



# PocketCryptor

Der PocketCryptor ist ein äußerst kompaktes Netzwerkverschlüsselungsgerät, konzipiert für den Einsatz in LAN, WAN und Secure Remote Access Bereichen. Zuverlässigkeit, Leistung und die extrem kompakte Bauform machen den PocketCryptor zur idealen Lösung für unterschiedlichste Einsatzgebiete.

- Verschlüsselung von Behörden- und Unternehmens-Netzwerken
- Verschlüsselung in Fahrzeugen (LKW, PKW, Motorrad, Schiff...)
- Verschlüsselung von Selbstbedienungsautomaten (Parkscheinautomaten, Ticketautomaten...)
- Verschlüsselung von WLAN & VLAN
- Verschlüsselung der Verbindung von/zu Heimarbeitsplätzen
- Verschlüsselung der Verbindung von/zu Hotelräumlichkeiten
- Sichere VoIP-Telefonie

Der PocketCryptor kann zusammen mit anderen PocketCryptor'en, MicroCryptor'en, PowerCryptor'en, GigaCryptor'en, IPCrypt Clients und CompuSec HSM's betrieben werden. Das Produkt ist weiterhin kompatibel zur ANIS Produktfamilie, wenn der gleiche Verschlüsselungsalgorithmus verwendet wird. Die zentrale Verwaltung erfolgt über die GlobalAdmin Management Station.

## Kryptographie

Der PocketCryptor nutzt den AES Verschlüsselungsalgorithmus mit 256Bit Schlüssellänge. Die austauschbaren S-Boxen des AES Algorithmus ermöglichen die Verwendung von kundeneigenen / proprietären Algorithmen, z.B. für behördliche Anwendungen. Weitere Details hierzu erhalten Sie auf Anfrage.

Der PocketCryptor nutzt einen FPGA Chip zur Verschlüsselung in Hardware. Ein Konzept mit zwei Prozessoren ist verfügbar, um die im Produkt gespeicherten Informationen sicher zu verwalten.

## Leistungsdaten des PocketCryptor:

PocketCryptor	MicroCryptor*
Anschlüsse: 10/100/1000 MBit Kupfer Ethernet	Anschlüsse: 10/100 MBit Kupfer Ethernet
> 120 MBit full duplex Durchsatzleistung im Gateway Modus	93 MBit full duplex Durchsatzleistung im Gateway Modus.
Maximaler Durchsatz bei größter Paketlänge. Das Leistungsdiagramm zeigt die Durchsatzleistung bei unterschiedlichen Paketgrößen.	Maximaler Durchsatz bei größter Paketlänge. Das Leistungsdiagramm zeigt die Durchsatzleistung bei unterschiedlichen Paketgrößen.
>100 MBit full duplex Durchsatzleistung im Layer-2 Modus	74 MBit full duplex Durchsatzleistung im Layer-2 Modus
Maximaler Durchsatz bei größter Paketlänge. Das Leistungsdiagramm zeigt die Durchsatzleistung bei unterschiedlichen Paketgrößen.	Maximaler Durchsatz bei größter Paketlänge. Das Leistungsdiagramm zeigt die Durchsatzleistung bei unterschiedlichen Paketgrößen.
Beispiel für kleine Pakete: VoIP Pakete mit 200Byte Länge: entspricht 800 Telefongesprächen parallel	Beispiel für kleine Pakete: VoIP Pakete mit 200Byte Länge: entspricht 500 Telefongesprächen parallel
Paket Übertragungsverzögerung vom letzten erhaltenen Byte bis zum letzten gesendeten Byte: 1400Byte Paket mit 100MBit Anschluss < 95uS 200Byte Paket mit 100MBit Anschluss < 22uS	Paket Übertragungsverzögerung vom letzten erhaltenen Byte bis zum letzten gesendeten Byte: 1400Byte Paket mit 100MBit Anschluss < 180uS 200Byte Paket mit 100MBit Anschluss < 40uS
Paketgröße: die Pakete beinhalten einen Security Header, das Datenmaterial und eine zusätzliche Prüfsumme (optional). Diese zusätzlichen Daten benötigen Bandbreite im verschlüsselten Kanal. Konstante zusätzliche Größe: 28Byte (inklusive Prüfsumme) Variable zusätzliche Größe für codiertes Datenmaterial: 0-15Byte	Paketgröße: die Pakete beinhalten einen Security Header, das Datenmaterial und eine zusätzliche Prüfsumme (optional). Diese zusätzlichen Daten benötigen Bandbreite im verschlüsselten Kanal. Konstante zusätzliche Größe: 28Byte (inklusive Prüfsumme) Variable zusätzliche Größe für codiertes Datenmaterial: 0-15Byte

\*Daten dienen nur als Vergleichsreferenz

## Überblick der Betriebsmodi

Der PocketCryptor unterstützt **Gateway Verschlüsselung** oder **Layer-2 Verschlüsselung** und ist somit die Lösung für unterschiedlichste Infrastrukturen einer Organisation.

