100GBPS ENCRYPTION USE CASES

SOLUTION PAPER

SENETAS

Security without compromise

100GBPS ENCRYPTION USE CASES

Senetas CN9000 Series 100Gbps Encryption in Action

What does 100Gbps look like? Imagine encrypting, transmitting and decrypting 20,000 HD streaming movies in just one second! Or, streaming the entire contents of your local library in just one second.

This is the power of the Senetas CN9000 series encryptors: ultra-fast, ultra-secure, ultra-reliable performance; every second of every day.

Senetas CN9000 Series encryptors represent the very best in electronics engineering, data network security R&D, ultra-fast 100Gbps bandwidth performance and future-proof data security.

"The Senetas CN9000 series is the first commercially available range of certified high-assurance 100Gbps Ethernet encryptors that support the most complex fully meshed topologies - enabling 100% security for Big Data, Cloud and data centre services' ultra-fast networks".

When it came to planning the future of ultra-fast data network security, Senetas collaborated with stakeholders from a broad cross section of service provider and end-user organisations. We spoke with cloud and data centre service providers, national governments, telecommunications giants and commercial enterprises in three continents.

Everyone recognised the impact of big data, the IoT and ubiquitous connectivity. As bandwidth and data volumes increase, so does risk.

Service providers acknowledge that network security is not negotiable. As a core component of modern IT and communications infrastructure, security is a potential source of competitive advantage. However, security cannot come at the expense of network performance or user experience.

THE CASE FOR ULTRA-FAST 100GBPS NETWORKS

The first commercially available 100Gbps fibre network implemented in the USA was in Cleveland, Ohio.

The network was the result of a collaborative effort to meet the exacting demands of the world's fastest bandwidth network within the well-known Cleveland Health-Tech Corridor.

The business imperative was simple. The campus-like (data network) collaboration of scientific, medical, research and related Big Data analytics demanded 100Gbps bandwidth speed to:

- Deliver business and economic growth advantages
- Enable high-tech and innovation development
- Meet the needs of scientific research organisations
- Provide a platform for advanced healthcare
- Enable the best technology infrastructure for Big Data, data centre, and Cloud service providers

Using the first US Carrier-provided 100Gbps fibre network links, these data-intensive organisations continue to report significant ROI benefits:

- Real-time collaboration using hi-resolution medical images is speeding up diagnoses and helping to save lives
- Scientific research & development is accelerated with instant access to 'mega data' and analytics
- Enabling next-generation video streaming by overcoming bandwidth barriers to "4D", holographic and immersive video
- Real-time data mining and multi-dimensional analytics enables emerging Big Data apps –such as genomics and UHD medical imaging
- Virtualization and convergence of data storage and data networks – enabling instantaneous access to long term stored and archived 'mega data'.

However, the development of high-profile, ultra-fast networks and high-value 'mega data' links expose the collaborating partners to a significantly increased risk of cyber-attack.

All 100Gbps networks have similar security threat profiles and demand certified high-assurance network data encryption security if they are to be fully protected from an array of cyber-threats, including:

- Eavesdropping
- Intellectual property theft
- Rogue data attacks
- Financial harm
- Redirection of sensitive data
- Technical or human errors
- Vulnerable network devices.

100Gbps encryption needs

Throughout the partner, customer and service provider engagement process, six key requirements kept coming up as being "non-negotiable".

1. Any solution must provide robust high-assurance^ network security, and preferably certified by a recognized independent testing authority
2. Robust encryption must not interfere with 100Gbps network and link bandwidth and application performance
3. Anything but consistent, ultra-low latency would not be acceptable because of the real-time nature of applications
4. Any new solution should represent a future-proof investment, delivering a rapid ROI and providing interoperability with similar, lower bandwidth solutions
5. As modern networks come in all shapes and sizes, the solution should provide support for all topologies
6. Any data overheads caused by the encryption solution must be as low as to be immaterial
7. The solution's total cost of ownership (TCO) profile, including overheads, must be efficient.

^ Click here to read more about criteria for 'high-assurance' Ethernet network encryption.

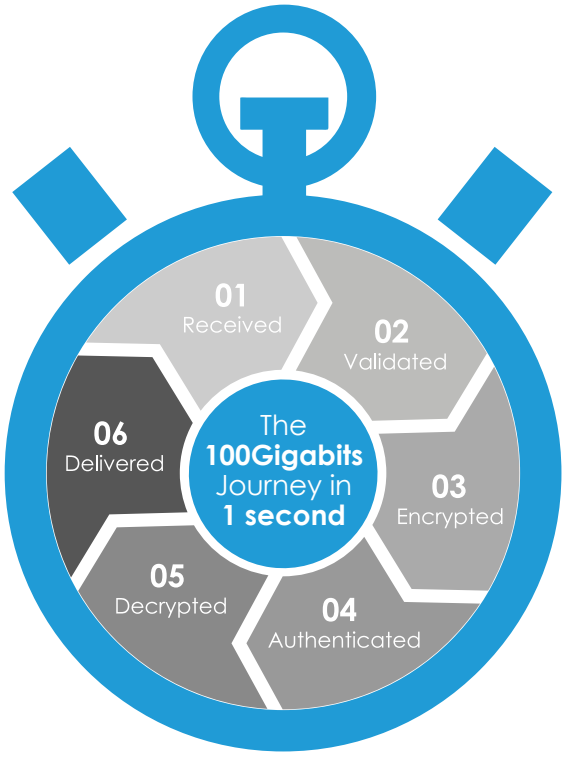
100GBPS USE CASES

Until recently, ultra-fast network links were largely the domain of data centre-to-data centre and location-to-location applications – a simple point-to-point network topology.

Today, this ultra-fast bandwidth demand is increasingly driven by more complex applications, such as cloud and data centre services, campus networks and more complex data aggregation architectures.

The issue for high-assurance encryption of ultra-fast networks and links is the need to support complex network topologies – in particular, various multi-point, fully meshed and hub-and-spoke architectures.

This represents a challenge, as it demands high-assurance encryption of a range of complex network topologies, including multi-point to multi-point, hub and spoke and fully meshed infrastructure.



Use case 1

High-assurance network security for a simple 100Gbps point-to-point data centre to data centre service provider – an ultra-fast performance network requiring maximum data security.

This data centre-to-data centre application enables safe and highly cost and performance efficient data back-up and multi-redundancy disaster recovery capability.

A key advantage offered by the CN9120 is the QSFP28 interface for up to 80kms signal transmission enabling optimal MAN performance and benefiting the service provider through savings on the cost of additional OTN network hardware that would otherwise be necessary.

Use case 2

Senetas CN9000 Series encryptors' support for all Layer 2 topologies is something no other vendor may claim today. Consequently, support for multi-point-to-multi-point campus-style networks and topologies offer a major customer benefit.

In this campus network, research, scientific and medical 'mega data' is captured, aggregated, shared and analyzed in real time.

Ultra-low latency (a customer environment average of just 1.5 micro-seconds) and no detectable bandwidth loss on data encryption overhead ensures real-time collaboration.

Use case 3

For a large-scale, international cloud computing service provider, CN9100 encryptors provide maximum backbone security for the delivery of a range of Software-as-a-Service (SaaS) solutions.

This increasingly important use case typically requires multi-point or hub-and-spoke network topologies. It is where no other high-assurance 100Gbps solution is likely to offer a solution.

Cloud and SaaS service providers are aware that enterprise and government customers are risk-averse. They demand high-assurance encryption security and ultra-low latency. In this instance, 10/25/40Gbps links are aggregated for single 100Gbps link data transmission.

Network topologies for data aggregation can also be complex. These customers are also aware that if today's 100Gbps high-assurance 'mega data' network encryption solution only supports limited topologies; their investment may become redundant in the short term.

Use case 4

Multiple data centre-to-data centre applications supporting both 'mega data' cloud, data storage and back-up services often requires a hub-and-spoke network topology.

Both private and (public) service provider use cases for 100Gbps links within such networks often comprise multiple topologies. These customers prefer support for all topologies to ensure a flexible and cost effective solution.

Additionally, within the overall data network there will be a variety of link bandwidth speeds – from modest 100Mbps to high speed 1Gbps and 10Gbps.

Customers prefer or demand that all the vendor's encryptors are 100% interoperable. The Senetas interoperability extends well beyond 'among current products', to fully backward compatible.

Here ultra-low latency, near-zero data overheads and support for all topologies may be necessary to fully meet customer requirements.

This use case highlights typical total cost of ownership (TCO) and return on investment (ROI) requirements that are met by the CN9000 Series.

Use case 5

A large scale, global cloud services provider's ultra-fast network infrastructure backbone linking major customer locations; internationally distributed data centre facilities; and a wide range of SaaS delivery locations.

The customers' business case included three competing requirements:

- Maximum high-assurance encryption security
- No detectible reduction in network performance
- Future-proof and 'end-to-end' network interoperability investment – from ultra-fast, to high-speed to modest Layer 2 network links, supporting all topologies.

In this use case, maximum data security and network performance were pre-requisites. Also, because of the sensitive nature of the data carried by government customers, the solution needed to be certified as suitable for government or defence applications.

Use case 6

Commercial provision of 100Gbps national and international fibre network links to enterprise and government customers.

In this instance, the customer's 100Gbps links were used to support SaaS, cloud-based 'mega data' applications and data centre interconnect services.

Additionally, the customer already encrypts Layer 2 Carrier Ethernet 10Gbps and 1Gbps links to meet government customers' requirements for FIPS certified high-assurance network data encryption security.

The certified high-assurance encryption of

the 100Gbps 'backbone' links is provided by Senetas CN9100 and CN9120 (WAN and MAN respectively) encryptors. Similarly, the 1Gbps and 10Gbps high speed links are protected by Senetas CN6010 and CN6100 encryptors respectively.

In addition to certified high-assurance requirements, it was essential that the Senetas solutions provided:

100% encryptor interoperability among CN6000 and CN9000 Series encryptors and any future Senetas CN products implemented

Support for all topologies by all CN Series encryptors

- The same crypto-agility and Quantum ready features among all CN Series encryptors
- Flexible multiple topology support within the overall architecture.

The service provider's multiple data centre-to-data centre data transmission and aggregation and storage and back-up are included in the complex network architecture.

Use case outcomes

The certified high-assurance security capabilities of the CN9000 Series encryptors have operated without any measurable network performance compromise in either customer use case.

In both the customer and service provider use cases, two network performance measures have been beneficial and supported the 100Gbps networks' business cases:

Ultra-low latency. In all practicalities, the experiences have been real time with consistent latency at approximately 1.5 micro-seconds.

Near-zero data overheads. Senetas technology fully meets the customer performance and security demands without compromising bandwidth availability.

Like all Senetas CN encryptors, the CN9000 series platform provides high-assurance security and full line-rate transparent encryption for data transmitted across dark fibre, metro area, local area and wide area Ethernet networks in all topologies.

The state-of-the-art, automatic zero-touch encryption key management capability in all Senetas CN encryptors removes the reliance upon external key servers; providing a robust, fault-tolerant security architecture.

The secure and tamper-proof chassis also gives uncompromising protection to key material held in the encryptor.

End-to-end authenticated network data encryption is essential to high-assurance solutions. This ensures that even at 100Gbps ultra-fast bandwidth speed there is never a point or 'hop' at which data is not 100% protected.

Standards based encryption algorithms are also essential for high-assurance. In all these cases AES256 has been the standard.

Full interoperability among all Senetas CN series encryptors provides end-user customers with peace of mind not often available from other network encryption solutions.

Designed-in crypto-agility and solution flexibility is a hallmark of the entire CN Series range. The flexible and efficient FPGA architecture enables flexibility of custom solutions and advanced 'future-proof' crypto-agility.

With Quantum computing on the horizon, unnecessary redundancy is eliminated by the CN Series encryptors' 'Quantum ready' features.

100% network device compatibility allows all customers and partners to standardise on one platform. This has resulted in both low TCO and high ROI – quite a rare experience with technology products.

From the outset, both variants of the CN9100 encryptors proved their security and network performance - in partner testing and in customer proof of concept deployments – well beyond simple lab testing.

As Senetas 'security aware' customer organisations seek to maximize their secure 'mega data', Cloud Computing and data centre solutions, they are also sensitive to the need for both certified high-assurance encryption and maximum 100Gbps network performance.

Support for all topologies

Whatever the chosen network topology and technology use case, Senetas CN9000 Series encryptors ensure maximum 100Gbps security for Big Data, Cloud and data centre applications across point-to-point, multi-point and fully meshed network topologies.

Sample use case mandatory requirements

Primary Specification	Senetas **CN9100**	Senetas **CN9120**
Customer profile	Multi-national commercial enterprise – Fortune 500 profile	Global Cloud Services provider to government & enterprise customers
Network design	Local Area	Metro Area
Transceiver type	Interface – (up to approx. 10Kms)	Interface – (approx. 70Kms)
Bandwidth	100Gbps	100Gbps
Customer Application	Big Data / 'Mega Data' applications	Global Cloud services and multiple data centre back-bone/s.
Security Requirements	Robust, high-assurance network encryption	FIPS certified, high-assurance encryption
Network performance requirements	Zero impact on 100Gbps bandwidth Business Case	Zero impact on 100Gbps bandwidth applications Business Case
Latency	Low latency <4 micro-seconds	Low latency <3 micro-seconds
Data overheads	Minimal	Near-zero
Transceiver connectivity	Regular distance transceiver signal	Must enable 'long haul' transceiver signal to avoid net-work OTN costs
Security performance require-ments	Maximum – high-assurance components	Maximum – per FIPS certification
Certifications	N/A	FIPS
High-assurance attributes	Yes	Yes
Automatic 'zero-touch' key management	Yes	Yes
No adverse impact on 100Gbps network performance	Yes	Yes
High ROI	Yes	Preferred
Efficient TCO	Yes	Yes
'Real time' applications performance	Yes	Yes
Network architecture / topology - hub & spoke, fully meshed, 'multi-point'	Yes	Yes

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.

CN9KUC-SP0821

SENETAS