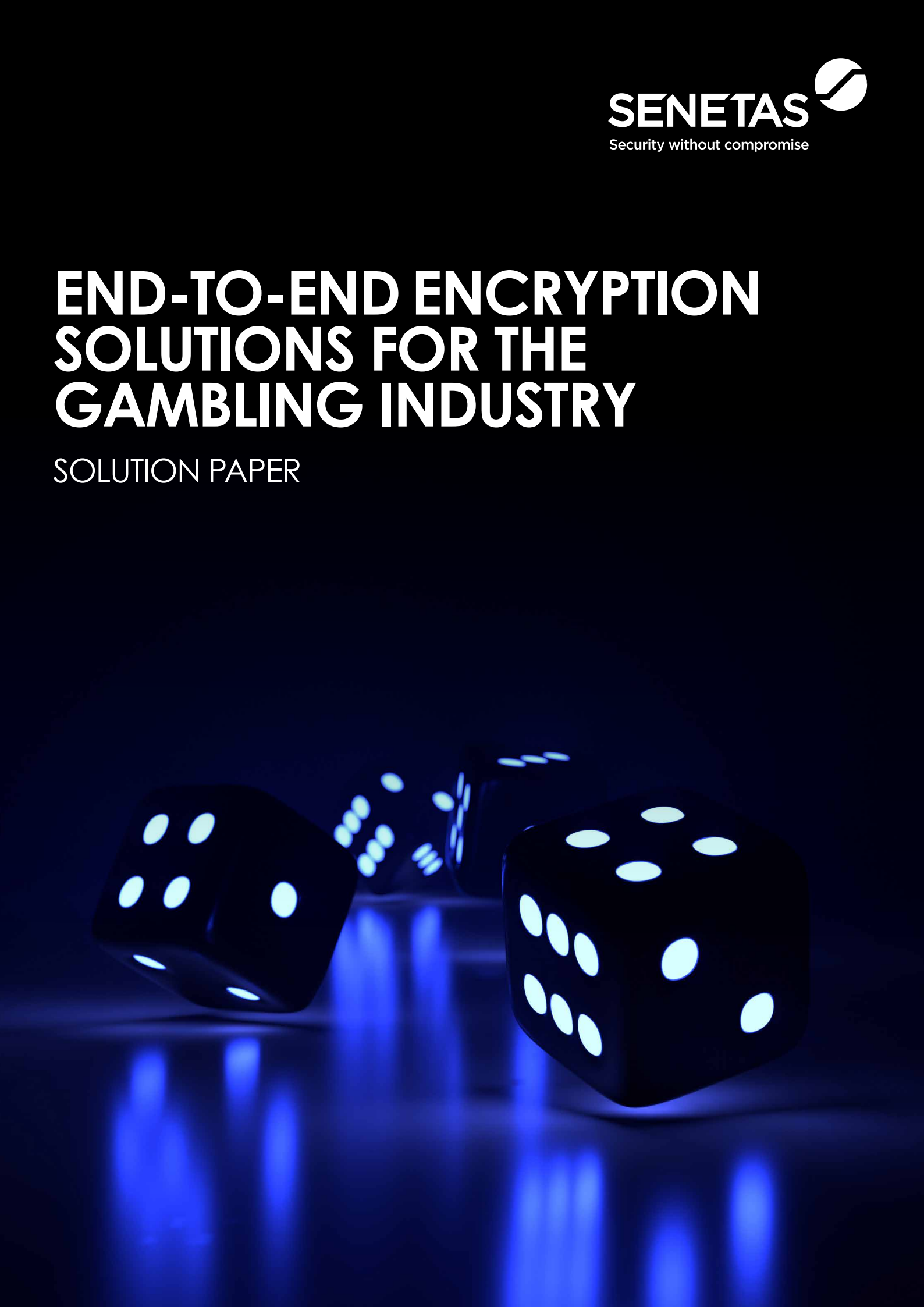
SENETAS
Security without compromise

END-TO-END ENCRYPTION SOLUTIONS FOR THE GAMBLING INDUSTRY

SOLUTION PAPER



GAME CHANGING TECHNOLOGY

Overview

The gambling industry (including casinos, manufacturers of gaming technology, lottery operators and sports betting companies) has becoming increasingly dependent upon CCTV, Big Data Applications, Cloud and Data Centre Services.

High speed network-delivered services not only enable the gambling industryto maximise financial and operational efficiencies, they also support regulatory control and compliance.

However, because of the potential for significant financial gain, the gaming industry is a high-risk, high-profile target for cyber-criminals.

In a big-data world, the information exchanged across an organisation's high speed networks is often of a sensitive nature.

The security and integrity of this data is essential, whatever its use:

- Personal safety
- Regulatory compliance
- Operational standards
- Asset protection
- Business analytics
- Financial transactions

Whatever the application, from HD CCTV to big data analytics, networks require high-assurance data encryption security and maximum network performance.

Where the gambling industry differs from other commercial sectors is its dependence upon:

- Real-time data availability
- 100% data integrity
- High-definition video
- Ultra-high speed network performance
- Unified data, video and voice

CCTV ENCRYPTION

CCTV Encryption

Robust encryption security and high speed data network performance are both essential to real-time HD CCTV monitoring.

