



PocketCryptor

The PocketCryptor is a highly reliable and compact network encryption device, designed for use in LAN, WAN, VLAN and Secure Remote Access applications. Robust performance and extreme small size makes the PocketCryptor to the ideal solution for a large number of security applications:

- Encryption of government and company networks
- Encryption in mobile vehicles (cars, motorcycles, vessels,...)
- Encryption in Self-Service Devices (POS devices, ATM machines, ...)
- Encryption of Wireless Access Points & VLAN
- Encryption of Home Office connections
- Encryption of hotel room connections
- Secure VOIP Telephony

The PocketCryptor encrypts the communication to other PocketCryptor's, MicroCryptor's, PowerCryptor's, GigaCryptor's, IPCrypt Client's as well as CompuSec HSM's. The product is also compatible to the ANIS product family whenever identical encryption algorithms are used. The product can be centrally managed using GlobalAdmin.

Cryptography

The PocketCryptor uses standard AES encryption with 256 bit key length. The substitution boxes of the AES algorithm can be customized to provide proprietary algorithms for government applications. Details are available to our customers on request. PocketCryptor uses a FPGA chip to perform the encryption in Hardware. A two CPU concept is implemented providing a separate CPU to manage the secrets stored in the product.

Performance Overview of the PocketCryptor:

PocketCryptor	MicroCryptor*
Connection: 10/100/1000 MBit Copper Ethernet	Connection: 10/100 MBit Copper Ethernet
> 120 MBit throughput full duplex in Gateway mode. Maximum throughput is provided for full packet length. Refer to the throughput diagram for individual packet length.	93 MBit throughput full duplex in Gateway mode. Maximum throughput is provided for full packet length. Refer to the throughput diagram for individual packet length.
>100 MBit throughput full duplex in Layer-2 mode. Maximum throughput is provided for full packet length. Refer to the throughput diagram for individual packet length.	74 MBit throughput full duplex in Layer-2 mode. Maximum throughput is provided for full packet length. Refer to the throughput diagram for individual packet length.
Example for short packets: VOIP packets with 200 byte total length: 800 telephone talks in parallel	Example for short packets: VOIP packets with 200 byte total length: 500 telephone talks in parallel
Packet propagation delay from last byte received until last byte send out after processing: 1400 byte packet with 100 Mb Interface < 95uS 200 byte packet with 100 Mb Interface < 22uS	Packet propagation delay from last byte received until last byte send out after processing: 1400 byte packet with 100 Mb Interface < 180uS 200 byte packet with 100 Mb Interface < 40uS
Packet Size: Packets have a security header, padding and an additional checksum (option). These additional data need bandwidth on the encrypted channel. Constant additional size: 28 byte (including checksum) Variable additional size for cipher padding: 0-15 byte	Packet Size: Packets have a security header, padding and an additional checksum (option). These additional data need bandwidth on the encrypted channel. Constant additional size: 28 byte (including checksum) Variable additional size for cipher padding: 0-15 byte

**Data are for reference only*

Overview Mode of Operation

PocketCryptors supports **Gateway encryption** and **Layer-2 encryption** and caters for different implementations in the organisation.

Layer-2 encryption	Gateway encryption
Ideal for integration in existing networks without the need for extra subnets	A VPN solution in the organisation Enabling secure remote access for mobile users
AES algorithm using a key length of 256 bit	AES algorithm using a key length of 256 bit
UDP Tunnelling for NAT pass-through and other complex network designs available	UDP Tunnelling for NAT pass-through and other complex network designs
Recommended for use in MPLS networks	255 pools of addresses for WAN applications (each pool allows unlimited number of IP address)
	Hold time of an assignment can be defined
	Provides source and destination address translation in both directions

Enhanced IPSec

The PocketCryptor provides an alternative key management protocol called Enhanced IPSec. With Enhanced IPSec, faster connections are achieved without requiring a lengthy negotiation for a session key to establish a tunnel.

In addition, the session keys used for encryptions can be changed with every 1, 5, 10 or 20 packets. These rapidly changing session keys protect the networks from attacks such as statistical analysis of large amount of encrypted packets. The lifetime of the session keys can be pre-determined using the GlobalAdmin management station.



Packet Authentication

The enhanced IPsec mode allows the PocketCryptor to authenticate every single IP packet. Defective or modified packets will automatically be rejected. This property allows Secure Remote Access applications to automatically identify the connected user. Radius applications are supported, but not longer needed.

High Availability

In a high availability configuration, 2 PocketCryptors are used in redundant hot standby mode. When the active PocketCryptor fails or a cable is broken, the standby PocketCryptor will automatically take over the network traffic and inform the network management about this event.

Management of PocketCryptor

The policies used by PocketCryptors are defined at the GlobalAdmin. Key material used by the product is generated by the hardware security module of the GlobalAdmin or is provided by the customer using an external random source of his trust. Operational data of the products like network statistics are provided to the GlobalAdmin station or are available at a local diagnostic USB port.

Logging and Reporting

PocketCryptors are configured to send SMTP and Syslog messages for logging functions. The status of each PocketCryptors and the packet counts can be viewed from GlobalAdmin. The SMTP and Syslog are configured in GlobalAdmin and then sent to the PocketCryptor using encrypted remote control packets.

Reliability & Physical Dimensions

PocketCryptor is designed to be very small and therefore be used in many mobile applications. The casing hermetically encloses the electronics of the product. No moving parts are used, providing highest reliability for the customer. Very little power consumption is required. The product comes with an external power supply providing 12 Volt DC. The 12V supply can be used in mobile vehicles like Police Motorbikes, boats, satellite communication suitcases or just in hotel rooms. The casing is made of solid metal having only two components.

PocketCryptor Dimensions: 9.5cm (W) x 3.1cm (H) x 7.8cm (L)

Interface Specification

Layer-2 encryption / Gateway encryption		
All Ports are Auto-Sensing and Support Half and Full Duplex Operation		
1st Ethernet Port	Plain Interface	10, 100, 1000 Megabit Auto-Sensing
2nd Ethernet Port	Encrypted Interface	10, 100, 1000 Megabit Auto-Sensing
USB Client	Diagnostic Port	12 Mb full speed
USB Host Adapter	SmartCard Reader or USB Token	1,5 Mb low speed & 12 Mb full speed



CE-Infosys GmbH
Am Kümmerling 45
D-55294 Bodenheim
Germany
Tel.: +49 (0) 6135 / 77 0
Fax: +49 (0) 6135 / 77 77
de.sales@ce-infosys.com

CE-Infosys Pte Ltd
12 Tannery Road
#09-01/02 HB Centre 1
Singapore 347722
Tel.: +65 6899 9392
Fax: +65 6899 9373
sg.sales@ce-infosys.com

CompuSec is a registered trademark of CE-Infosys Pte Ltd in Singapore.

Reseller: