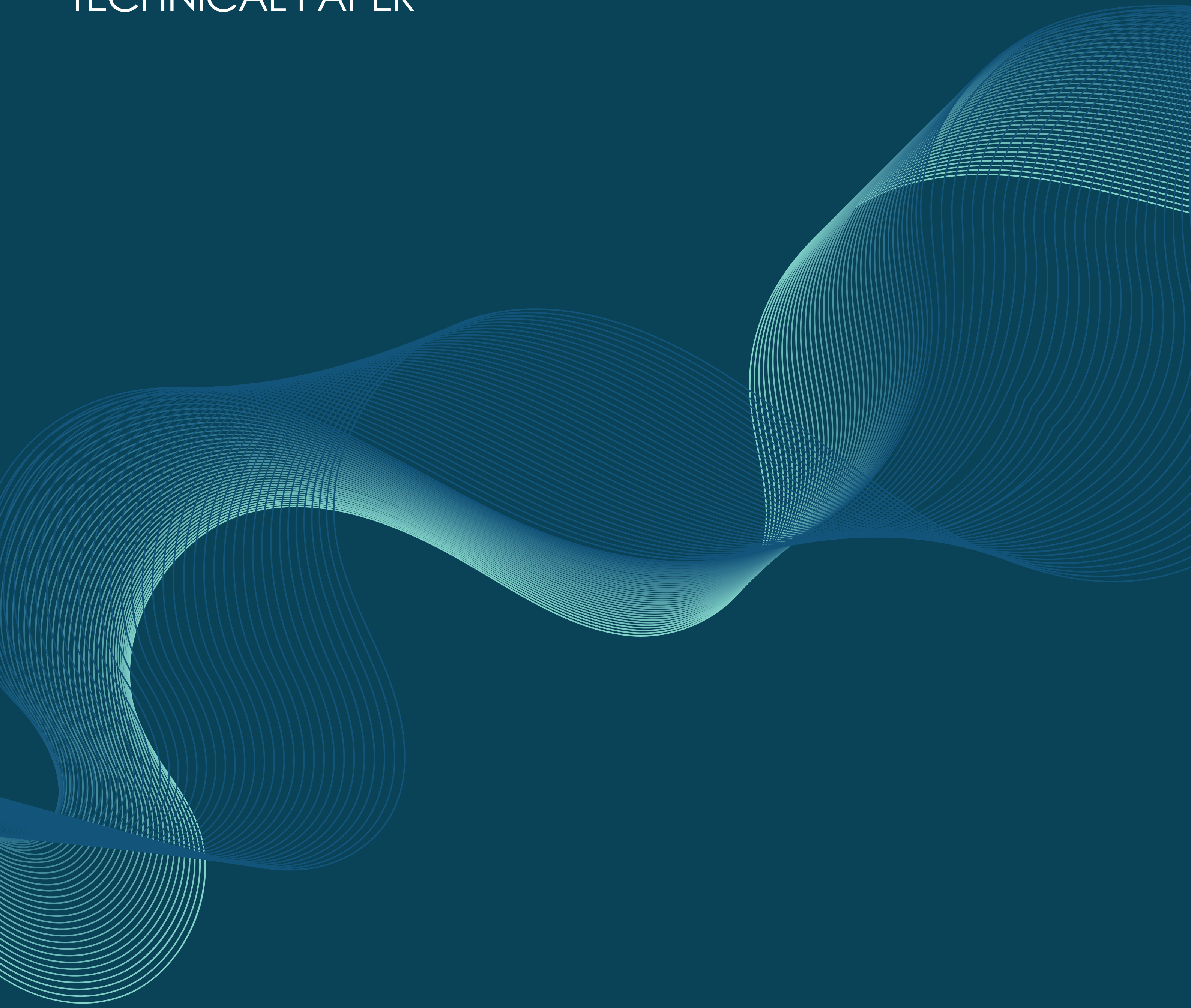
SENETAS

Security without compromise

CRYPTO-AGILITY

TECHNICAL PAPER



BRINGING AGILITY TO CRYPTOGRAPHY

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.

