

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Modem Encryptor ME100

Handbuch



Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 1 1 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Copyright

Copyright (C) 2002

IBB Ingenieurbüro Bergmann
Karolinenhofweg 18
D-12527 Berlin

Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf in irgendeiner Form (Fotokopie, Druck oder andere Verfahren) ohne ausdrückliche Genehmigung des Herstellers reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Der rechtmäßige Erwerb des Sicherheitssystems ME100 erlaubt eine Nutzung ausschließlich entsprechend Lizenzvertrag.

Ausgabe vom 14.09.2007

Haftung

Bei der Erarbeitung dieser Dokumentation wurde größter Wert auf die Vollständigkeit und Richtigkeit des Inhalts gelegt. Es kann dennoch keine Garantie für die Vollständigkeit und Richtigkeit übernommen werden.

Für Hinweise zu dieser Dokumentation sind wir dankbar.

Hotline

Die Hotline des Herstellers erreichen Sie unter 030 65489970

Informationen

www.ibbergmann.org

Warenzeichen

MS Windows ist eingetragenes Warenzeichen der Microsoft Corp.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 2 2 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

INHALTSVERZEICHNIS

1. EINLEITUNG	5
2. VERWENDUNGSZWECK.....	5
3. FUNKTIONEN UND LEISTUNGEN	6
<i>PRINZIPELLER AUFBAU.....</i>	<i>6</i>
<i>FUNKTIONALITÄT DER LEUCHTDIODEN</i>	<i>7</i>
<i>KRYPTIERVERFAHREN.....</i>	<i>7</i>
<i>Verschlüsselungs-Algorithmus</i>	<i>7</i>
<i>Schlüsselmanagement.....</i>	<i>8</i>
<i>Sicherheitsfunktionen</i>	<i>8</i>
<i>SCHUTZ DER DATEN IM GERÄT.....</i>	<i>9</i>
<i>SICHERHEIT DER ÜBERTRAGENEN DATEN.....</i>	<i>9</i>
4. INSTALLATION	10
5. START	10
6. KONFIGURATION DES ME100.....	11
<i>HAUPTMENÜ.....</i>	<i>12</i>
<i>BAUDRATE</i>	<i>12</i>
<i>REPORTS.....</i>	<i>13</i>
<i>USERKEY UND PIN</i>	<i>14</i>
<i>DIVERSES.....</i>	<i>15</i>
<i>PHYSIKALISCHER ZUFALLSGENERATOR.....</i>	<i>16</i>
<i>SYNCHRONISATION</i>	<i>16</i>
<i>WERKSEINSTELLUNGEN</i>	<i>17</i>
<i>SELBSTTEST.....</i>	<i>17</i>
<i>SPRACHAUSWAHL</i>	<i>18</i>
<i>BEENDEN.....</i>	<i>18</i>
7. DATENÜBERTRAGUNG IM KLARTEXT	18
8. EINSATZHINWEISE.....	19
<i>TERMINALPROGRAMM</i>	<i>19</i>
<i>UNBEMANNTE STATION.....</i>	<i>19</i>
<i>WAS NICHT FUNKTIONIERT.....</i>	<i>20</i>
<i>Internet</i>	<i>20</i>

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 3 3 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

<i>Vernetzte Übertragungen</i>	20
<i>Fax</i>	20
9. FEHLERMELDUNGEN	20
10. TECHNISCHE DATEN	21

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 4 4 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

1. Einleitung

Mit den Möglichkeiten zur Übertragung von Daten und dem Zugriff auf Informationen sind auch Risiken verbunden. Oftmals sind Daten vertraulich oder personenbezogen und tragen somit einen sensitiven Charakter. Diese Daten sind nicht nur bei ihrer Speicherung vor nicht autorisierten Zugriffen zu schützen, sondern auch bei ihrer Übertragung zwischen Rechnern und Netzwerken. Eine verbreitete Art der Übertragung von Informationen ist die Nutzung von seriellen Verbindungen. Die Daten werden dabei im Allgemeinen über Modems und öffentliche Telefonnetze übertragen. Da diese Übertragungswege für Unbefugte zugänglich sind, bestehen Bedrohungen für die Vertraulichkeit und die Integrität der Daten. Ohne daß dies durch den Sender oder den Empfänger bemerkt wird, können Daten z.B.

- abgehört (Vertraulichkeit),
- manipuliert (Integrität) oder
- zurückgehalten (Verfügbarkeit) werden.

Es ist erforderlich, sensitive Daten auf geeignete Weise vor diesen Bedrohungen zu schützen. Die beste Möglichkeit ist dabei die Nutzung von kryptographischen Methoden. Bei einer Verschlüsselung werden Daten in eine solche Form gebracht, aus der keinerlei Rückschlüsse auf ihren Inhalt gezogen werden können. Geeignete Mechanismen verhindern außerdem eine unbemerkte Manipulation an den übertragenen Informationen.

2. Verwendungszweck

In der modernen Industrie werden zunehmend Systeme mit Fernwartung/Ferndiagnose ausgerüstet. Damit sind auch über große Entfernungen Funktionalität, Service und Kundennähe gewährleistet. Jedoch werden dabei auch sensible Informationen wie Passwörter, Meßdaten, Parameter und firmeneigenes know-how übertragen. Der Schaden durch Spionage und Manipulation werden jährlich bundesweit auf über 10 Mrd. Euro geschätzt (2001).

Deshalb ist Verschlüsselung in modernen Kommunikationssystemen unerlässlich. Die Verschlüsselung aller übertragenen Daten garantiert die Vertraulichkeit, so daß Unberechtigte keine sinnvollen Informationen erlangen können. Der nachfolgend beschriebene Modem-Encryptor

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 5 5 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

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 Punkt-zu-Punkt-Übertragung der Daten und den Schutz sicherheitsrelevanter Daten im Gerät. Die notwendigen Schlüssel für die verschlüsselte Übertragung werden automatisch mittels integrierten physikalischen Zufallsgenerators in höchster statistischer Qualität erzeugt. Das Schlüsselmanagement wird vom ME100 verwaltet, so daß vom Anwender kein Handlungsbedarf besteht.

3. Funktionen und Leistungen

Prinzipieller Aufbau

Das Gerät besteht aus zwei Modulen

- RS232C-Schnittstellen für Übertragungsraten bis 115.200 Bit/s
- Verschlüsselungs-Modul für eine garantiert sichere Datenübertragung

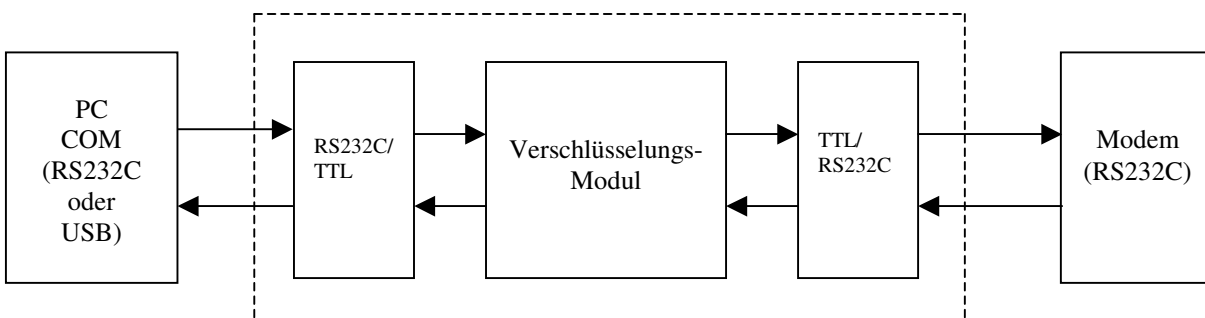


Abbildung 1: Blockschaltbild des Gerätes ME100

Das Verschlüsselungs-Modul ist jederzeit in der Lage, Daten und Handshake-Signale zu steuern. Wird ein Fehler im Gerät oder bei einer Verbindungsaufnahme mit einer Gegenstelle festgestellt, bestimmt das Verschlüsselungs-Modul die notwendigen Handlungen. Leuchtdioden an der Geräte-Oberseite reflektieren Funktionalität und Zustand des Moduls.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 6 6 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Vorraussetzung für den automatischen Aufbau einer verschlüsselten Verbindung ist die Generierung des Modemsignals DCD (Data Carrier Detect). In den Modemeinstellungen ist der unbedingt notwendige relevante AT-Befehl „at&c1“ meist eine Standard-Einstellung. Überprüfen Sie vor der ersten Verbindungsaufnahme diese Modemeinstellung.

Funktionalität der Leuchtdioden

An der Geräteoberseite zeigen Leuchtdioden Funktionalitäten des Gerätes an. Die Abkürzungen stehen für folgende Bedeutung:

- RX: Empfangene Daten von der Übertragungsseite (Modem)
- TX: Gesendete Daten von der PC-Seite
- CD: Data Carrier Detect, Modem hat eine Verbindung mit der Gegenstelle hergestellt
- OK: das Gerät arbeitet fehlerfrei
- CRYPT: alle übertragenen Daten werden verschlüsselt

Blinken die Leuchtdioden „OK“ und „CRYPT“, liegt ein interner Fehler vor. Aktivieren Sie ein Terminalprogramm, um den Fehler anzuzeigen.

Kryptierverfahren

Ein Kryptierverfahren setzt sich im Wesentlichen aus den Komponenten Verschlüsselungs-Algorithmus, Schlüsselmanagement und Sicherheitsfunktionen zusammen:

Verschlüsselungs-Algorithmus

Um mit minimaler Hardware eine hohe Kommunikationsgeschwindigkeit zu erreichen, ist ein leistungsfähiger und garantiert sicherer, symmetrischer Algorithmus mit einer Stromchiffre ausgewählt worden. Es wurde ein RC4-kompatibler Algorithmus mit einer Schlüssellänge von 128 Bit implementiert. Algorithmus und Schlüssellänge setzten der modernen Kryptoanalyse einen unüberwindbaren Widerstand entgegen.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 7 7 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Schlüsselmanagement

Die Funktionalität des Gerätes wird mit folgenden verschiedenen Schlüsseln gewährleistet:

- *Devicekey* (128 Bit): dieser Schlüssel ist für jedes Gerät unikat und nicht ausles- und manipulierbar im eingesetzten Mikrocontroller gespeichert. Er dient der Verschlüsselung aller sicherheitsrelevanten Daten im ME100 und wird mittels physikalischen Zufallsgenerators höchster statistischer Qualität in der Fertigung für jedes Gerät neu generiert und ist dann ausschließlich in diesem vorhanden.
- *Sessionkey* (128 Bit): mit diesem Schlüssel werden alle zu übertragenen Daten verschlüsselt. Er wird vor jeder Verbindungsaufnahme vom integrierten physikalischen Zufallsgenerator erzeugt und vor der Verwendung qualitativ (statistische Gleichverteilung der 0/1-Bits) bewertet.
- *Masterkey* (128 Bit): mit diesem Schlüssel wird der Sessionkey verschlüsselt zur Gegenstelle übertragen. Der Masterkey wird in der Fertigung, für alle Geräte gleich, aus Zufallszahlen erzeugt und nicht ausles- und manipulierbar im eingesetzten Microcontroller gespeichert.
- *Userkey* (128 Bit): der Anwender kann den Masterkey durch mathematische Verknüpfung mit eigenen Zeichenfolgen variieren. Der Userkey ist mit dem Devicekey verschlüsselt im Gerät gespeichert. Nur Geräte mit gleichem Userkey können miteinander verschlüsselt kommunizieren.
- *Initialvektor* (128 Bit): dient dem Aufbau von unikat verschlüsselten Verbindungen und der unikat Speicherung von Daten im Gerät. Die benötigten 128 Bit werden vom physikalischen Zufallsgenerator generiert. Vor jeder neuen Verschlüsselung wird ein neuer Initialvektor generiert und mit dem jeweiligen Schlüssel mathematisch verknüpft.