Layer-2 Verschlüsselung	Gateway Verschlüsselung
Ideal für die Integration in bereits existierende Netzwerke, ohne weitere Subnetze	Als VPN Lösung in der Organisation. Ermöglicht Secure Remote Access (SRA) für mobile Anwender
AES Algorithmus mit einer Schlüssellänge von 256Bit	AES Algorithmus mit einer Schlüssellänge von 256Bit
UDP Tunnel für NAT und weitere Netzwerkstrukturen möglich	UDP Tunnel für NAT und weitere Netzwerkstrukturen möglich
Empfohlen für den Einsatz in MPLS Netzwerken	255 Pool's für Adressen von WAN Anwendungen (jeder Pool mit unbegrenzter Anzahl von IP-Adressen)
	Haltezeit eines Auftrags kann definiert werden
	Bietet Quell- und Ziel-Adressübersetzung in beide Richtungen

## Enhanced IPsec

Der PocketCryptor bietet ein alternatives Schlüsselmanagementprotokoll, genannt Enhanced IPsec. Mit Enhanced IPsec sind schnellere Verbindungen möglich, da keine Sitzungsschlüssel ausgetauscht werden müssen, um einen Tunnel zu erzeugen.

Enhanced IPsec ermöglicht die Änderung, der für die Verschlüsselung verwendeten Paketschlüssel, in unterschiedlichen Abständen. Diese können nach jedem ersten, fünften, zehnten oder zwanzigsten Paket geändert werden, um eventuelle Angriffe per statistischer Analyse der verschlüsselten Pakete zu erschweren. Die Schlüsselwechselintervalle werden über die GlobalAdmin Management Station festgelegt.



## Paketauthentifizierung

Mittels Enhanced IPsec ist es dem PocketCryptor möglich jedes einzelne IP-Paket zu authentifizieren. Somit werden geänderte oder schadhafte Pakete automatisch verworfen. Diese Funktion ermöglicht Secure Remote Access Anwendungen die automatische Identifizierung des verbundenen Benutzers. Radius Anwendungen werden zwar unterstützt, sind aber nicht länger notwendig.

## Höchste Ausfallsicherheit

Zur Gewährleistung höchster Ausfallsicherheit können 2 PocketCryptor'ern in redundantem Hot-Standby Modus betrieben werden. Sollte der aktive PocketCryptor ausfallen oder die Verbindung unterbrochen werden, übernimmt automatisch der passive standby PocketCryptor und versendet gleichzeitig eine Meldung an die GlobalAdmin Management Station.

## Verwaltung des PocketCryptor

Der PocketCryptor wird über GlobalAdmin verwaltet. Die vom PocketCryptor verwendeten Schlüssel werden im Hardware Sicherheitsmodul des GlobalAdmin erzeugt oder von einer kundenseitig ausgewählten vertrauenswürdigen externen Quelle eingelesen. Betriebsdaten der Geräte wie beispielsweise Netzwerkstatistiken werden an die GlobalAdmin Station weitergegeben oder sind über den lokalen USB-Anschluss abrufbar.

## Logs und Berichte

Der PocketCryptor sendet SMTP und Syslog Meldungen als Log-Funktionen. Der Status jedes PocketCryptor und der Paketzähler kann über GlobalAdmin abgerufen werden. SMTP und Syslog werden über GlobalAdmin eingestellt und als verschlüsseltes Remote-Kontrollpaket an den PocketCryptor versendet.

## Design & Abmessungen

Der PocketCryptor wurde bewußt als sehr kleines kompaktes Gerät konzipiert. Ideal für die Verwendung im mobilen Bereich. Das Gehäuse besteht aus 2 Teilen solidem Metall, ist hermetisch abgeschlossen und schützt somit die darin enthaltene Elektronik optimal. Aus Gründen der Ausfallsicherheit werden keine drehenden Teile verwendet. Durch das externe 12 Volt Netzteil ist der Einsatz in Fahrzeugen wie beispielsweise Polizeimotorrädern, Booten, in Kofferlösungen mit Satellitenkommunikationseinheiten oder auch nur in Hotelräumlichkeiten möglich.

PocketCryptor Maße: 9,5cm (B) x 3,1cm (H) x 7,8cm (T)

## Anschlusspezifikation

Layer-2 Verschlüsselung / Gateway Verschlüsselung		
Alle Anschlüsse verfügen über automatische Erkennung und unterstützen sowohl halb- als auch full Duplex Betrieb		
1ster Ethernet Anschluss	Klartext Anschluss	10/100/1000 MBit – automatische Erkennung
2ter Ethernet Anschluss	Verschlüsselter Anschluss	10/100/1000 MBit – automatische Erkennung
USB Client	Diagnose Anschluss	Geschwindigkeit 12MBit
USB Host Adapter	Chipkartenleser oder USB Token	Geschwindigkeit 1,5MBit oder 12MBit



**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 sind registrierte Markenzeichen der CE-Infosys Pte Ltd in Singapur.

Händler: