SENETAS CRYPTO-AGILE ETHERNET ENCRYPTORS

TECHNICAL PAPER

SENETAS

Security without compromise

Senetas high-assurance network data encryptors provide state-of-the-art cryptography; meeting the broadest range of international encryption certification standards.

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.

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.

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.

Senetas will soon add Quantum Resistant Algorithms that will complement today's asymmetric algorithms and provide an additional layer of security.

Quantum key distribution

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

Quantum Key Distribution (QKD) is a technology that relies upon two fundamental principles of quantum physics to generate 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.

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.

The dawn of the quantum computer

Unlike classical encryption key generation, which is based on mathematical algorithms, QKD will not become compromised as computing power increases. More importantly, it is not vulnerable to passive attacks, where data is captured for subsequent decryption.

Passive attacks are potentially the most dangerous for many organisations as they often go un-detected until the data has been decrypted and the consequences felt by the business.

In a passive attack, data is typically copied or captured and stored offline for future decryption – either through brute force attacks or when current PKS algorithms are broken.

Data such as customers' financial, credit card or personal details have long-term relevance for identity theft or fraud, so longer-term protection is essential.

The Senetas and QKD integrated solution has been successfully deployed in several major European financial institutions, providing forward-secrecy for the most sensitive long-term data.

Whilst the current state of the technology is limited in terms of distance, companies are already utilising QKD to secure 10GB Ethernet connections, as a part of their back-up and business continuity strategies, to disaster recovery sites up to 100km away.

Outside of real-life applications, QKD has been successfully demonstrated in laboratory conditions over distances as great as 300km.

However, the future of long-distance QKD is likely to come in the form of satellite-based key exchange, with low-orbit communications satellites transmitting keys securely to a network of terrestrial base-stations.

By harnessing the power of quantum mechanics, QKD ensures a provably secure key exchange, alerting to any potential eavesdropping, as well as providing forward secrecy of the encryption keys.

Organisations need to start preparing today for the threat posed by the development of Quantum Computers.

As encrypted data has a critical "shelf life", it is not sufficient for organisations to wait until a viable quantum computer is developed before acting to mitigate the threat. The long-term security of today's secrets relies on us finding a solution to this problem sooner rather than later.

NIST has formally recognised the Quantum Computing threat and recently began the process of standards setting for a new generation of algorithms.

Customers investing in encryption solutions today need to ensure that they buy future-proof; i.e. crypto-agile, technology that will solve both today's and tomorrow's problems.

"In order to protect our cyber security infrastructure from the threat of the quantum computer, we have to plan the transition to quantum-safe security right now."

Bruno Huttner, ID Quantique

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.

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 35 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.

CRYAGI-TP0817