SENETAS

Beyond Theory: Real World Encryption for Modern Networks

Contents

1. Company Overview
2. Use Cases
3. Post Quantum
4. Innovations, Credentials & Products

SECTION 1

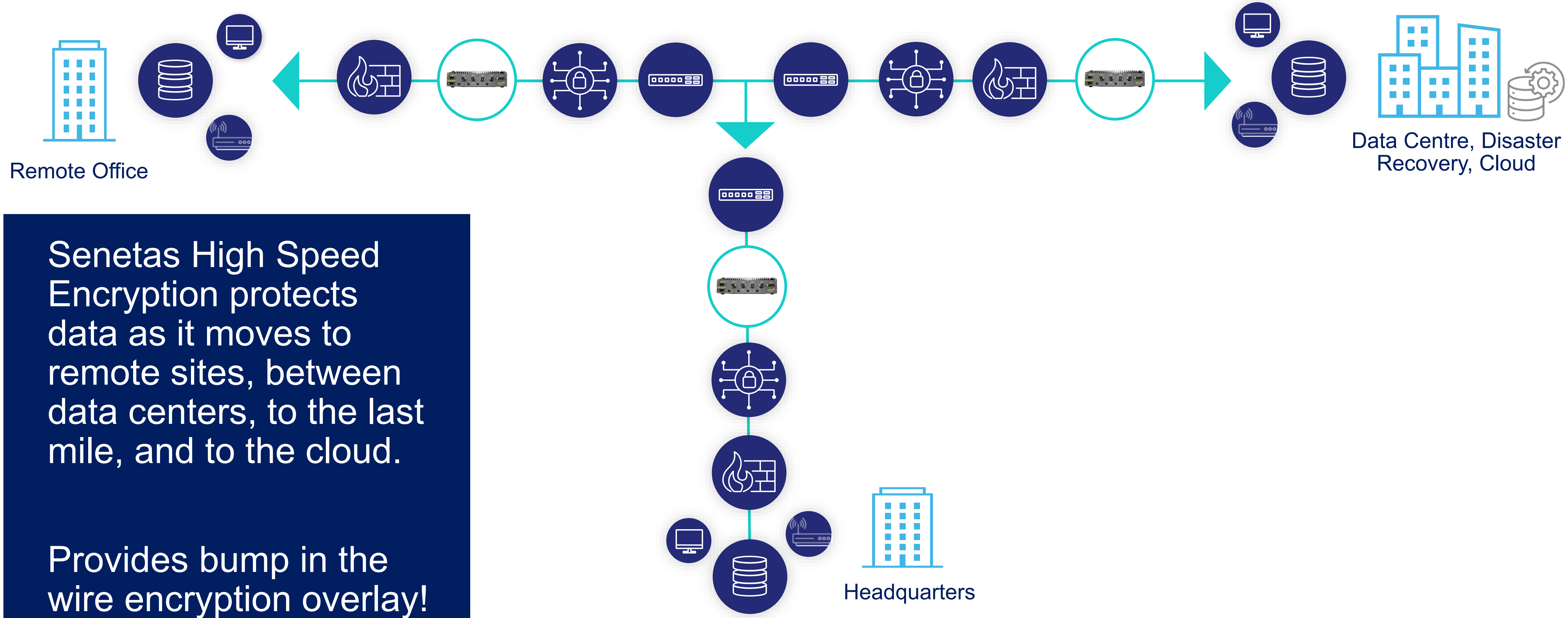
Company Overview

Introduction

- **Trusted Australian Cybersecurity Leader**: More than 25 years of experience protecting sensitive data in more than 60 countries.
- **Specialized Solutions:** Australian-designed and manufactured defence-grade high-speed network encryption, as well as secure file sharing.
- **Advanced Performance**: Deliver quantum-resistant and crypto-agile performance without compromising speed or user experience.
- **Certified Technology**: Award-winning technology is certified by top security authorities.
- **Global Delivery**: Solutions are delivered worldwide in partnership with Thales, a global leader in advanced technologies.

CELEBRATING 25

Encrypting data in motion



Senetas High Speed Encryption protects data as it moves to remote sites, between data centers, to the last mile, and to the cloud.

Provides bump in the wire encryption overlay!

Our Approach

- Traditional encryption standards such as MACsec (IEEE 802.1AE) and IPsec (RFC 2401, 1998) have provided essential security for network communications.
    - Standards designed for simpler network topologies don’t always scale efficiently in modern, complex network infrastructures.
- Emerging network deployments necessitate a more flexible and lower-overhead encryption approach.
    - Evidenced by the various proprietary vendor extensions to these standards.
- Our design strategy focuses on delivering modern solutions for modern networks.
- Assurance remains a core requirement including FIPS140-3, Common Criteria, DoDIN APL and NATO certifications.

High Speed Encryption (HSE)

- **Purpose-built encryption appliances**
  Hardware and virtual options available.
- **Network Fit**
  Compatible with any network topology and type.
- **High Assurance Security**
  Tamper-proof enclosure, hardware encryption engine, and hardware random number generators (RNG).

- **Security Certifications include**
  - FIPS140-2 Level 3
  - Common Criteria EAL2+, EAL4+, NPcPP
  - DoDIN APL
  - NATO (NIAPC)
  - ASD Evaluated Products List
- **Future Proof**
  Secure against quantum computing threats (FPGA).