Sicherheitsfunktionen

Das Verschlüsselungs-Modul des ME100 garantiert folgende Sicherheitsfunktionen:

- Kontrolle der qualitätsgerechten Funktion des physikalischen Zufallsgenerators, d.h. die statistische Verteilung der erzeugten Bits wird kontrolliert.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 8 8 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

- Kontrolle der Integrität der verschlüsselt gespeicherten Daten mittels verschlüsselter Prüfsummen. Nach jeder Änderung der auf dem Modul gespeicherten Daten wird ein neuer Initialvektor für die erneute Verschlüsselung dieser Daten generiert.
- Blockierung der Datenübertragung und erzwungener Verbindungsabbruch bei fehlerhafter Authentisierung und bei Fehler des physikalischen Zufallsgenerators.
- Ausgabe und Änderungen des Userkeys sind nur über eine PIN-Eingabe möglich. Die 4-stellige PIN ist durch alle ASCII-Zeichen (89 verschiedene) charakterisiert, somit ergeben sich 62,7 Millionen Varianten. Die Bestätigung einer PIN-Eingabe erfolgt verzögert nach 1 Sekunde, so daß ein Durchprobieren aller Möglichkeiten etwa 2 Jahre benötigt.

Schutz der Daten im Gerät

Alle benötigten Schlüssel sind auslese- und manipulationsgeschützt im Mikrocontroller und die Konfigurationsdaten und der Userkey mit Prüfsumme auf einem Speicherchip verschlüsselt gespeichert. Bei der Programmierung jedes Mikrocontrollers (in der Produktion) wird mittels physikalischen Zufallszahlengenerators ein zufälliger Devicekey erzeugt, geprüft (statistische Qualität des Zufalls) und nach der Programmierung jedes Mikrocontrollers vernichtet. Die kundenspezifischen Daten und Parameter auf dem Speicherchip sind also nur mit diesem Mikrocontroller wieder entschlüsselbar.

Sicherheit der übertragenen Daten

Der international bekannte und sichere Verschlüsselungs-Algorithmus RC4 mit einer Schlüssellänge von 128 Bit garantiert die Integrität Ihrer Daten. Die totale Probiermethode (brute force) aller Schlüsselmöglichkeiten (10^{38}) ist völlig sinnlos: Selbst wenn 200 Millionen Computer der Welt parallel 1 Millionen Schlüssel pro Sekunde testen, würde es immer noch eine Millionen mal länger als das Alter des Universums dauern, bis der Schlüssel gefunden wäre. Durch die Schlüsselerzeugung mit einem physikalischen Zufallsgenerator werden menschliche Schwächen bei Schlüsseleingaben vermieden und die Varianz des Schlüssels voll ausgeschöpft.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 9 9 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

4. Installation

Das ME100 wird mit Verbindungskabel und Steckernetzteil geliefert. Der Stecker des Netzteils wird in die vorgesehene Buchse und das Netzteil in eine Netzsteckdose gesteckt. Bei der USB-Version erfolgt die Stromversorgung über den USB-Port. Werden Sie bei der Erstinstallation zur Eingabe der Treiber aufgefordert, so benutzen Sie diese von der mitgelieferten CDROM. Das ME100 wird zwischen dem Datenendgerät (z.B. ein PC) und einem Modem geschaltet.

Nach Zuschalten der Stromversorgung wird im Gerät ein Selbsttest durchgeführt. Ist der Selbsttest beendet, werden je nach Ergebnis zwei Leuchtdioden aktiviert. Leuchten die grünen Leuchtdioden „OK“ und „CRYPT“, ist das Gerät einsatzbereit. Blinken beide Leuchtdioden, liegt ein Fehler vor. Dann lesen Sie bitte im Abschnitt „Fehlermeldungen“ nach.

