successful network breach occurs, unauthorised parties are simply left with meaningless encrypted data.

Critical CCTV data protection issues include:

- > Integrity – prevention of interference with CCTV footage (EG. input of rogue data)
- > Reliability – provision of uninterrupted, real-time surveillance coverage
- > Quality - 100% HD quality video with no noise, jitter or latency
- > Privacy – compliance with identity and data protection obligations
- > Complexity – CCTV systems typically comprise multiple devices

Traditional “border” security has proved to be ineffective when it comes to preventing network breaches.

Unlike other encryption solutions, Senetas high-assurance, encryptors provide maximum protection without compromising data network performance.

Real-world tests repeatedly prove Senetas CN Series encryption technology maintains maximum HD CCTV image quality and real-time CCTV network performance.



© Senetas

BIG DATA, CLOUD & DATA CENTRE SERVICES

The gaming industry continues to increase its use of Big Data applications and analytics to improve financial, competitive and operational performance.

The scalability, flexibility and on-demand nature of Cloud computing has proven popular within the gaming industry.

Organisations have been transitioning away from on-premises solutions as they seek operational efficiencies, greater systems availability, ease of management and lower cost of ownership of their IT infrastructure.

Consequently, data centre services have become essential resources for the processing, storage, backup and recovery of the rapidly growing volumes of CCTV video files.

Systems redundancy and failover means this data is often located across multiple sites, to ensure business continuity.

THE ADDED PEACE OF MIND OF MULTIPLE CERTIFICATIONS

All Senetas CN series encryptors are multi-certified. Whether or not certification is mandated by local regulations, Senetas is committed to 'certifications' as a key element of product development.

The Senetas CN encryptors are certified by leading independent, international testing authorities as "suitable for government and defence use."

Certifications held are: FIPS (USA), Common Criteria (International) and NATO (member states).

As the gaming industry becomes more dependent upon high-speed data networks to facilitate day to day operations, it is inadvertently exposing itself to an increased risk of cyber-attack and the potentially catastrophic consequences of a data breach:

- > Disruption of day-to-day operations
- > Inability to meet compliance obligations
- > Loss of reputation and brand equity
- > Theft of intellectual property (IP)
- > Financial penalties / loss of revenue
- > Breach of data protection / privacy laws

High-speed data networks are not inherently secure. Organisations do not have 100% control over the networks they utilise. Consequently, the data travelling across these networks is vulnerable to:

- > Eavesdropping
- > Data theft
- > Input of rogue data
- > Data redirection
- > User or technical error
- > Criminal negligence

CERTIFIED HIGH-ASSURANCE NETWORK ENCRYPTION SECURITY

The best network security solutions for the gaming industry require both high performance data networks and high-assurance encryption.

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 encryptors 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.

There are four essential capabilities necessary for high-assurance network data encryption:

- > Secure, tamper-proof, dedicated hardware
- > State-of-the-art automatic zero-touch key management
- > End-to-end, authenticated network encryption
- > Standards-based encryption algorithms

SENETAS ENCRYPTORS

All Senetas encryptors are certified, high-assurance security products. The CN Encryptor Series provides a complete range of data network encryption solutions:

CN4000

Small form-factor (desktop) encryptors for 'in the field' network link security (e.g. CCTV) – offering 10Mbps, 100Mbps and 1Gbps bandwidth speeds.

CN6000

Rack-mounted high speed encryptors for business-critical applications – offering 1Gbps to 10Gbps bandwidth speeds.

CN8000

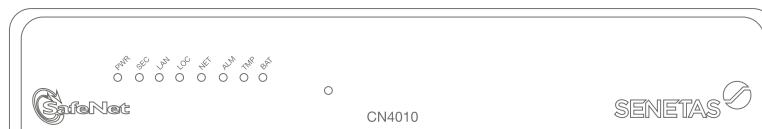
Multi-link, multi-protocol rack mounted device – offering up to 10 x 10Gbps encryption in a single unit.

CN9000

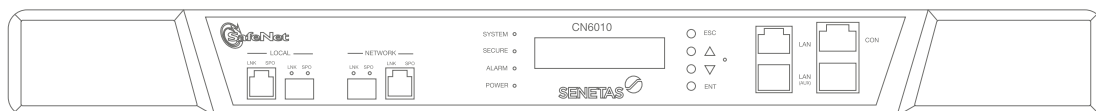
Ultra-high bandwidth, rack-mounted encryptor with "mega-data" performance – offering speeds of up to 100Gbps.

Senetas Layer 2 Carrier Ethernet WAN and MAN encryptors support all Layer 2 network protocols and topologies. All Senetas CN encryptors are 100% compatible and interoperable.

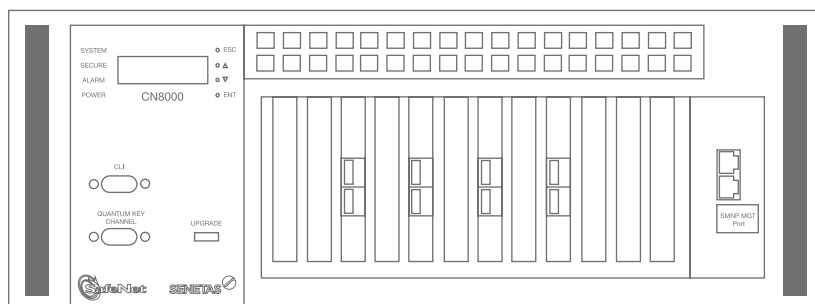
CN4000



CN6000



CN8000



CN9000



SUPPORT FOR ALL NETWORK TOPOLOGIES

The gaming industry often uses a mix of high speed network architectures to support its specific service requirements.

Whatever your chosen network topology, Senetas CN Series encryptors support the efficient operation of CCTV, Big Data, Cloud and Data Centre applications; across point-to-point, multipoint and fully-meshed networks.

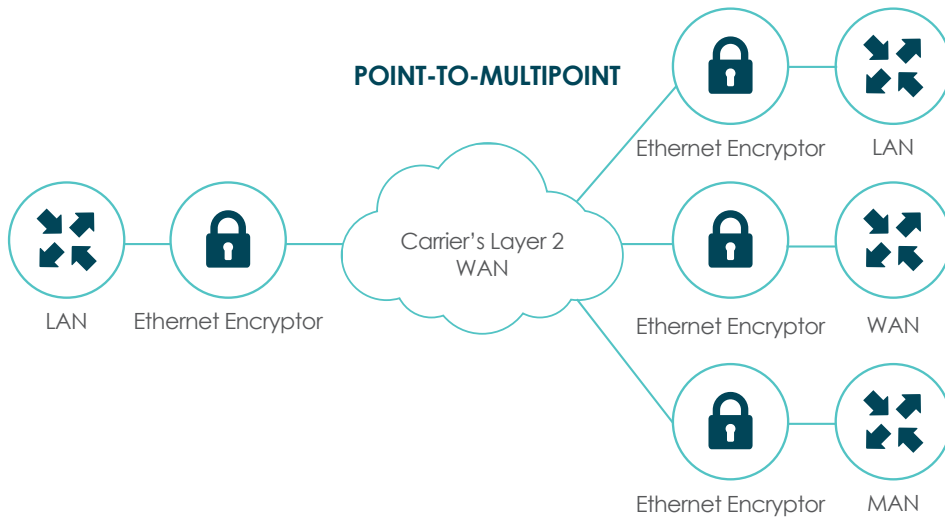
Maximum network performance is enabled via:

- > Cut-through technology
- > Full duplex mode at full line speed without loss of packets
- > Near-zero latency (as low as 1.5 micro-seconds)
- > Zero data and management overhead

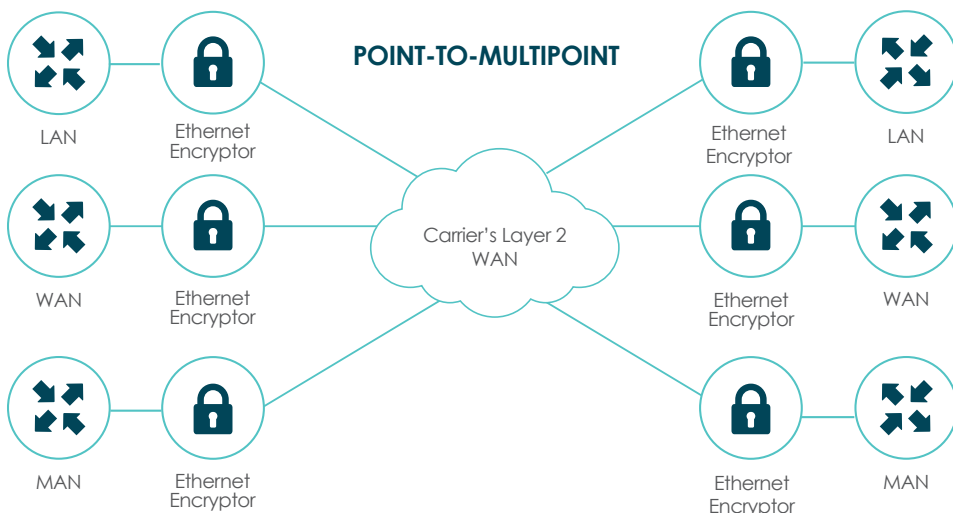
POINT-TO-POINT



POINT-TO-MULTIPOINT



POINT-TO-MULTIPOINT



What makes Senetas encryptors stand out from the crowd? Security without compromise!

Senetas encryptors' leading performance is not limited to their maximum data protection without loss of network performance.



Best Performance

HIGH-SPEED

The designed-in, market-leading performance capabilities of Senetas encryptors 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 encryptors ideally suited to the most demanding network environments.

ULTRA-LOW LATENCY

Senetas high-speed encryptors 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 10Gbps, 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

Because Senetas encryptors include the only multi-certified products of their types, 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 encryptors are certified by: FIPS, Common Criteria and NATO.

For 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 so called 'hybrid' encryptors.

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

Through proven Senetas R&D and global market reach, all Senetas encryptors are 'crypto-agile'. From 100% compatibility and interoperability; to customisable encryption and FPGA based flexibility; and 'Quantum safe' features.

Today, crypto-agility is increasingly essential to long-term data security – especially high value encrypted data stolen and stored by criminals awaiting new technologies to exploit the data in the future.

SUPPORT FOR ALL PROTOCOLS

The Senetas CN range of encryptors provides the widest feature-set.

Able to operate at 10Mbps to 100Gbps, they are designed for Layer 2 Carrier Ethernet WAN and MAN networks and support all current Layer 2 protocols: Ethernet, Fibre Channel; SONET/SDH and LINK.

SUPPORT FOR ALL TOPOLOGIES

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

The Senetas CN9000 encryptors are the only 100Gbps encryptors that support multipoint-to-multipoint topologies.'

Whether the network topology is simple or complex, the same high-assurance benefits apply.

EASY TO INSTALL

The 'bump in the Wire' design of Senetas CN encryptors makes them easy to install.

Simply place the encryptor at the access point to the Layer 2 network and all data passing through the unit is encrypted.

CUSTOM ENCRYPTION

In addition to the standards-based GCM AES - 256 and 128 bit algorithms, Senetas CN encryptors may be implemented with customized, customer requested algorithms.

Designed-in encryption agility enables the use of custom curves (BYOC) and entropy (BYOE).

QUANTUM-READY

Selected Senetas encryptors also support Quantum Key Distribution (Quantum Cryptography) and Quantum random number generation, making them 'Quantum safe'

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 encryptors feature automatic zero-touch key management. They also feature automatic network discovery and connection.

That simplicity continues with an intuitive user interface, providing meaningful diagnostics, such as early warnings and simple fault-finding.

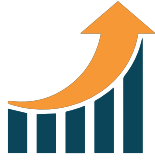
INTEROPERABILITY

Senetas encryptors supporting the same Layer 2 network protocol are fully interoperable. All Senetas CN models are backward compatible.

They may be relocated to other duties and newer models added over time to suit your changing needs; without becoming technically redundant.

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

Because all Senetas CN encryptors operate at full line speed; enable maximum network performance and deliver 'set and forget' management simplicity; they provide low-cost and high efficiency.

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 encryptors provide excellent total cost of ownership TCO through a mix of comparative network bandwidth savings, ease of network management and reliability. Customers benefit from low direct and indirect costs of ownership

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

Other cost benefits include, low power consumption minimal rack space use and combined rack space/power utilisation efficiency as well as 99.999% up-time reliability.

RELIABILITY

Senetas CN encryptors provide proven reliable 99.999% uptime and conform to international requirements for safety and environment.

All carrier-grade, rack mounted Senetas encryptors are hot-swappable and provide further network operations up-time benefits thanks to dual redundancy of encryptor consumables such as fans and power supplies.

Unlike hybrid encryptors and other low-assurance solutions, network up-time is not disrupted by Senetas encryptors.

FLEXIBILITY

Senetas encryptors' use of FPGA technology enables maximum operational flexibility.

They are better able to meet customers' specific requirements and provide an optimised high-speed data encryption solution.

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

R&D COMMITMENT

Senetas's leading high-assurance encryptors result from our commitment to research and development; to independent international testing certifications and high-speed encryption advances, such as support for Quantum Key Distribution.

SENETAS CORPORATION LIMITED

E info@senetas.com
www.senetas.com



Senetas manufactures high-assurance Layer 2 Metro Area and Carrier Ethernet network encryptors. They support all Layer 2 protocols and topologies.

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 30 countries.

SafeNet[®]

SafeNet CN Series
Ethernet encryptors

www.gemalto.com

GEMALTO DISTRIBUTION & SUPPORT

Senetas CN Series certified high-assurance network encryptors are distributed and supported internationally by Gemalto (North America, Europe, Asia, Middle East and Africa) as SafeNet CN Ethernet Encryptors.

GLOBAL SUPPORT AND DISTRIBUTION

Senetas high-assurance encryptors are supported and distributed globally (excl. AUS & NZ) by Gemalto – the world's largest data security company - under its SafeNet Identity and Data Protection Solutions brand.

Gemalto also provides pre-sales technical support to hundreds of accredited partners around the world; including systems integrators, data network providers, cloud and data centre service providers, telecommunications companies and network security specialists.

TALK TO SENETAS OR OUR PARTNERS

Senetas and Gemalto also work with customers' own data network service providers, systems integrators and information security specialists to specify the optimal high-assurance encryption solution for their needs.

Wherever you are, simply contact Senetas or Gemalto to discuss your needs. Or, if you prefer, your service provider may contact Senetas or Gemalto on your behalf.

CERTIFIED HIGH-ASSURANCE NETWORK DATA ENCRYPTION

Whatever your Layer 2 Ethernet network security needs, Senetas has a high-assurance solution to suit. They support data network links from modest 10Mbps and 100Mbps to high speed 1Gbps and 10Gbps as well as 10 x 10Gbps and ultra-fast 100Gbps bandwidth.

Certified, scalable, agile and easy to use; Senetas high-assurance encryptors provide maximum data security without compromising network performance.

GAMING-SP0417