SECTION 2

Use Cases

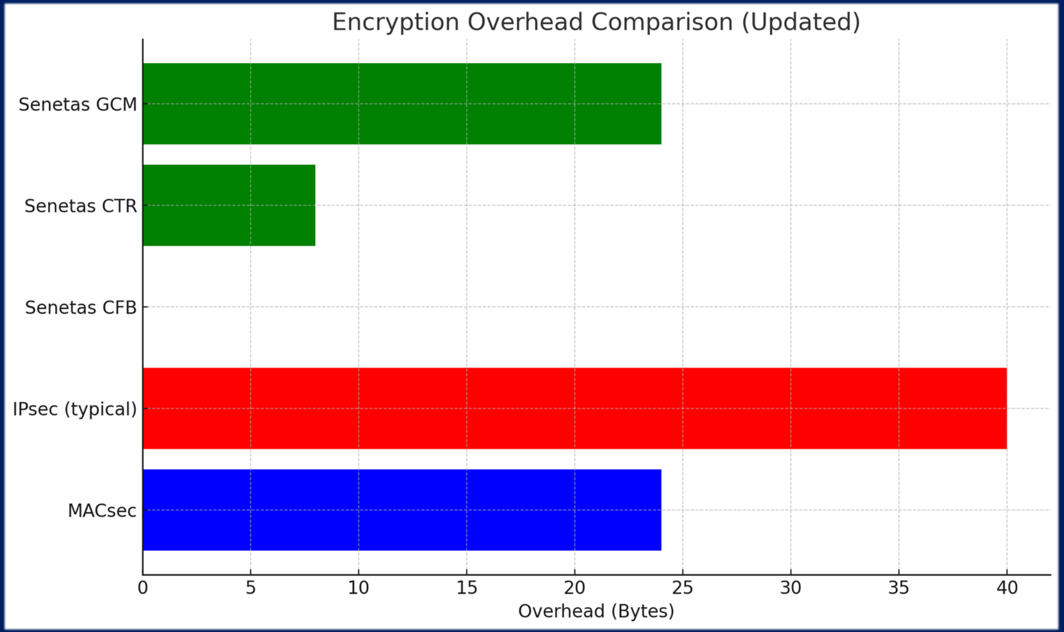
HSE: Private Links (Line Mode)

Challenge:

- **Common Use Case**: High-speed encryption for dedicated data centre links.
- **Dedicated Links**: Typically dedicated dark fibre or leased lines.

Solution:

- Point-to-point encryption in Line Mode.
- Low-latency, deterministic encryption for financial or other operational transactions.
- Simple drop-in installation and set-and-forget operation.
- Supports PKI X.509 certificates (external and internal CA) with standards-based cryptography.



- As speeds increase, so does the impact of overhead!
- Not all dark fiber links are as they appear!

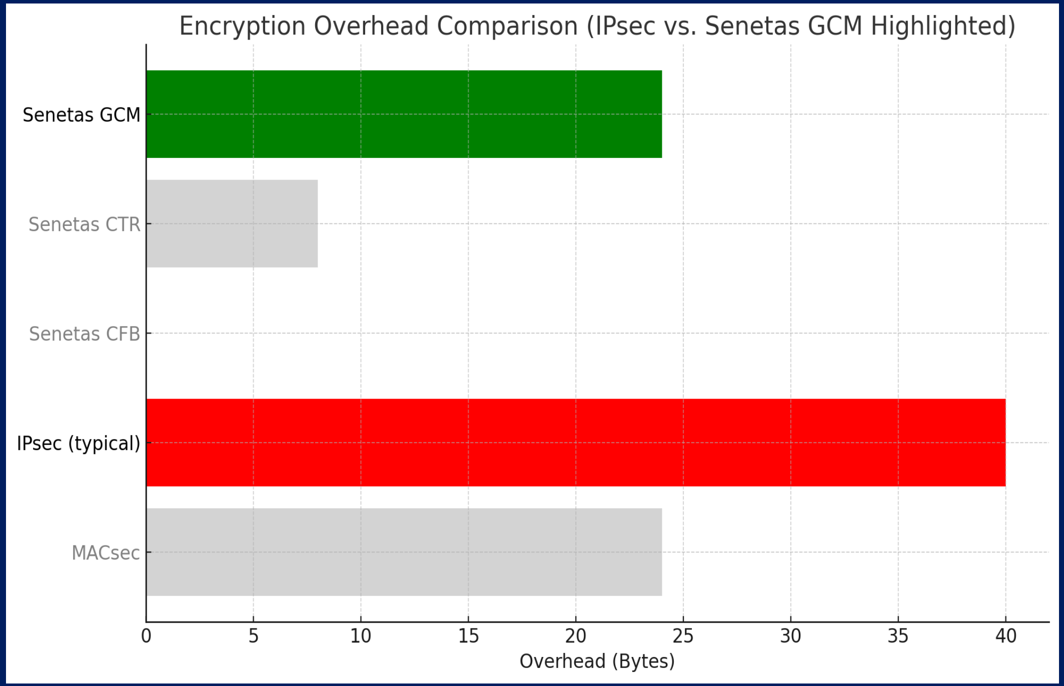
HSE: European Air Traffic Control: MPLS & TIM

Challenge:

- Customer needed to encrypt MPLS backbone traffic (between PE and backbone).
- Implement redundant network infrastructure with two independent vendor sets and providers.

Solution:

- TIM (Transport Independent Mode) fully meets requirements.
- Highly scalable due to its control plane-less design.
- Supports both mesh and hub-and-spoke network topologies.
- Enables simultaneous L2/L3 and L4 operation based on policy.



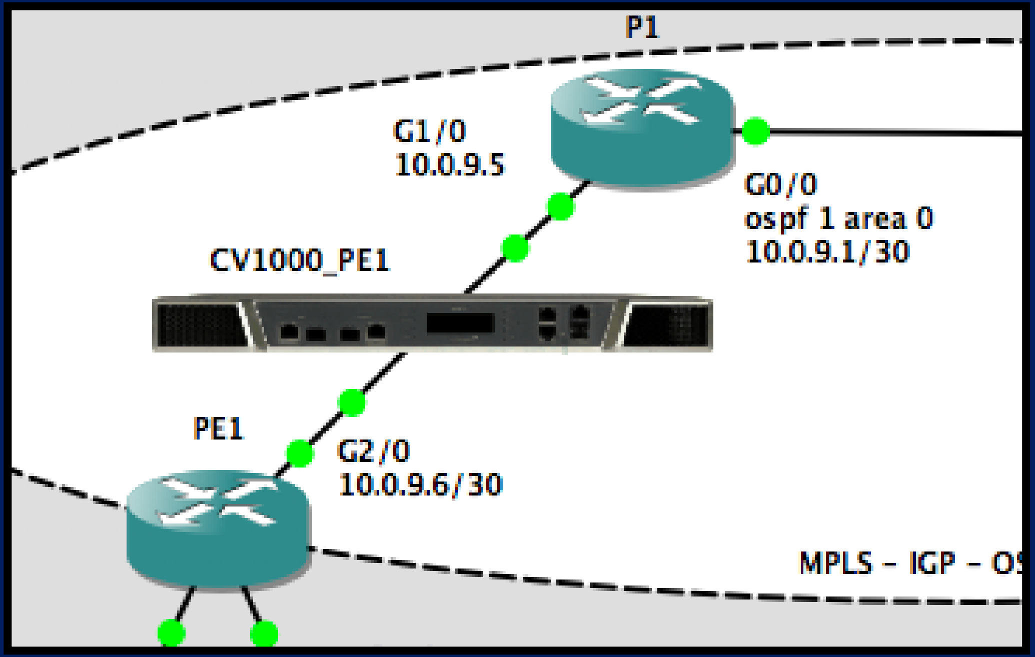
HSE: Transport Independent Mode

Challenge:

- Encryption required between Provider Edge and Backbone.
- BGP, OSPF fabric protocols must be bypassed.
- MPLS labelled customer traffic must be encrypted.
- PHP (Penultimate Hop Popping) can remove labels on egress - (explicit-null) to disable.