Versatility and agility are core components of the Senetas high-assurance encryption proposition.

In addition to leading network and security performance, they are a part of what makes Senetas encryptors stand out from the crowd.

More agile than some might think, the best modern encryption solutions are not only suitable for networks of all shapes and sizes, from modest 10Mbps to ultra-fast 100Gbps speeds, they occupy a barely perceptible presence on the network, are transparent to all other devices and result in minimal latency.

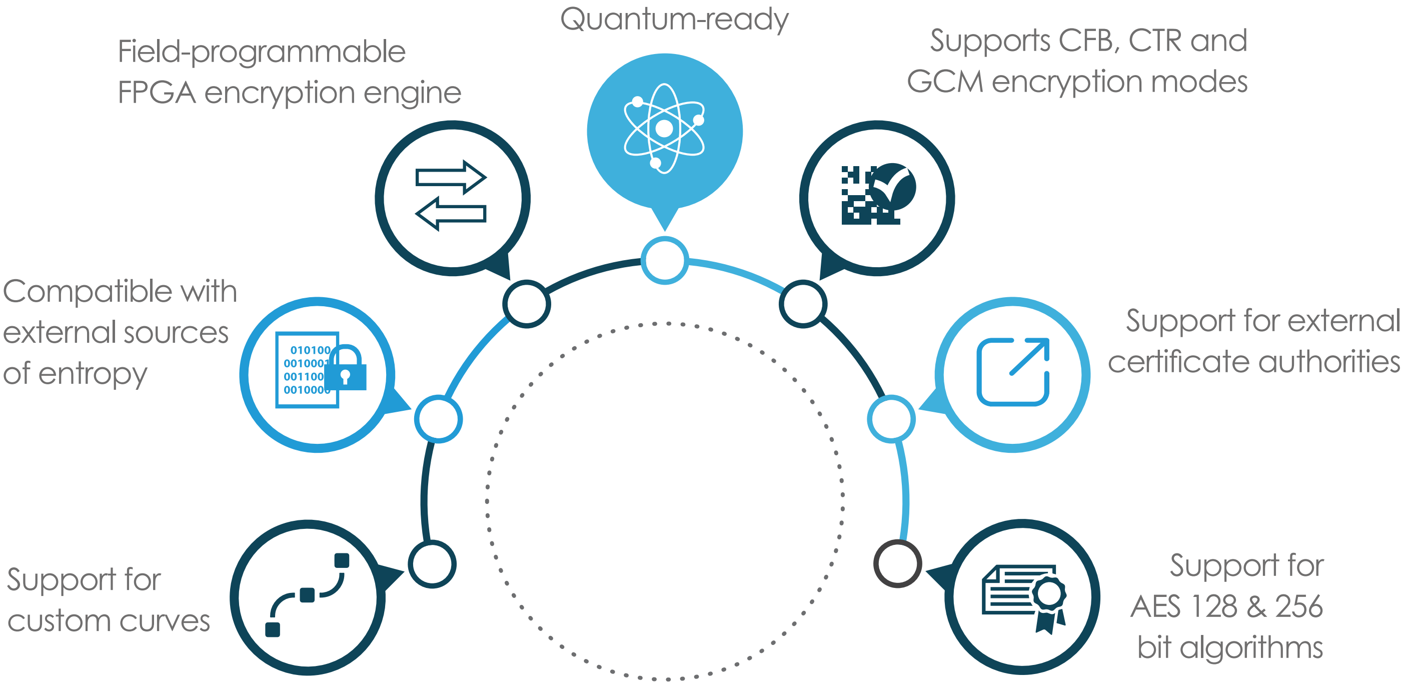
Crypto-agility, however, is much more than simple performance statistics. It comes from compatibility and interoperability, from FPGA-based flexibility and from the ability to support custom cryptographic elements. It even enables a choice of encryption algorithms and standards.

Truly high-assurance encryption solutions are based on standards-based algorithms, typically AES 128 or 256bit. However, If you are able to provide your own, you may prefer to use those; there's nothing that says you must use the manufacturer's standard algorithm.

An encryption platform should offer support for as many of these algorithms as possible. For example, CFB (Cipher Feedback) mode, CTR (Counter) mode and GCM – an authenticated encryption mode.

Beyond encryption modes, agility should extend to support for other custom components, such as user-defined curves, external certificate authorities and sources of randomness.

That's true agility.


Quantum-ready
Field-programmable FPGA encryption engine
Supports CFB, CTR and GCM encryption modes
Compatible with external sources of entropy
010100
001000
001100
001000
Support for external certificate authorities
Support for custom curves
Support for AES 128 & 256 bit algorithms

Support for AES 128-bit and 256-bit algorithms with programmable S-boxes

AES (the Advanced Encryption Standard) was established by the National Institute of Standards and Technology (NIST) in 2001 and has become the industry standard symmetric encryption algorithm. Senetas encryptors support both 128-bit and 256-bit AES keys.

In addition, Senetas has a programmable S-box capability that allows customers to modify the standard S-box values to create a bespoke symmetric cipher.

Key size is an important aspect of long-term data protection and all modern cryptographic systems should support AES key sizes of 256 bits.

However, the emergence of the quantum computer threatens the status quo of current cryptographic systems. The exponential growth in computing power represented by the move to qubits will make much of today's public key infrastructure redundant.

Although quantum computers pose less of a threat to symmetric encryption solutions than they do asymmetric systems, a quantum computer of sufficient scale will halve the effective key size of algorithms such as AES. This means that today's 128-bit key may only be as effective as a 64-bit key in the future.

Encryption systems that only support 128-bit keys today, and that cannot be upgraded to larger keys, will not be secure against tomorrow's post-quantum threats.

Although AES is the NIST approved encryption algorithm, and widely used across the globe, some customers have bespoke encryption requirements that dictate the use of modified or non-standard cryptography.

In-field programmable FPGA encryption engine

All Senetas encryptors feature programmable silicon technology called Field Programmable Gate Arrays (FPGA); which are used for both the encryption engine and network protocol processing.

The versatility of this technology means the functions it performs may be changed even when the encrytor is embedded within a network environment; allowing functionality to be added on the fly.

Most encryption hardware, such as that commonly offered in routers or switches, has encryption implemented in high-performance but fixed function chips called ASICs (Application Specific Integrated Circuits). These "hybrid" devices also happen to pose other encryption security weaknesses.

ASICs are designed to perform one set of functions only and cannot be modified to extend or change that functionality.

Like all standards, cryptographic protocols and algorithms evolve naturally over time to improve security and performance, or counter new threats.

For this reason, or to meet customer-specific requirements, it is important that encryption systems may easily evolve and adopt alternative cryptographic approaches when required.

ASIC based encryption solutions cannot be modified to meet emerging threats (such as Quantum Computing) nor to extend functionality - e.g. to support new key sizes or algorithms. When support for new functionality or standards is required the only option with ASIC-based solutions is to throw them out and replace them with new hardware.

Senetas encryption hardware is future-proof because it is fully in-field programmable; enabling it to meet new standards or customer requirements and providing a measurable, long-term return on investment.

Support for GCM, CFB and CTR encryption modes

A symmetric block cipher such as AES may operate in several different modes. These modes combine confidentiality and authentication in a variety of ways, with differing performance characteristics.

Senetas encryptors support a wide range of encryption modes; including confidentiality only (e.g. CTR, CFB) and confidentiality with authentication (GCM).

This flexibility allows customers to decide what level of security and performance they require in their environment.

By building this level of agility into the standard management of all Senetas encryptors, customers are free to secure their networks with the most efficient and lowest overhead encryption possible.

At the same time, organisations that are seeking fully authenticated encryption can do so, at the cost of a slightly higher network overhead.