This is where Senetas encryption solutions excel; delivering robust CCTV encryption without loss of network performance – the most challenging of network security tests.

As CCTV technology advances (EG: real-time HD streaming, face recognition, motion tracking and night-vision) the volume and sensitivity of data transmitted across an organisation's high speed networks increases.

Video content is tightly regulated in many countries. This not only impacts on the streaming of video content, but also on the storage, sharing and archiving of data.

The last, best line of defence is to ensure the data itself is protected. This means, when a successful network breach occurs, unauthorised parties are simply left with meaningless encrypted data.

Critical CCTV data protection issues include:

- Integrity – prevention of interference with CCTV footage (EG. input of rogue data)
- Reliability – provision of uninterrupted, real-time surveillance coverage
- Quality - 100% HD quality video with no noise, jitter or latency
- Privacy – compliance with identity and data protection obligations
- Complexity – CCTV systems typically comprise multiple devices

Traditional "border" security has proved to be ineffective when it comes to preventing network breaches.

Unlike other encryption solutions, Senetas high assurance encryptors provide maximum protection without compromising data network performance.

Real-world tests repeatedly prove Senetas CN Series encryption technology maintains maximum HD CCTV image quality and real-time CCTV network performance.

BORDERLESS INFRASTRUCTURE

Big Data, Cloud & Data Centre Services

The gambling industry continues to increase its use of Big Data applications and analytics to improve financial, competitive and operational performance.

The scalability, flexibility and on-demand nature of Cloud computing has proven popular within the gambling industry.

Organisations have been transitioning away from on-premises solutions as they seek operational efficiencies, greater systems availability, ease of management and lower cost of ownership of their IT infrastructure.

Consequently, data centre services have become essential resources for the processing, storage, backup and recovery of the rapidly growing volumes of data.

Systems redundancy and failover means this data is often located across multiple sites, to ensure business continuity.

As the gambling industry becomes more dependent upon high-speed data networks to facilitate day to day operations, it is inadvertently exposing itself to an increased risk of cyber-attack and the potentially catastrophic consequences of a data breach:

- Disruption of day-to-day operations
- Inability to meet compliance obligations
- Loss of reputation and brand equity
- Theft of intellectual property (IP)
- Financial penalties / loss or revenue
- Breach of data protection / privacy laws

High-speed data networks are not inherently secure. Organisations do not have 100% control over the networks they utilise. Consequently, the data travelling across these networks is vulnerable to:

- Eavesdropping
- Data theft
- Input of rogue data
- Data redirection
- User or technical error
- Criminal negligence

Notable Breaches

Casinos and gambling applications have a reputation for strict security, but they are not immune to cyber attacks. In recent years, the industry has been hit by several high-profile breaches.

The Hard Rock Casino was hit by a series of data breaches between 2015 and 2017. Attackers were able to steal credit card details of guests at the resort using malware installed on POS systems.

Throughout the second half of 2019 and into 2020 reports were rife about a group of hackers targeting online betting sites. Hacks were confirmed by several gambling companies across South East Asia.

In 2020 a huge data breach was discovered at Clubillion. The breach exposed personally identifiable information of millions of customers, including email addresses, private messages and details of winnings.

END-TO-END ENCRYPTION SOLUTIONS

CN Series Encryption Hardware

The CN Series of Ethernet encryptors provide certified, high-assurance data protection for core IT and communications network infrastructure.

All CN Series encryptors share a common encryption platform and are 100% compatible and interoperable.

CN Series hardware is used to secure sensitive data in motion across networks operating at anything from modest 10Mbps to ultra-fast 100Gbps bandwidths.

CN4000

Small form-factor (desktop) encryptors for 'in the field' network link security (e.g. CCTV) – offering 10Mbps, 100Mbps and 1Gbps bandwidth speeds.

CN6000

Rack-mounted high speed encryptors for business-critical applications – offering 1Gbps to 10Gbps bandwidth speeds.

CN9000

Ultra-high bandwidth, rack-mounted encryptor with "mega-data" performance – offering speeds of up to 100Gbps.

CV Series Virtualised Encryption

The CV1000 virtual encryptor provides strong and effective data encryption for large-scale and virtualised wide-area networks.

Scalable to thousands of end-points, the CV series of virtual encryptors is a software application of the trusted Senetas encryption platform. It delivers cost-effective, transport Layer agnostic data protection at up to 15Gbps (with DPDK).

As a Virtualised Network Function (VNF) that will run on any x86 hardware, the CV Series virtual encryptor is 100% interoperable with Senetas CN Series hardware encryptors and is built on FIPS compliant technology.

SureDrop Encrypted File Sharing and Collaboration

SureDrop delivers the file-sharing convenience of popular box-style applications, but with the addition of end-to-end encryption security and 100% data location control.

It also offers users a choice of the resilience of a bespoke, on-premises solution or the flexibility of a managed service provider solution.