Solution:

- Prototyped under RAD and PoC trials were executed.
- Ultimate solution implemented in FPGA, offering low latency and deterministic performance.



SENETAS

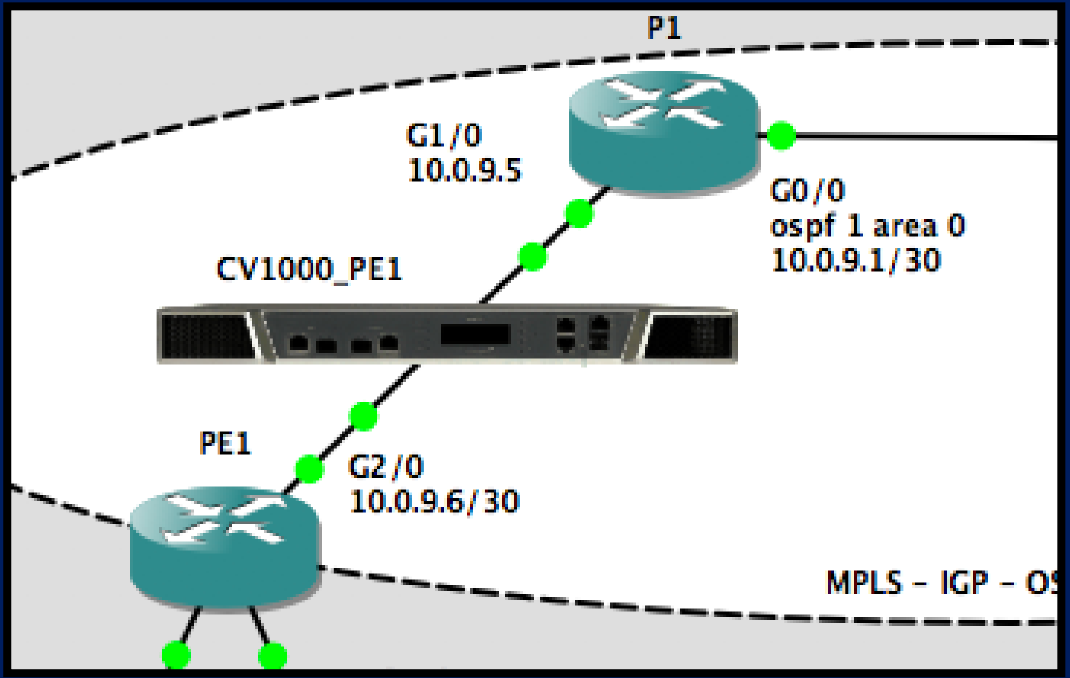
HSE: SD-WAN & Transport Independent Mode

Challenge:

- Encrypt multiple transport channels in SD-WAN deployment.

Solution:

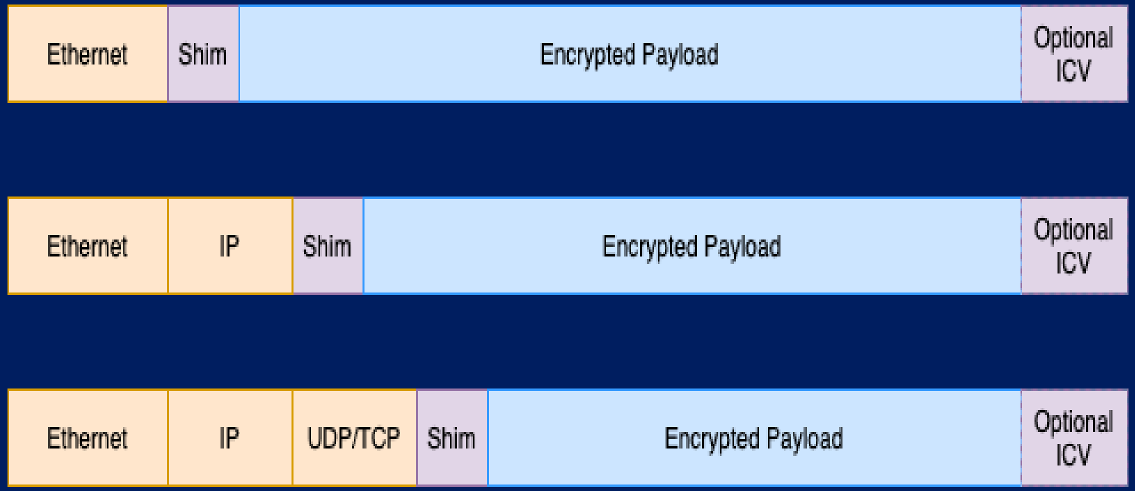
- TIM Mode enables concurrent encryption at L2, L3, or L4.
- SD-WAN flows can be encrypted at the most secure layer across various transports: MPLS, Internet, Leased Line.



HSE: SD-WAN & Transport Independent Mode

Solution:

- Encryption application is policy-driven.
- GCM adds an optional 16-byte ICV for integrity and authentication.
- Supports transport mode encryption only (not tunnel mode).
- Encryptor operates as a bump-in-the-wire/fibre.
- Tunnel encryption is independent and customer-managed (e.g., GRE/VXLAN).



Ethernet | Shim | Encrypted Payload | Optional ICV

Ethernet | IP | Shim | Encrypted Payload | Optional ICV

Ethernet | IP | UDP/TCP | Shim | Encrypted Payload | Optional ICV

- All frames include an 8-byte encryption shim.
- Shim placement is after Layer 2, 3, or 4 headers.

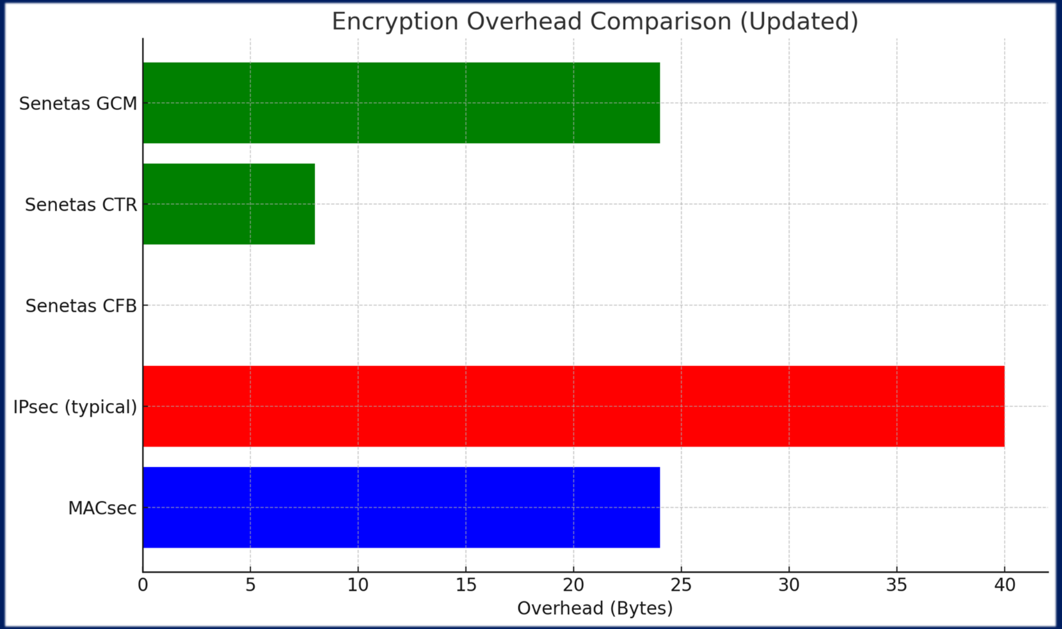
HSE: CCTV Performance

Challenge:

- Australian Customs requires high-speed, jitter-free encryption for CCTV feeds.

Solution:

- CCTV traffic typically uses small delta frames.
- Traditional cryptography like IPsec adds jitter and latency.
- Resulting in unusable CCTV Motion Control (e.g., Hitachi Pan and Tilt).
- Attempts with IPsec equipment suppliers were unsuccessful.
- The customer required a higher-performance solution.

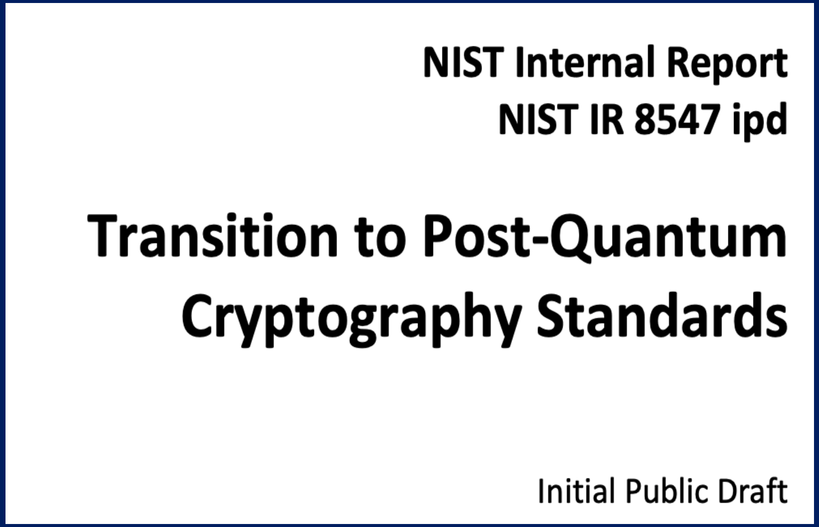


- Our encryption appliances can operate with zero performance impact, depending on the mode.