The importance of authenticated encryption is often overlooked. In addition to protecting the confidentiality of data in motion, GCM encryption also secures the network link itself. Any attempt to inject rogue data into the system is automatically detected - something that is of particular importance in SCADA and industrial control systems.

Support for custom curves

Elliptic Curve Cryptography (ECC) is an efficient, and highly secure, public key encryption mechanism; commonly used to protect the web and crypto-currencies such as Bitcoin.

An elliptic curve is essentially a set of points described by an equation and there are many to choose from.

Industry bodies such as NIST in the US, or ANSSI in France, have defined certain sets of curves that are required for securing government networks in those countries.

Support for custom curves allows Senetas customers not only to choose from a very broad set of industry / national standard curves, but also to define any curve of their choice by entering their own parameters to define the required curve.

This allows customers to move away from reliance on a small, pre-defined group of curves and, in effect, gives them the freedom to design their own, bespoke asymmetric encryption engine.

Curve parameters do not need to be shared with anyone (including Senetas) and may be kept secret within the community of encryptors that uses them.

Support for custom entropy (BYOE)

Senetas encryptors have one or more built-in sources of entropy that provide FIPS approved random numbers for generating key material.

BYO entropy is the ability to replace the hardware sources with a user-defined entropy pool that may be secretly and dynamically loaded into the encryptor.

Users may create a simple file of random numbers using a method of their choice and load this directly into an encryptor for direct use as encryption keys during normal use.

The encryptor provides clear feedback to the user with statistics such as entropy pool size, bytes used and estimated days remaining.

BYOE provides customers with direct control over the generation of random numbers for the seeding of encryption keys. Direct control over the souce of entropy may be required to meet regulatory requirements in some jurisdictions.

Support for external certificate authorities

Support for third-party certificate authorities (CAs) allows Senetas encryptors ro use an external CA as a root of trust between authenticating devices.

A fully-featured CA capability is provided as a part of the Senetas CM7 management suite. However, some uses may need to use an existing third-party CA to issue and sign the encryptor's digital certificates.

As long as the third-party CA supports the standard X.509v3 certificate format, the external CA may generate its own root keys and sign certificates for any encryptor in the network.

Quantum-ready cryptography

Quantum-ready is the term Senetas uses to describe its products' ability to support encryption technologies that will be resistant to future attacks by quantum computers on conventional encryption algorithms.

Quantum key generation and distribution

Senetas encryptors already support Quantum Key technologies in conjunction with technology partner, Swiss quantum technology company ID Quantique.

Quantum key management technologies leverage the fundamental principles of quantum physics both in the generation and distribution of encryption keys.

Firstly, that the generation of the quantum key is truly random and secondly, that any attempt to interrupt or eavesdrop on the encrypted data will disturb the system and be detected.

In the joint Senetas/IDQ solution, the QKD server autonomously generates, manages and distributes quantum keys to one or more encryptors through a secure, dedicated channel.

A quantum random number generator embedded in the QKD server guarantees that the encryption keys are produced in an absolute random way with high-quality entropy.

Senetas encryptors support the latest European Telecommunication Standards Institute (ETSI) standards for quantum key distribution – an important and emerging security capability that has significant applications in 5G networks.

In practice, QKD is combined with conventional key distribution techniques (dual key agreement) to produce a key that is as secure as the strongest of the two original keys. This approach offers the best of the classical and quantum worlds.

Quantum Resistant Encryption

In 2020 Senetas became the first cybersecurity firm to bring to market a range of high-assurance, high-speed network encryptors that provides quantum resistant encryption (QRE).

The new, hybrid CN Series combines support for the best of today's state-of-the-art, classical encryption security with the next generation of NIST shortlisted

quantum resistant algorithms to provide the ultimate in long-term data protection.

The NIST shortlisted algorithms are expected to be standardised by 2022. In the meantime, support for QRE will be made available to Senetas customers via their current crypto-agile platform.

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