

ModemEncryptor ME100

Verschlüsseln von Modemverbindungen

- Wird zwischen PC und beliebigem Modem geschaltet
- Generiert automatisch hochwertige Schlüssel für die sichere Datenübertragung
- Integrierter physikalischen Zufallsgenerator ausgezeichneter Qualität
- International anerkannter und leistungsfähiger Verschlüsselungs-Algorithmus
- Sichere Authentisierung durch Challenge-Response-Verfahren
- Einfache Konfiguration über ein beliebiges Terminalprogramm



ME100 ist ein **Zusatzgerät für beliebige Modems** zur Verschlüsselung von Daten bei ihrer Übertragung über ein **Datenübertragungsnetz (Telefon-, GSM-, Funknetz)**.

Es wird **zwischen PC (COM- oder USB-Schnittstelle) und Modem** geschaltet. Durch Konfiguration und Schlüsselverwaltung über ein beliebiges Terminalprogramm ist das Gerät unabhängig von Anwenderplattform und Betriebssystem. Alle zu übertragene Daten werden automatisch verschlüsselt und in der ebenfalls mit einem ME100 ausgerüsteten Gegenstelle entschlüsselt.

Typische Anwendungsfälle

- Schutz von Daten, die über unsichere Netzwerke (Telefonleitungen, drahtlose Übertragungssysteme) übertragen werden sollen (Dateitransfer, Mailboxen, Fernwartung/Ferndiagnose von Datentechnik)
- Telearbeitsplätze
- Flexibler und mobiler Einsatz durch kleine Abmessungen

Leistungs- und Funktionsparameter

Die **Größe** des Gerätes beträgt 100x55x16 mm.

Die **Stromversorgung** erfolgt durch ein externes Steckernetzteil (Lieferumfang) bzw. über den USB-Anschluß.

Das Gerät verschlüsselt und entschlüsselt automatisch die übertragenen Daten im Übertragungsnetz bis zu einer Geschwindigkeit von 115.200 Bit/s halbduplex. Die Verbindung zur COM- oder USB-Schnittstelle verfügt über eine **automatische Baudratenerkennung von 1.200 bis 115.200 Bit/s**. Es kann auch eine feste Baudrate eingestellt werden. Unterstützt wird ein Hardware-Handshake sowie das Standardprotokoll 8 Bit, keine Parität, 1 Stopbit.

Das ME100 beinhaltet ein **vollständiges Kryptierverfahren** und ist ohne spezifische Kenntnisse auf dem Gebiet der Kryptologie **sofort einsetzbar**. Das implementierte Kryptierverfahren (Verschlüsselungs-Algorithmus, Schlüsselmanagement und Sicherheitsfunktionen) organisiert automatisch die garantierte sichere Übertragung der Daten und den Schutz sicherheitsrelevanter Daten im ME100. Die notwendigen Schlüssel für die verschlüsselte Datenübertragung werden automatisch mittels integrierten **physikalischen Zufallsgenerator** in ausgezeichneter Qualität erzeugt. Das Schlüsselmanagement wird vom Gerät selbst verwaltet, so daß vom Anwender kein Handlungsbedarf besteht. Für eine sichere Authentisierung gegenüber der Gegenstelle ist ein Challenge-Response-Verfahren integriert. Bei Bedarf können auch Daten im Klartext übertragen werden, dadurch ist Kompatibilität mit jedem Modem gewährleistet.

Verschlüsselungs-Algorithmus

Um mit minimaler Hardware eine hohe Kommunikationsgeschwindigkeit zu erreichen, ist ein leistungsfähiger und garantiert sicherer Algorithmus mit einer **Stromchiffre (RC4-kompatibel)** ausgewählt worden. Die Schlüssellänge beträgt bei allen verschlüsselten Daten 128 Bit.

Schlüsselmanagement

Verschiedene Schlüssel sichern sowohl die Daten bei ihrer Modem-Übertragung als auch alle sicherheitsrelevanten Informationen im Gerät:

- **Sessionkey (128 Bit)**: verschlüsselt die zu übertragenen Daten und wird per Zufallsgenerator vor jeder Verbindungsaufnahme erzeugt und qualitativ getestet.
- **Masterkey (128 Bit)**: verschlüsselt den Sessionkey bei seiner Übertragung zur Gegenstelle, dieser feste Zufallswert ist nicht auslesbar im Mikrocontroller gespeichert und bei allen Geräten gleich.
- **Userkey 128 Bit**: Der Masterkey kann mit einer vom Anwender einzustellenden Zeichenfolge mathematisch verknüpft werden. Dadurch können nur Geräte mit gleichem Userkey verschlüsselt kommunizieren. Die Zeichenfolge wird verschlüsselt gespeichert und kann nur nach einer **PIN-Eingabe** variiert werden. Die PIN kann geändert werden und ist im Gerät verschlüsselt gespeichert.
- **Devicekey (128 Bit)**: verschlüsselt alle sicherheitsrelevanten Daten im Gerät, unikater Zufallswert für jedes Gerät, wird per Zufallsgenerator bei der Fertigung erzeugt und ist nicht auslese- und manipulierbar im Mikrocontroller gespeichert.

Weitere Eigenschaften

- Sprachauswahl deutsch und englisch
- Kompatibel zu den Verschlüsselungs-Systemen OEM-Modul CM200, GSM-Modem GCM100, ISDN-Modem ICM100 und Analog-Modem ACM100

Bestell-Bezeichnung: ME100-232 (RS-232-Interface)
ME100-USB (USB 1.1-Interface)