CEP Variable Speed Encryptors
Multi-Layer 3Mbps to 10Gbps Tunnel-less Encryptors

Product Overview
The Certes Enforcement Point (CEP) Variable Speed Encryptors (VSEs) are bandwidth customizable multi-layer encryption appliances that provide tunnel-less data protection, including Ethernet frame encryption for Layer 2 networks, IP packet encryption for Layer 3 networks, and Layer 4 data payload encryption for IP and MPLS networks. The VSEs offer full-duplex encryption at 15 standardized rates ranging from 3Mbps to 10Gbps using the AES 256 algorithm.

The VSEs enable organizations to standardize on a single platform capable of encrypting at various throughputs, based on software licenses. This allows organizations to continue to use the same encryption hardware as their bandwidth needs increase, providing both flexibility and investment protection. The VSEs integrate easily into any existing network, operating transparently to the network infrastructure; ensuring data transmissions are encrypted, without compromising performance.

Scalable and Secure Group Encryption
The VSEs use Certes Networks' web-based management platform, TrustNet Manager, to securely generate and distribute group keys to authorized endpoints. By avoiding the use of IPsec tunnels, group encryption greatly reduces deployment complexity and provides fully meshed encryption that is easy to manage. The solution is also compatible with load balancing, highly available network designs, QoS and network monitoring tools.

Ethernet Frame Encryption
The VSEs are compatible with all Layer 2 unicast, multicast, point-to-point, and multipoint-to-multipoint topologies. They also authenticate all Ethernet frames, preventing man in the middle attacks. Encryption polices can be based on VLAN ID's for cryptographic segmentation of data, or can be set to encrypt all Ethernet frames.

Persistent authentication of frames ensures that the data received at the remote end of a connection originated from a trusted source. While encryption directly protects data, without authentication, data streams remain vulnerable to modification from man in the middle attacks. Unlike many encryption solutions, the VSE's provide continuous authentication to ensure that both the data and the communication streams are uncompromised. Without both, the network and data are less than secure.

IP Packet Encryption
Using the IP Security (IPsec) protocol, the VSEs provide full data encryption for Layer 3 IP networks. The VSE family utilizes the Certes Networks Encapsulating Security Payload protocol (CN-ESP) to encrypt the IP packet, while preserving the original IP header. This unique functionality maintains network transparency, while providing maximum data protection. By preserving the original header and encrypting only the payload, the VSEs can protect data over any IP infrastructure including multi-carrier, load-balanced, and high availability networks.

Payload Only Encryption
In addition to standard IPsec encryption, (which encrypts the Layer 4 header), the VSEs offer a Layer 4 compatible "payload only" encryption option. This unique, patent-pending capability allows network services, such as Netflow/Jflow, and Class of Service (CoS) based traffic shaping, to be maintained through the service provider network while the payload itself is encrypted.

Central Policy Management
The VSEs can be configured and centrally managed via the TrustNet Manager. TrustNet allows both security and network administrators to quickly and easily manage network security from a centralized interface with simple yet powerful drag and drop policy creation capability. Encryption policies can be based on source or destination IP addresses, source or destination port numbers, protocol IDs, or VLAN tags. Policies can be quickly and easily modified in seconds on even the largest networks, without traffic disruptions or interaction with remote personnel. TrustNet Manager also provides logging and audit mechanisms to meet or exceed compliance and audit requirements.

PRODUCT FAMILY
- Encrypted throughput from 3Mbps to 10Gbps
- Layer 2 Ethernet frame, Layer 3 IP packet, and Layer 4 payload protection
- Per-frame/packet authentication
- Microsecond latency
- Preserves VLAN and MPLS tags
- FIPS 140-2 validated

FEATURES AND BENEFITS
- Multiple encrypted throughput options
- Transparent to network and applications
- Seamless scalability
- Infrastructure neutral
- Easy installation and management
- Create secure network groups

COMPREHENSIVE DATA PROTECTION
- IPsec site-to-site networks
- MPLS meshed networks
- Metro Ethernet and VPLS networks
- Voice and video over IP applications

Variable Speed Encryptors (VSEs)
Multi-Layer 3Mbps to 10Gbps Tunnel-less Encryptors

Performance (Encrypted Throughput)
CEP10 VSE
- 3, 6, 10, 25, or 50Mbps
CEP100 VSE
- 25, 50, 75, 100, 155, or 250Mbps
CEP1000 VSE
- 100, 155, 250, 500, 650Mbps and 1Gbps
CEP10G VSE
- 500, 650Mbps and 1, 2.5, 5 and 10Gbps

Security
- Encryption: AES-CBC (256 bit) (FIPS 197), Triple-DES-CBC (168 bit) (NIST 800-67)
- Authentication (Message Integrity): HMAC-SHA-1-96, HMAC-SHA-256-96 (FIPS 180-3, FIPS 198)
- Signature generation and verification: ANSI X9.31, RSASSA-PS, RSASSA-PKCS v1.5, DSA FIPS 186-2
- Management session authentication: RSA, DSS
- Automatic or manually triggered hitless key rotation
- Group keying with TrustNet Manager SSL/TLS (bilateral authentication) based on certificates
- Certificate revocation: OCSP (RFC 2560), CRL (RFC 5280)
- IPSec (RFC 2401) for Layer 3 encryption
- IKE in Layer 2 peer-to-peer mode (RFC s 2407, 2408, 2409)

Network Support
- Ethernet
- VLAN tag preservation
- MPLS tag preservation
- IPv4
- IPv6 (Layer 2 Ethernet encryption mode)
- Secure NTP

Policy Selector Options
- Source or destination IP address
- Source or destination port number
- Protocol ID (L3 and L4 options)
- VLAN ID (L2 option)
- Multicast address

Environmental
- Operating temperature: 0° to 40° C (32° to 104° F)
- EU WEEE
- EU RoHS-5

Regulatory
- Safety: UL 60950-1
- Emissions for CEP10, CEP1000, CEP10G VSEs: FCC part 15 subpart B class A
- Emissions for CEP100 VSE: FCC part 15 subpart B class B

Physical
CEP10 VSE
- 1U tamper evident chassis
- Dimensions: 1.6"H x 8.0"W x 5.8"D
- Rack mountable in standard 19" rack or desktop option
- Power (external adapter): 100-240 V AC, 60 W max output, 50-60 Hz
- Max input current: 1.8 A
- Weight: desktop 2.2 lbs, rack mount 2.6 lbs (including external AC adapter)
- MTBF: 388,999 hours
- FIPS 140-2 Level 2 validated (certificate # 1622)

CEP100 VSE
- 1U tamper evident chassis
- Dimensions: 1.75"H x 17"W x 10"D
- Rack mountable in standard 19" rack or desktop option
- Power: 100-240 V AC , 180 W max output, 50-60 Hz, auto-sensing
- Max input current: 4 A
- Weight: 6 lbs
- MTBF: 59,794 hours
- FIPS 140-2 Level 2 validated (certificate # 1605)

CEP1000 VSE
- 1U tamper evident chassis
- Dimensions 1.75"H x 17"W x 10"D
- Rack mountable in standard 19" rack
- Dual hot-swappable AC power: 100-240 V AC, 200 W max output (per supply), 47-63 Hz, auto-sensing
- Max AC input current: 3 A (per supply)
- Dual hot-swappable DC power: -36 V DC to -72 V DC, 250 W max output (per supply)
- Max DC input current: 11 A @ 36V, 5.5 A @ 72 V (per supply)
- Weight: 9 lbs
- MTBF: 158,520 hours
- FIPS 140-2 Level 2 validated (certificate # 1605) (hardware designed to meet FIPS 140-2 Level 3 Requirements)

CEP10G VSE
- 2U tamper resistant chassis
- Dimensions: 3.5"H x 17"W x 15"D
- Rack mountable in standard 19" rack
- Customer replaceable fan assemblies
- Dual hot-swappable AC power: 100-240 V AC, 350 W max output (per supply), 50-60 Hz auto-sensing
- Maximum AC input current: 8 A (per supply)
- Dual hot-swappable DC power: -36 V DC to -72 V DC, 350 W max output (per supply)
- Maximum DC input current: 15 A (per supply)
- Weight: 22 lbs
- MTBF: 106,376 hours
- FIPS 140-2 Level 2 validation in progress (hardware designed to meet FIPS 140-2 Level 3 Requirements)

Interfaces
CEP10 VSE:
- Data: Two 10/100/1000 RJ45 Ethernet ports
- Management: One 10/100 RJ45 Ethernet and one RS232 serial port

CEP100 VSE:
- Data: Two 10/100/1000 RJ45 Ethernet ports
- Management: One 10/100 RJ45 Ethernet and one RS232 serial port

CEP1000 VSE:
- Data: Two full-duplex Gigabit Ethernet ports with SFP interfaces (single mode, multimode or copper)
- Management: One 10/100 RJ45 Ethernet and one RS232 serial port

CEP10G VSE:
- Data: Two full-duplex 10 Gigabit Ethernet ports with SFP+ interfaces (single mode or multimode)
- Management: One 10/100/1000 Ethernet RJ45, one Gigabit Ethernet (SFP) and one RJ45 serial port