SENETAS CERTIFIED HIGH-ASSURANCE ENCRYPTION FOR THE DEFENCE INDUSTRY

SENETAS

Security without compromise

The defence industry has become dependent upon the fixed, high-speed data networks that serve as its core network infrastructure; providing Big Data, Cloud, SaaS and other digital transformation technologies

These critical technologies and applications generate huge volumes of data. Data that is often transmitted across wide and Metro Area Networks; exposing it to a variety of cyber-threats. Unfortunately, this "data in motion" is often over-looked when it comes to cyber-security planning.

Across the world, defence industry organizations are required to comply with a wide variety of cyber-security regulations. Adherence to these standards, whether independent or business/ department specific are generally a prerequisite to operate within the sector.

However, private and public-sector organizations operating within the defence sector need to understand that managing cyber-security risks to network data goes well beyond essential privacy and compliance issues.

Some of the risks are serious enough that they can threaten the core of an organization's operations; its value, intellectual property, business intelligence or physical assets.

Despite the high-profile stories of data breaches that have dominated the headlines for the past five years, research repeatedly highlights that these risks are underestimated.

This is often because of a presumption that fibre-optics used in core network infrastructure, such as high-speed Ethernet networks, are safe. They are not.

Whether your network infrastructure is carrier-provided (public) or corporate-owned (private), it could be carrying large volumes of data, streamed at anything from 10Mbps to 100Gbps.

As a result, it is a high-value target for eavesdropping and all manner of cyber-attacks. As James Caplan from McKinsey and Company puts it "The larger the data volume, the greater the risk."

When it comes to securing core data networks, the risk is even greater. The vulnerabilities present in major vendors' network devices (such as routers and switches) place an addition burden on infrastructure managers.

Interrupting day-to-day network operations to implement a long list of security software patches is nobody's idea of best practice.

Assuming they can stay up to date with the latest patches, IT professionals are still fighting a losing battle. High-speed networks are not inherently secure and breaches are inevitable.

Why encrypt sensitive network data?

The need to protect government organisations' sensitive information within their systems is clear. But, the need to protect transmitted network data has not been so obvious.

Leading data security organisations highlight that many organisations do not sufficiently protect network data once outside their direct control.

Who really knows what happens to their data while it is being transmitted to another location?

If nothing else, the vast number of recorded data network breaches in recent years highlight the importance of protecting the data itself.

Encrypting Data in Motion

In its Global Data Security Report, information security experts – Trustwave – noted that 62.5% of data theft occurred while in transit.

Data travelling through networks is not just exposed to an increased risk of cyber-attack; there is a genuine risk of human error and equipment failings that can manifest more often than you would think.

However, these risks can be eliminated – and security assured - by automatically encrypting network data (including voice and video) while it's in motion.

Data security advisors highlight that almost all network data should be encrypted. They argue that in large volumes even low value data, when aggregated, can be useful to cyber-criminals and any network breach has the potential to be harmful to reputations and stakeholders' trust.

Security Without Compromise

In the past, data encryption came at the expense of network performance, due to excessive latency and encryption overheads.

Senetas encryptors provide maximum network performance and maximum data protection; featuring ultra-low latency, zero network overhead and zero impact on other network devices.

Typically, data networks used to transmit information are known as Layer 3, but when you encrypt Layer 3 networks, it comes at a serious cost of 50% to 70% of network performance.

On the other hand, Layer 2 networks do not suffer the same lost performance. They are used when high data volumes and performance needs demand more bandwidth and improved cost efficiency, together with best practice data security.

Certification. Your Assurance, Our Commitment

Senetas government customers are assured of our encryptors' performance by the certifications provided by the leading testing authorities (FIPS, NATO, Common Criteria).

Certification involves years of rigorous testing by the testing authorities' own labs. Without these certifications, products are unable to be installed in the respective government data networks.

In addition to our encryptors' certifications, government and defence customers have also undertaken their own proof of concept and benchmarking testing. In every case, Senetas encryptors have excelled.

Importantly, organisations providing services to the government and defence sectors – such as Cloud computing or data centre storage services – can meet the certification requirements of their own government customers by using Senetas certified high-assurance products.

That's why Senetas encryptors secure much of the world's most sensitive data.

Certified high-assurance network encryption security.

The best network security solutions for government and defence applications 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:

> Dedicated, secure and tamper proof hardware

> Automatic, 'zero-touch' encryption key management

> Authenticated, end-to-end network encryption

> Robust, standards-based encryption algorithms

Senetas Encryptors

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

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

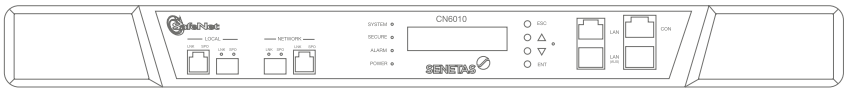
Multi-link, multi-protocol rack mounted device – offering up to 10 x 10Gbps encryption in a single unit

CN9000

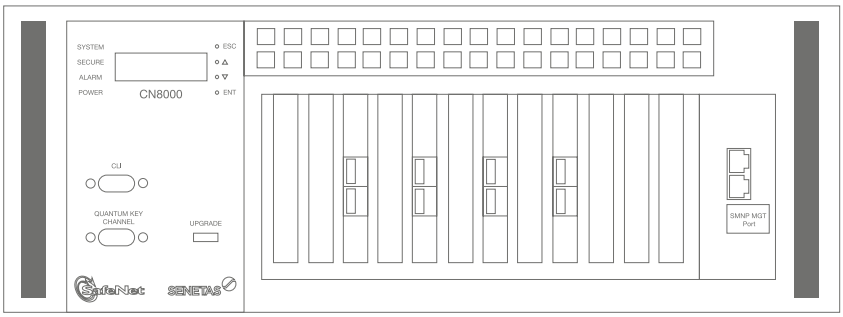
Ultra-high bandwidth, rack-mounted encryptor with "mega-data" performance – offering speeds of up to 100Gbps.

CN4000

CN6000



CN8000



CN9000

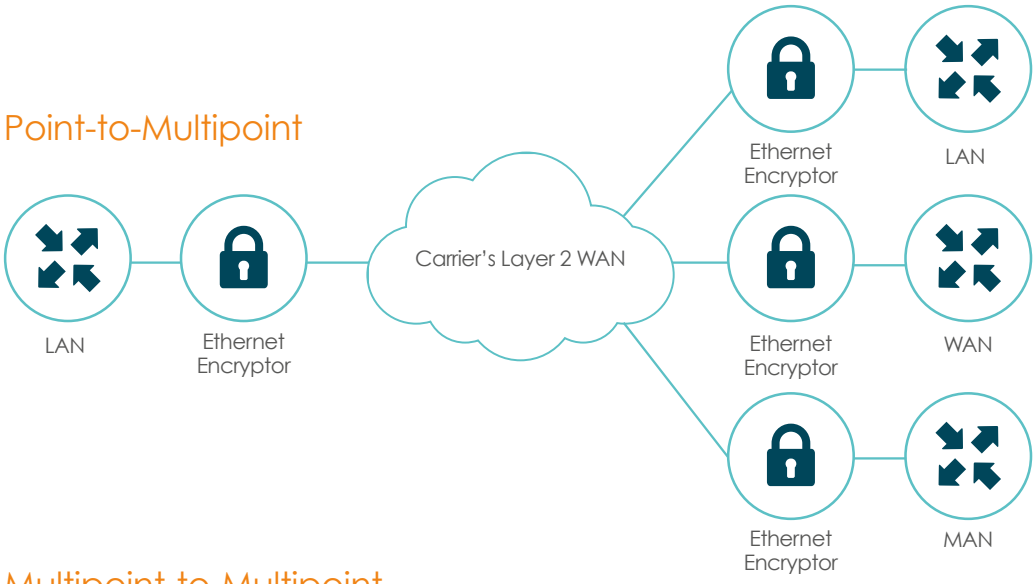
Support for all network topologies.