SECTION 3

Post Quantum

Crypto Agility: Post Quantum Hybrid Encryption



NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

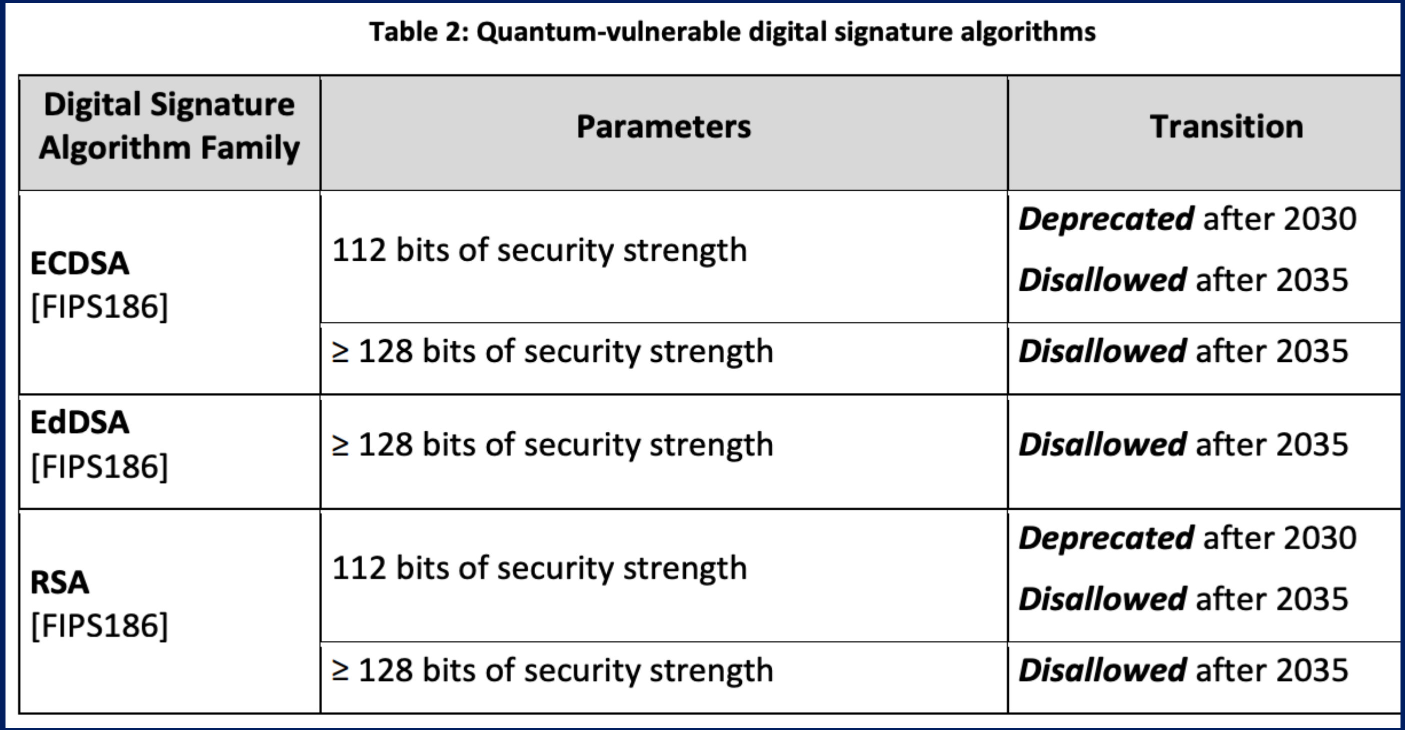


Table 2: Quantum-vulnerable digital signature algorithms

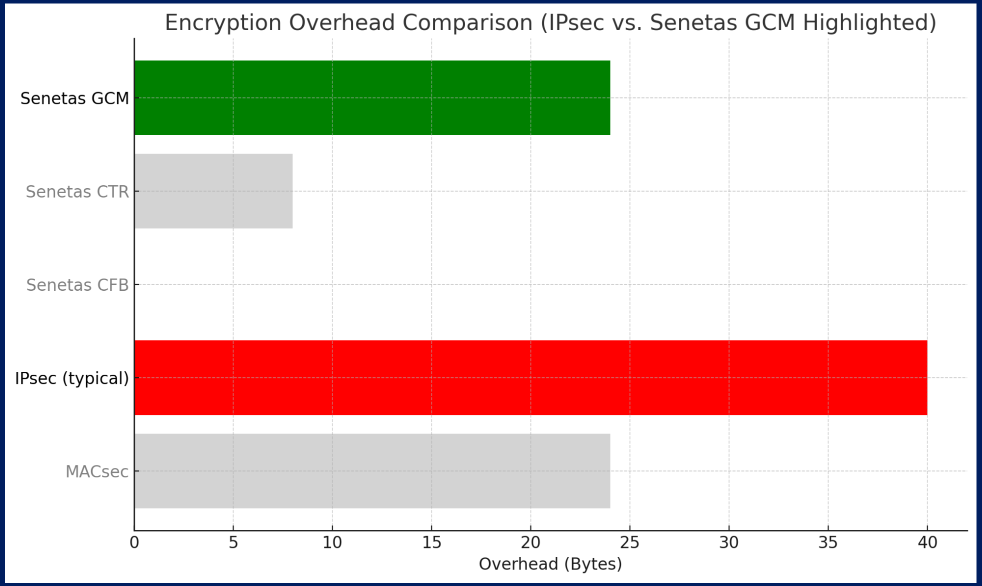
Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Crypto Agility: Post Quantum Hybrid Encryption

- This guidance is already within a typical switch, router or firewall refresh cycle (5-7 years).
- Senetas devices are FPGA based, field upgradable devices.
- No rip and replace of ASIC based devices.

What was our process:

- PQC implemented in hybrid mode in early 2020's.
- PQC fully integrated in PKI/X509 for ease of use.
- QKD – first implemented in 2007, then updated.



- Available in VLAN/LINE/MAC Mode.
- TIM quantum safe by design (no control plane).

Crypto Agility: QKD + Quantum safe hybrid scheme

Multiple AES Keys can be established using

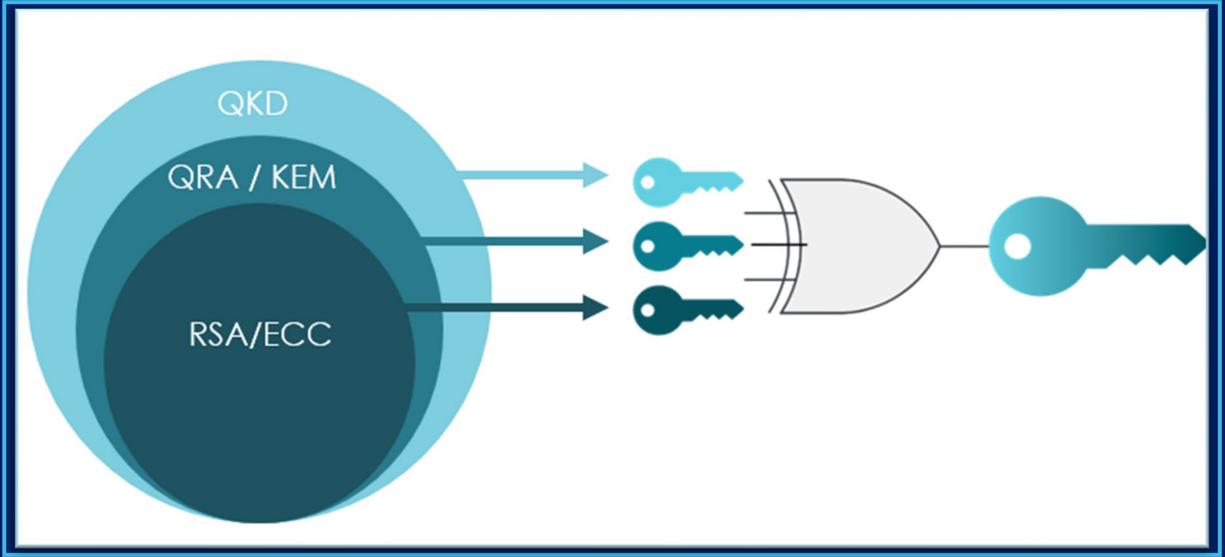
- Conventional RSA/ECC key exchange and
- Quantum resistant Key Establishment Mechanism and/or,
- Quantum Key Distribution.

Individual keys are securely combined.

Provides enhanced defence-in-depth.

No performance loss.

FIPS compliant operation.



