HIGH-ASSURANCE ENCRYPTION OF MAN INFRASTRUCTURE FOR "SMART CITY"

CAPABILITIES CASE STUDY

Application of High-Assurance Network Encryption	
Sector:	Local and state governments
Use Case:	Secure Ethernet Metro Area Network
Solution:	Secure encrypted MAN infrastructure for "Smart City"

SENETAS
Security without compromise

A major municipality is making a multi-million-dollar investment in a secure, encrypted Metro Area Networking solution that supports the communications needs of more than 20 separate agencies.

OVERVIEW

In a move to improve service performance, availability and security, the large-scale networking solution will deliver essential voice, video and data services to police, fire, healthcare, waste management agencies and more.

In essence, the new metro area network solution makes the concept of the "digital city" a reality.

Stakeholder data security was an essential component of the project from the outset. The municipality specified the need for a high-assurance encryption solution and chose Senetas encryptors as they offered the best combination of security and performance

BUSINESS NEED

The effective delivery of services for a modern municipality are as dependent upon its IT and communications infrastructure as any commercial organisation.

The seamless integration of network services across multiple service agencies and departments generates significant cost savings, process efficiencies and performance improvements; helping the municipality deliver a better citizen experience.

While cost is always a consideration, a public services network also must feature robust network data security to ensure the integrity and privacy of large volumes of potentially sensitive citizen data.

CHALLENGE

Deliver an integrated high-performance voice and data network with state-of-the-art security.

The solution would need to support 20 individual agencies across a major metropolitan area and ensure "government-grade" encryption whilst minimising any impact on network performance.

CONSIDERATIONS

Any organisation planning a major infrastructure project will have a range of networking solutions to choose from and our client considered technologies from all the leading vendors.

A 'Software Defined Network' infrastructure was the technology of choice, because of its inherent simplicity, scalability, flexibility and cost-effectiveness.

Other solutions were ruled out because of what was seen as unnecessary complexity or capital expenditure.

SOLUTION

The Software Defined Network infrastructure, featuring high-assurance network data encryption from Senetas.

Key benefits of the Senetas high-assurance encryption solution included:

> Simplified communications infrastructure

> Seamless and end-to-end network encryption

> Converged voice and data network

> High-assurance data encryption standards

> Scalable, low-latency, fully compatible

> Proven certified security performance

WHY SENETAS NETWORK ENCRYPTION

Although the networks' data security requirements were implicit, both the network systems vendor and its customer demanded that the encryption solution be high-assurance.

It was also essential that the encryption devices themselves should be transparent to the network and not compromise network performance by adding latency or data overhead.

SECURITY FIRST

Given the plethora of public sector data breaches over the past few years, our client placed a premium on network data security.

Data encryption was seen as a "must-have" to ensure the security and integrity of citizen data as it moved across the network. However, the client would not accept a solution less than high-assurance.

So-called "embedded encryption" network devices were ruled out almost immediately as they were seen as a potential point of vulnerability and would require on-going management to affect software updates and patches. Such devices also have future compatibility issues.

MACSec was seen as a low-assurance option, one with vulnerabilities or weaknesses that may expose network data to unnecessary risk.

The network provider selected high-assurance encryption solution from Senetas that had recently completed systems integration trials with Software Defined Networks.

The client was immediately sold on the benefits of truly robust encryption that did not impact on network performance or add any unnecessary management overhead.

The choice is also future-proof, due to Senetas CN encryptors' interoperability and network device compatibility.

HIGH-ASSURANCE ENCRYPTION

In order to be truly robust, high-assurance encryption needs to feature:

> Secure, dedicated, tamper-proof encryption hardware

> State-of-the-art, automatic 'zero touch' key management

> End-to-end, authenticated network encryption

> AES standards-based encryption algorithms

KEY BENEFITS

Seamless integration with the chosen network architecture – with identical performance and management efficiency.

Maximum network security without compromising on performance or availability – near-zero latency and zero impact on network devices and operations.

Set and forget simplicity – all Senetas encryptors are fully interoperable and are managed both locally and remotely.

Peace of mind that comes from a genuinely robust encryption solution (what the FBI refers to as "unbreakable encryption").

In summary the Senetas CN Series encryptors provide the municipality with high-assurance network encryption security:

> Maximum network performance for Big Data applications and analytics

> Ultra-secure, client-side encryption key management

> Ease of deployment, configuration and management

> <6 microsecond latency and near zero data overheads

> FIPS Level 3 140-2 certification meeting government requirements

> 100% compatibility across network protocols and topologies

> 100% interoperability among all Senetas CN devices

> Long-term return on investment and low total cost of ownership

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.

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.

FABCON-CS1017