Local and national governments frequently use a mix of high speed network architectures to support their specific service requirements. Senetas encryptors provide support for all data network topologies, at speeds from 100Mbps to 100Gbps.

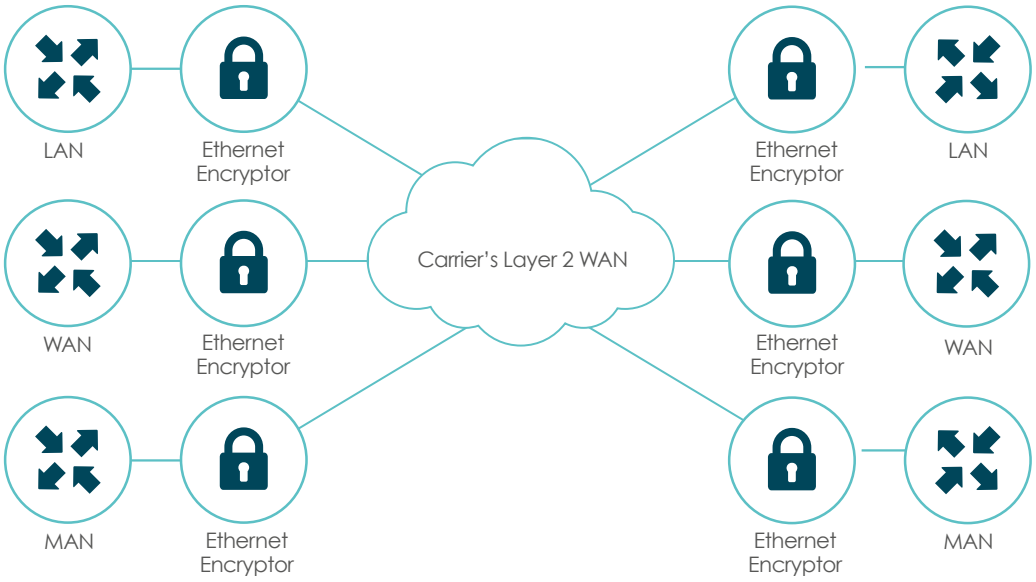
Whatever your chosen network topology, Senetas CN Series encryptors support the efficient operation of CCTV, Big Data, Cloud and Data Centre applications; across point-to-point, multipoint and fully-meshed networks.

Point-to-Point

Point-to-Multipoint



Multipoint-to-Multipoint



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

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

All Senetas encryptors are 'crypto-agile'; 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 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 Layer 2 protocols: Ethernet, Fibre Channel; SONET/SDH and LINK.

Support for all topologies

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

Interoperability

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

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 encryptors 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 encryptors provide excellent total cost of ownership 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 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.

GLOBAL SUPPORT AND DISTRIBUTION

Senetas CN Series High-Assurance Encryptors and CV Series Virtual Encryptors are distributed and supported by Gemalto, the world's largest data security company, as SafeNet Ethernet Encryptors.

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 encryption solution for their needs.

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

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your Layer 2 Ethernet network security needs, Senetas has an encryption solution to suit. They support data network links from modest 10Mbps and 100Mbps bandwidths to high speed 1Gbps, 10Gbps and even ultra-fast 100Gbps networks.

Scalable, agile and easy to use; Senetas encryptors provide maximum data security, without compromising network and application performance.

SENETAS CORPORATION LIMITED

E info@senetas.com

www.senetas.com

Senetas designs, develops and deploys high-assurance network data encryption solutions. Designed for today's core Metro Area and Carrier Ethernet WAN infrastructures, Senetas solutions support all Layer 2 protocols and topologies.

Our multi-certified CN Series hardware encryptors have crypto-agility built in and 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.

gemalto

www.gemalto.com

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

DEFDSG-SP1017