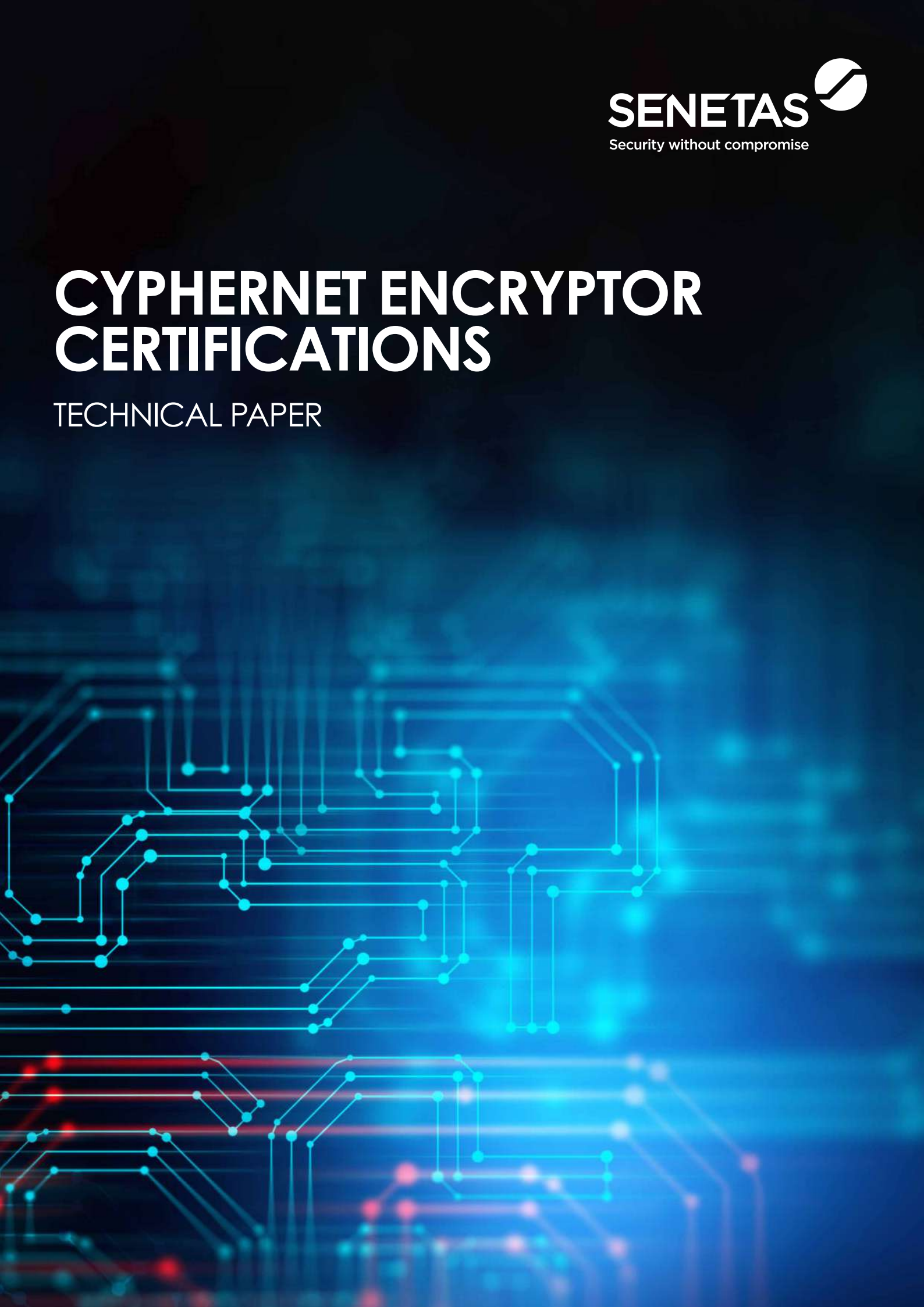
SENETAS

Security without compromise

CYPHERNET ENCRYPTOR CERTIFICATIONS

TECHNICAL PAPER



INDEPENDENT CERTIFICATION

Senetas CypherNET encryptors include the security assurance of certification by leading independent testing authorities. They are certified as suitable for government and defence use by FIPS, Common Criteria, NATO and CAPS.

Independent certification is well documented by data security experts and analysts as an important feature of high-quality encryption products. It provides assurance to both enterprise and government customers that their high-speed network transmitted data is protected to the highest possible security standards.

Certification by leading testing authorities is considered a primary differentiator among encryption products. "Not all encryption is the same…" is the warning provided by security experts.

In simple terms, it isn't that standards-based (EG. AES GCM 256) encryption algorithms differ – they don't. The issue is how that encryption algorithm is used. It is the encryption methodology that differs among vendor solutions.

Consequently, it is the process of encrypting network transmitted data that is certified. Of course, different testing authorities may use different models for certification; the details of which are all publicly available.

The process of having an encryption security product certified is both expensive and time-consuming and involves a lot of skilled staff on both sides. Certification is not a one-time thing; it involves a long-term commitment to maintaining certification over time.

Senetas made that commitment and has maintained it for over 20 years. Since developing our very first encryptor, we have chosen to differentiate our products through certification.

Multiple certifications forms a key part of the high-assurance security standard and promise you receive from Senetas encryptors.

Senetas encryptors are the only products of their type to be certified by all four leading independent international testing authorities as suitable for government and defence use.

Our high-assurance encryptors also maintain maximum network performance; delivering security without compromise.