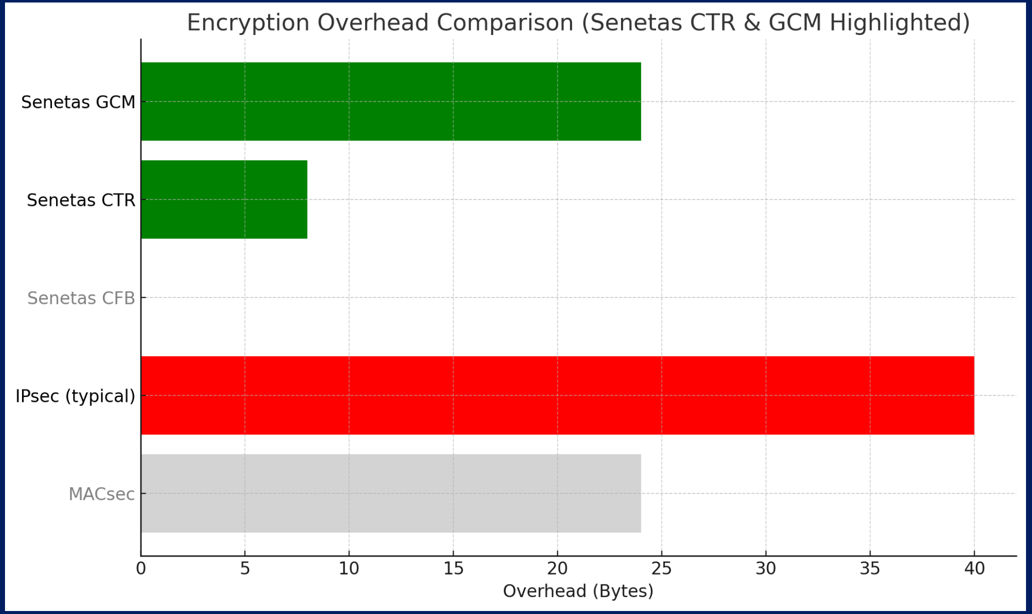
HSE: VLAN Mode

Challenge:

- A bank customer with a large, multi-VLAN tagged network needs group key separation aligned with VLAN broadcast domains.

Solution:

- VLAN group key mode is fault-tolerant and self healing.
- Operates seamlessly at L2.
- PKI X509 certificate support (External and Internal CA).
- Support VLAN Auto-discovery for connections.



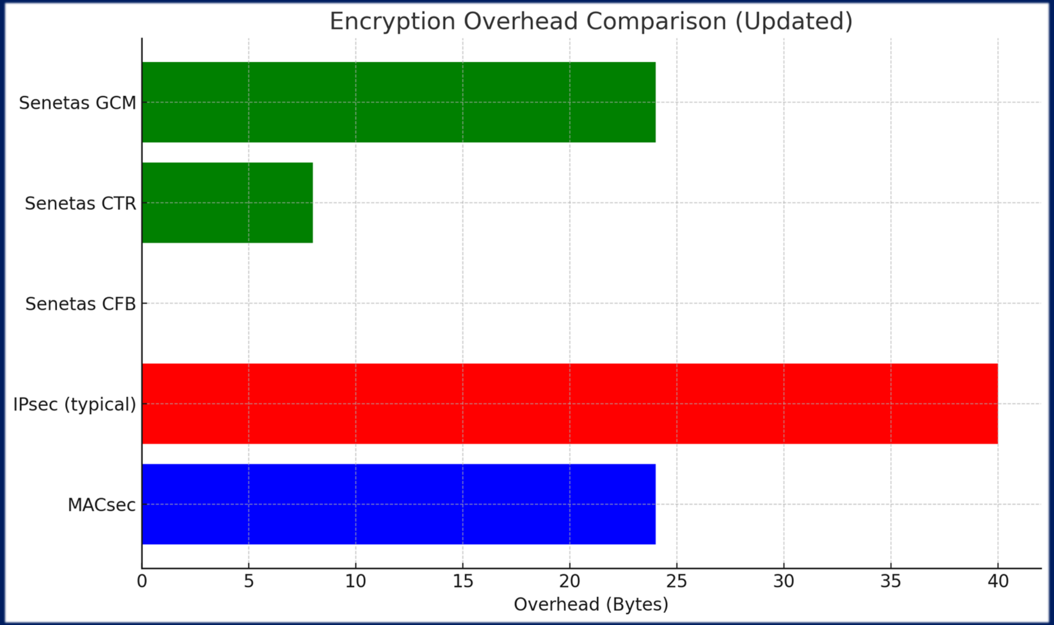
HSE: Transmission Security

Challenge:

- Customer needed high-speed encryption providing transmission security.

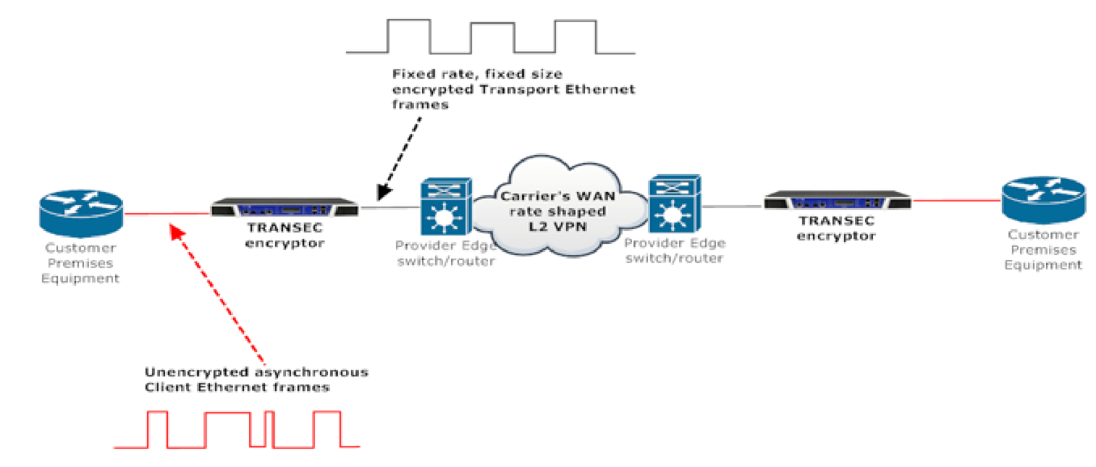
Solution:

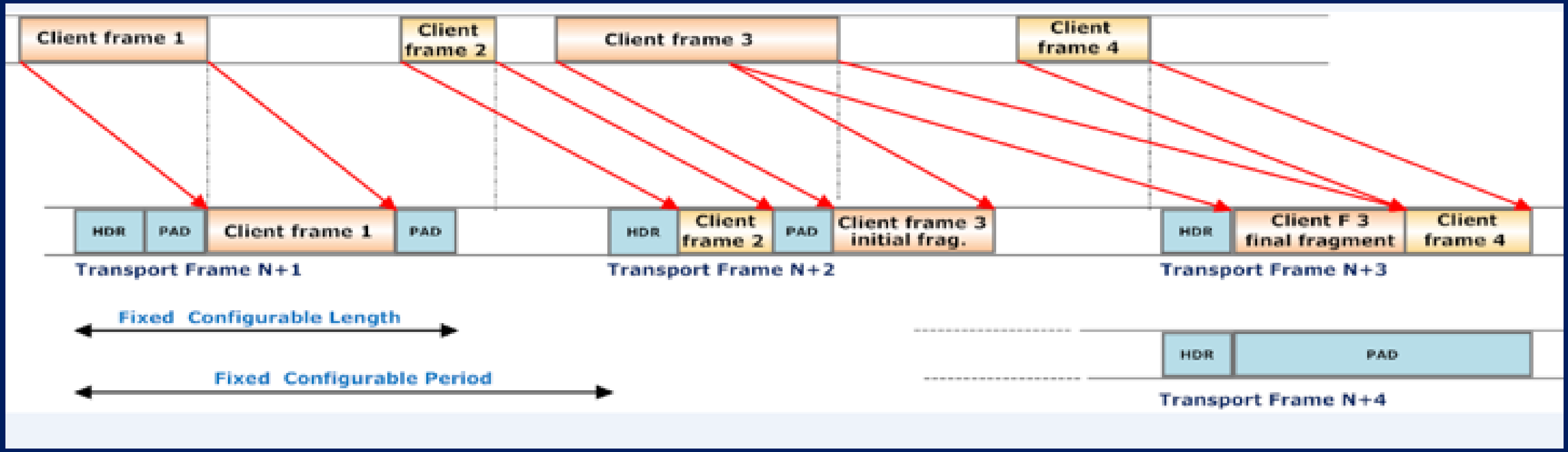
- Low latency, deterministic encryption for financial & operational transactions.
- Drop in installation and set and forget operation.
- PKI X509 certificate support (External and Internal CA).



HSE: Transmission Security

- Prevents traffic analysis by hiding patterns in the encrypted data.
- Outputs fixed size, fixed rate packets.
- Layer 2 point-to-point only.


Fixed rate, fixed size encrypted Transport Ethernet frames
Customer Premises Equipment
TRANSEC encryptor
Provider Edge switch/router
Carrier's WAN rate shaped L2 VPN
Provider Edge switch/router
TRANSEC encryptor
Customer Premises Equipment
Unencrypted asynchronous Client Ethernet frames



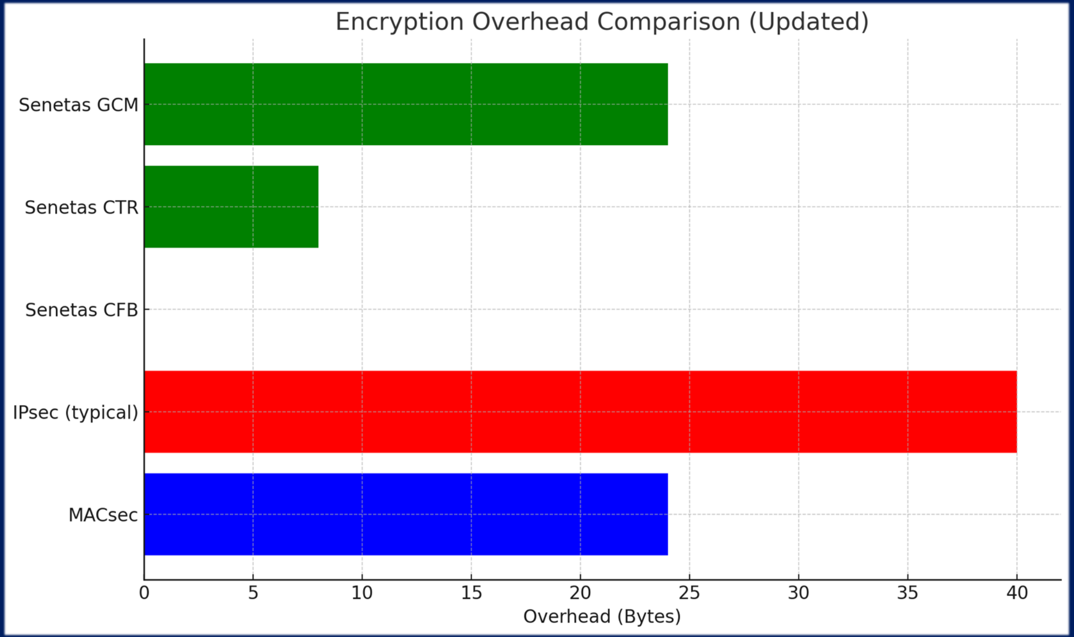
HSE: Sovereign Cryptography

Challenge:

- Customer needed high-speed encryption designed for their own sovereign requirements.

Solution:

- Built in customizations include (all models)
  - BYOC (bring your own curve)
  - BYOE (bring your own entropy)
  - Customizable AES S-boxes.
- CSDK – CV1000/CN7000 platforms
  - Cipher Software Development Kit
  - Senetas Hands off capability.

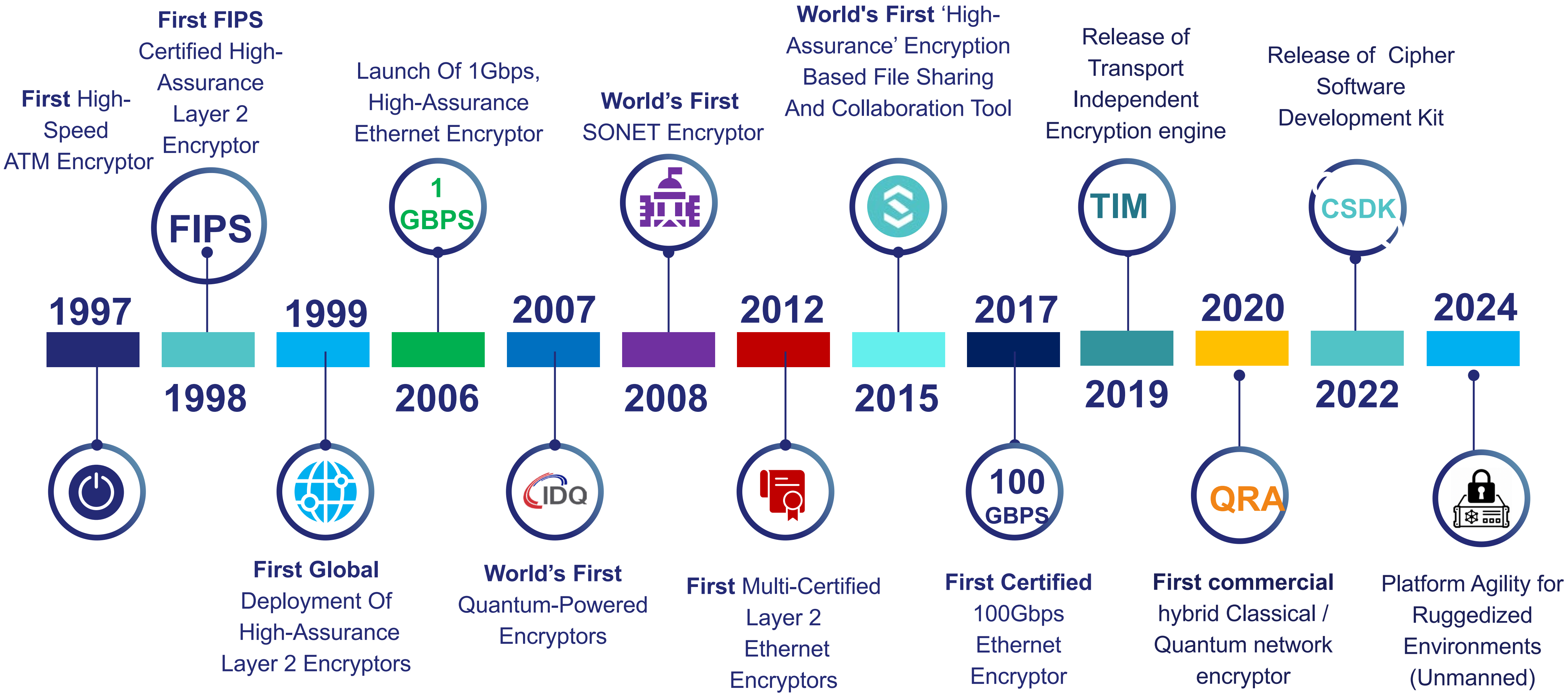


SECTION 4

Innovations, Credentials & Products

CELEBRATING 25

Celebrating 25 Years: Solving real world problems



1997 — **First** High-Speed ATM Encryptor

1998 — **First FIPS** Certified High-Assurance Layer 2 Encryptor

1999 — **First Global** Deployment Of High-Assurance Layer 2 Encryptors

2006 — Launch Of 1Gbps, High-Assurance Ethernet Encryptor

2007 — **World’s First** Quantum-Powered Encryptors

2008 — **World’s First** SONET Encryptor

2012 — **First** Multi-Certified Layer 2 Ethernet Encryptors

2015 — **World's First** ‘High-Assurance’ Encryption Based File Sharing And Collaboration Tool

2017 — **First Certified** 100Gbps Ethernet Encryptor

2019 — Release of Transport Independent Encryption engine

2020 — **First commercial** hybrid Classical / Quantum network encryptor

2022 — Release of Cipher Software Development Kit

2024 — Platform Agility for Ruggedized Environments (Unmanned)

Security tested by leading independent authorities

FIPS

140-2
Level 3
Level 1

CC

EAL 2+
EAL 4+
NDcPP

NATO

Restricted
Green

DoDIN

APL

HSE Product Portfolio

CN4010/CN4020	CN6010	CN6110*	CN9100/9120	CN6140	CN7000	CV1000
Compact desktop enclosure	1U rack mount enclosure	1U rack mount enclosure	1U rack mount enclosure	1U rack mount enclosure	Platform Agile	Virtual Network Function
100/1000Mbps (scalable licensing) 10Mbps – CN4010	100/1000Mbps (scalable licensing)	1/10Gbps (scalable licensing)	100Gbps	4 * 1/10Gbps (scalable licensing)	DPDK with Crypto acceleration (>5Gbps platform dependent)	DPDK with Crypto acceleration (>5Gbps platform dependent

RJ45 (CN4010)
SFP (CN4020)
	RJ45 electrical interfaces
	Pluggable optical SFP
		Pluggable optical SFP+/RJ45	CFP4(CN9100)
			QSFP28(CN9120)
				Pluggable optical SFP+	Min 3, mixed speed supported,
					Platform dependent
						Three para-virtualized interfaces

External plug pack	Dual redundant AC/DC supplies	Dual redundant AC/DC supplies	Dual redundant AC/DC supplies	Dual redundant AC/DC supplies	Platform dependent	VMware, KVM, Hyper-V hypervisor support
LEDs	LCD/Key Pad	LCD/Key Pad	LCD/Key Pad	LCD/Key Pad	Platform dependent	Integrated with SafeNet KeySecure
	User-replaceable fans/battery	User-replaceable fans/battery	User-replaceable fans/battery	User-replaceable fans/battery		
Latency < 10uS	Latency < 8uS	Latency < 6uS	Latency < 2uS	Latency < 6uS		
CC EAL2+ NDcPP, FIPS 140-3 level 3	CC EAL2+ NDcPP, FIPS 140-3 level 3	CC EAL2+, FIPS 140-3 level 3	CC EAL2+ NDcPP, FIPS 140-3 level 3	CC EAL2+ NDcPP, FIPS 140-3 level 3	FIPS 140-3 Level 1 (CE Crypto Module)	FIPS140-3 Level 1 (CE Crypto Module)

All devices are interoperable and can be managed by SMC or CM7 Management Platforms

* Soon to be released

John Weston

CHIEF ARCHITECT

e: john.weston@senetas.com

Nish Kawale

VICE PRESIDENT SALES ENGINEERING, AMERICAS

e: nish.kawale@senetas.com

SENETAS

Thank you

senetas.com