SureDrop clients include government agencies and service providers that are concerned about the inherent risks associated with sharing documents outside of their protected LAN.

SureDrop represents a new way to enjoy secure file sharing; with the emphasis on delivering a service that meets the needs of large commercial and government organisations who are required to frequently share sensitive and confidential information across the web.

SureDrop also provides organisations with the user-authentication security benefits of active directory compatibility.

Votiro Secure File Gateway

VOTIRO

Votiro Secure File Gateway leverages patented, next generation anti-malware technology to proactively protect your files from the most advanced, persistent cyber-attacks.

It sanitises incoming, shared and stored files, enterprise-wide; eliminating the risks associated with both known and zero-day, or undisclosed, attacks. At the same time, it preserves 100% of original file content and functionality, without disrupting user workflows.

WHAT MAKES SENETAS STAND OUT?

Best Performance

High-speed

The designed-in, market-leading performance capabilities of Senetas encryption solutions are what make them stand out from the crowd.

Whether operating at 10Mbps, 100Mbps, 1Gbps, 10Gbps or 100Gbps; time after time, they consistently win competitive performance tests.

Their encryption speeds, near-zero data overhead and near-zero latency make Senetas encryption solutions ideally suited to the most demanding network environments.

Ultra-low latency

Senetas high-speed encryption solutions operate in full duplex mode at full line speed 99.99% without loss of packets.

Latency is not affected by packet size (<2 microseconds per unit at 100Gbps) meaning maximum throughput with near zero protocol overhead.

Importantly, by using Field Programmable Gate Array (FPGA) technology, this outstanding performance is predictable and dependable.

Zero impact

The zero impact of Senetas encryptors is not limited to network bandwidth and latency; it extends to network operations and management.

They simply fit in within the user network. They don't require changes to other devices or network reorganisation; making them a favourite among network engineers.

High-Assurance

Certification in-depth

Senetas CN Series encryptors include the only multi-certified products of their types, as a result they are trusted by governments and defence forces around the world.

Rigorous testing is carried out over many years and provides our government and commercial customers with maximum confidence. Senetas CN Series encryption solutions are certified by: FIPS, Common Criteria and NATO.

For over 20 years, Senetas R&D has included a commitment to 'certification in depth'. Customers value the benefits of exhaustive and ongoing testing authorities' product evaluation.

Best encryption key management

All Senetas products adopt state-of-the-art encryption key management. Your encryption keys are only ever held by and accessible to you, on your premises; securely stored and encrypted.

Solution integrity

Senetas encryptors provide maximum solution integrity; unlike 'low assurance' solutions, such as router-based network data encryption or multi-function devices with embedded encryption.

Senetas high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption with standards-based (AES256) encryption algorithms.

Versatile & Simple

Crypto-agility

All Senetas encryption solutions are agile by design; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility.

Selected Senetas encryptors also support Quantum Key Distribution (Quantum Cryptography) and Quantum Random Number Generation, for long-term data security.

Support for all topologies

Senetas CN series encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies. Senetas CN9000 encryptors are the only 100Gbps encryptors that support multipoint-to-multipoint topologies.

Custom encryption

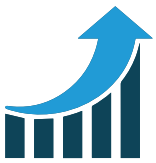
In addition to the standards-based AES256 and 128-bit algorithms, Senetas CN series encryptors support the use of customer-requested algorithms, custom curves (BYOC) and entropy (BYOE).

Ease of use

Set and forget simplicity and network transparency are underlying Senetas design themes. They ensure ease of implementation, operation and management. All Senetas encryption solutions feature automatic zero-touch key management. They also feature automatic network discovery and connection.

Local or centralised management

Configuration may be performed locally or remotely through the intuitive Senetas CM7 management software; which acts as the Certificate Authority in a network of encryptors by signing and distributing X.509 certificates.



Low Cost, High Efficiency

Suitability

All Senetas CN Series solutions operate at full line speed; enable maximum network performance and deliver 'set and forget' management simplicity.

The business investment case out-performs even 'cheap and cheerful' low-assurance solutions that prove very costly over time.

It is not necessary, nor beneficial, to opt for low-cost, low-assurance solutions to meet the toughest business case and TCO requirements.

Cost-efficiency

Senetas encryption solutions provide excellent TCO through a mix of network bandwidth savings, ease of management and reliability.

Longevity, interoperability, backward compatibility, minimal installation and management costs and solution flexibility all contribute to a rapid ROI.

Other cost benefits include, low power consumption minimal rack space use and combined rack space/ power utilisation efficiency.

Reliability

All Senetas hardware encryption solutions boast 99.999% uptime. Carrier-grade, rack mounted devices are hot-swappable and provide further network operations uptime benefits thanks to dual redundancy of consumables, such as fans and power supplies.

Flexibility

The use of FPGA technology enables maximum operational flexibility. This enables on-going operational simplicity, such as infield upgradability, as customers' requirements change; helping to protect their investment in technology.

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 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 5Gbps. 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 Disarmer extension.

DISARM MALICIOUS CONTENT

Votiro Disarmer 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.

GAM-SP0421

SENETAS