WHY IS CERTIFICATION IMPORTANT?

Simply put, certification provides both government and commercial customers with peace of mind; third party validation that Senetas encryptors provide maximum data protection.

Compliance with these independent, international certification standards is a strict requirement for many government and defence agencies when it comes to the protection of sensitive data (whether formally classified as sensitive or not).

Certification involves lengthy and rigorous testing; a process which may take years. Once the initial certification has been completed, products are subject to on-going assessment, where even the smallest change to the product specification requires a process of re-certification.

Senetas products are certified as "suitable for government and defence use". Within these organisations, network data is classified according to its degree of sensitivity.

Certification is used to further establish a product's suitability to handle data at varying levels of sensitivity; including 'confidential' and 'secret' information.

It's worth remembering that any organisation providing services to the government or defence sectors, including secure Cloud and data centre service providers, are required to meet the same security standards as their government department or agency clients.

Whether you're protecting big data applications, cloud or data centre services, CCTV networks or critical infrastructure and SCADA control systems; certification provides valuable security assurance.

The added assurance that comes from certification provides further benefits to the organisation, its staff and suppliers.

Not only does it demonstrate that they are committed to protecting stakeholder privacy and data security, but also that they are meeting their compliance obligations.

An investment in certifications by multiple international testing authorities reflects Senetas' continued commitment to product excellence and its desire to meet the most rigorous international security testing standards.

As a leading provider of multi-certified, high-assurance network encryption hardware, it is easy to see why Senetas products have been used to secure so much of the world's most sensitive data over the past 20 years.

Independent authorities

FIPS

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government computer security standard used to accredit cryptographic modules. FIPS 140-2 defines four levels of security; named "Level 1" to "Level 4".

CC

The Common Criteria for Information Technology Security Evaluation (aka Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. CC is a driving force for the mutual recognition of secure IT products in more than 25 countries.

NATO

The NATO Information Assurance Product Catalogue (NIAPC) provides NATO nations, civil and military bodies with a catalogue of Information Assurance products that are in use or available for procurement to meet operational requirements.

CAPS

The CESG Assisted Products Service defines standards to be employed where encryption is used to safeguard government classified data. CAPS verifies that products have met these standards.

CERTIFICATIONS

FIPS

Model/Series	Firmware Version	Last Validated	Certification Standard
CN4010	5.1.1	April 2021	FIPS 140-2 Level 3
CN4020	5.1.1	April 2021	FIPS 140-2 Level 3
CN6010	5.1.1	April 2021	FIPS 140-2 Level 3
CN6100	5.1.1	April 2021	FIPS 140-2 Level 3
CN6040	5.1.1	April 2021	FIPS 140-2 Level 3
CN6140	5.1.1	April 2021	FIPS 140-2 Level 3
CN9100	5.1.1	April 2021	FIPS 140-2 Level 3
CN9120	5.1.1	April 2021	FIPS 140-2 Level 3

FIPS Certified Module Catalogue

Common Criteria

International, French Network Information Security Agency (ANSSI) and Australian Information Security Evaluation Program (AISEP)

Model/Series	Firmware Version	Last Validated	Certification Standard
CN4010	5.0.2	July 2021	EAL 4+
CN4020	5.0.2	July 2021	EAL 4+
CN6010	5.0.2	July 2021	EAL 4+
CN6140	5.0.2	July 2021	EAL 4+
CN9100	5.0.2	July 2021	EAL 4+
CN9120	5.0.2	July 2021	EAL 4+

Common Criteria Certified Product Catalogue

NATO

Model/Series	Firmware Version	Last Validated	Classification
CN4010	5.0.2	April 2021	NATO Restricted
CN6010	5.0.2	April 2021	NATO Restricted
CN6040	5.0.2	April 2021	NATO Restricted
CN6100	5.0.2	April 2021	NATO Restricted

NATO Information Assurance Product Catalogue

SECURITY WITHOUT COMPROMISE

Senetas encryptors are designed specifically to meet the demands of the most challenging high-speed network environments, without impacting on network performance.

Near-zero latency, minimal data overheads, network transparency and interoperability combine to provide security without compromise.

Senetas high-assurance encryptors provide the best of both worlds; maximum security with minimum impact on the network:

- Near-zero data latency - the time delay between encryption and decryption).
- Minimal data overheads - the additional bits of data transmitted by the encryptor/s).
- Bump-in-the-wire network presence – Senetas encryptors have zero impact on other network assets.
- 100% compatibility – Senetas encryptors are fully interoperable, compatible with all network assets and transparent to the network.
- No network downtime – software upgrades and device maintenance can be carried out without disruption to the network/links.

Weaker encryption solutions, those based on less robust processes or built to a price, often result in a compromise between security and network performance. This can prove expensive over time:

- Lost bandwidth/speed – resulting in increased telecommunications costs.
- Business disruption – impacting on process efficiency and workforce productivity.
- Increased IT costs – more resource dedicated to managing network devices and security hardware.

Simply "turning up the bandwidth" to compensate for the impact on network performance is both unnecessary and expensive. The additional telecoms network expense may be greater than the cost of the encryption solution itself.

Furthermore, there are a number of intangible costs resulting from poor security and network performance in specific applications:

- Security risks associated with CCTV networks, where high quality and real time performance are essential within law enforcement and gaming environments.
- Safety implications for healthcare applications, where real time performance may be critical to patient care.

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:** infoemea@senetas.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 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.

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 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.

XXXXXX-TP0921

SENETAS