5. Start

Nach Öffnen eines beliebigen Terminalprogramms kann sofort eine Modemverbindung durch entsprechende AT-Befehle aufgebaut werden. Das Gerät ist auch im gelieferten Werkszustand sofort einsatzbereit. Es können jedoch auch anwenderspezifische Einstellungen konfiguriert werden.

Bei den möglichen Einstellungen des Terminalprogramms ist vor allem das Standardprotokoll 8 Bit, keine Parität, 1 Stopbit (oder 2) unbedingt beizubehalten. Beim Protokoll ist zwischen „kein“ oder „Hardware“ einzustellen. Keinesfalls ist bei verschlüsselten Übertragungen das XON/XOFF-Protokoll zu aktivieren. Ist kein Modem angeschlossen, muss das Protokoll auf „kein“ gestellt sein.

Wichtig! Voraussetzung für den automatischen Aufbau einer verschlüsselten Verbindung ist die Generierung des Modemsignals DCD (Data Carrier Detect). In den Modemeinstellungen ist der unbedingt notwendige relevante AT-Befehl „at&c1“ meist eine Standard-Einstellung. Überprüfen Sie vor der ersten Verbindungsaufnahme diese Modemeinstellung.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 10 10 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

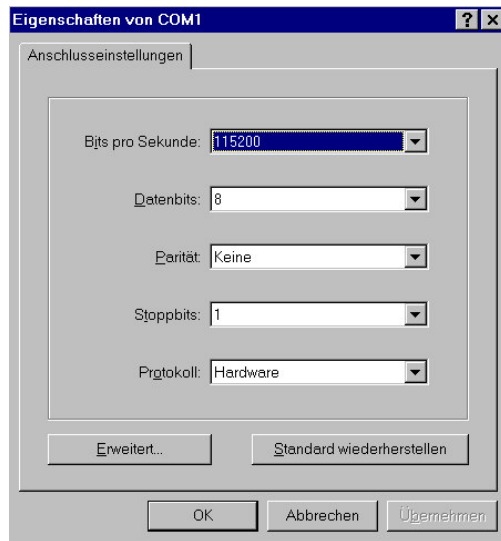


Abbildung 2: Beispiel mit Hyperterminal unter WINDOW `98

6. Konfiguration des ME100

Es werden die auf der Geräteoberseite abgebildeten Zeichen eingegeben: at#cm. Der Zugriff auf das Modem ist während der Konfiguration nicht möglich.

Das ME100 meldet sich mit der Geräte-Variante und dem Ergebnis eines Selbsttest

```
#####
#      ModemEncryptor ME100      #
#      RS-232C ENCRYPTOR         #
#      Version 1.0              #
#####

Selbsttest und Einstellungen

Gespeicherte Parameter : in Ordnung
Eingestellte Baudrate  : automatisch
Test Zufallsgenerator  : in Ordnung
Reports erzeugen       : ja
Synchronisation        : keine

Bitte Taste druecken..
```

Abbildung 3: Eröffnung der Konfiguration des ME100

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 11 11 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Hauptmenü

Nach Drücken einer beliebigen Taste öffnet sich das Hauptmenü. Durch Eingabe der in Klammern gesetzten Ziffer wird das gewünschte Untermenü aktiviert. Mit der Taste „ESC“ wird das Hauptmenü verlassen und die Modemfunktionen wieder aktiviert. In jedem Fall sollte die ordnungsgemäße Funktion mit dem Befehl at (Enter) geprüft werden. Ein angeschlossenes Modem quittiert mit „OK“.

Hauptmenue	
Baudrate	(1)
Reports	(2)
Userkey	(3)
Test Zufallsgenerator	(4)
Synchronisation	(5)
Werkseinstellungen	(6)
Selbsttest	(7)
Sprachauswahl	(8)
Konfiguration beenden	(ESC)
Ihre Auswahl:	

Abbildung 4: Eröffnung der Konfiguration des ME100

Baudrate

Über die Taste „1“ des Hauptmenüs wird in das Untermenü zur Einstellung der Baudrate gewechselt. Die gewünschte Baudrate wird durch Eingabe der Ziffer ausgewählt und im Gerät gespeichert. Die neue Baudrate wird erst nach Verlassen der Konfiguration aktiviert, während im Selbsttest bereits die neue gespeicherte Baudrate angezeigt wird. Das Menü kann mit der Taste „ESC“ ohne Änderung des Parameters verlassen werden. **Hinweis:** Ist eine automatische Baudrate eingestellt, muss nach dem Einschalten des Gerätes mindestens ein AT-Befehl zu Modem gesendet werden, um die Baudrate zu ermitteln. Bei einer festen Baudrate ist das nicht notwendig.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 12 12 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

----- Baudrate -----	
115.200 bps	(1)
57.600 bps	(2)
38.400 bps	(3)
19.200 bps	(4)
9.600 bps	(5)
4.800 bps	(6)
2.400 bps	(7)
1.200 bps	(8)
Automatisch	(9)
Hauptmenue	(ESC)
Ihre Auswahl:	

Abbildung 5: Auswahl der möglichen Baudraten

Reports

Bei der Verbindungsaufnahme kann nach einer Modem-Information zu Geschwindigkeit, Komprimierung und Protokoll noch eine zusätzliche Meldung des ME100 generiert werden. Bei der Einbindung des Gerätes in spezielle Applikation können zusätzliche Meldungen stören. Deshalb ist diese Funktion abschaltbar.

----- Reports -----	
Reports erzeugen	(1)
Keine Reports	(2)
Hauptmenue	(ESC)
Ihre Auswahl:	

Abbildung 6: Auswahl im Menü Reports

Folgende Meldungen können bei aktiviertem Report vom Verschlüsselungs-Modul angezeigt werden:

- „Offene Kommunikation!“
- „Kommunikation verschlüsselt“

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 13 13 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

- „Kommunikation beendet“
- „Fehler Verbindungsaufnahme“
- „Fehler Zufallsgenerator“
- „Abbruch durch falschen Parameter“
- „Keine Daten von Gegenstelle“

Userkey und PIN

Änderungen im Menü Userkey und PIN sind sicherheitsrelevant und nur durch Eingabe der aktuellen PIN erreichbar. Die Rückantwort nach der vierstelligen PIN-Eingabe (ohne Enter) ist verzögert, um ein Ausprobieren zu erschweren. Nach Eingabe der richtigen PIN eröffnet sich das gewünschte Menü:

```

Bitte Ihre PIN eingeben:
****

-----
                Userkey und PIN
-----
Userkey anzeigen           (1)
Userkey aendern           (2)
Userkey default           (3)
Neue PIN                   (4)
Diverses                   (5)
Hauptmenue                 (ESC)
Ihre Auswahl:              _

```

Abbildung 7: Menü Userkey und PIN

Die Werkseinstellung für Userkey und PIN sind „0“ (ASCII-Zeichen). Die Möglichkeiten im Menü sind plausibel dargestellt. Vor jeder Parameter-Änderung erfolgt eine Sicherheitsabfrage. Die Eingaben von Userkey und neuer PIN sollten unter der Beachtung der notwendigen Geheimhaltung erfolgen. Alle eingegebenen Zeichen werden nicht im PC gespeichert.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 14 14 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Diverses

Zum Verifizieren entscheidender Parameter des Verschlüsselungsverfahrens können Beispiele für die Generierung des Sessionkeys und die Implementierung des Algorithmus erzeugt werden. Die generierten Daten sind Unikate des physikalischen Zufallsgenerators. Damit ist gesichert, daß diese Daten nicht noch einmal benutzt werden. Weiterhin besteht die Möglichkeit, für statistische Untersuchungen beliebig lange Zufallsfolgen zu generieren. Die Ausgabe der vom physikalischen Zufallszahlengenerator erzeugten Daten kann nur mit der Taste „ESC“ abgebrochen werden. Das Menü „Firmware-Update“ ist ausschließlich dem Hersteller vorbehalten.

DIVERSES	
Sessionkey generieren	(1)
Testfolgen generieren	(2)
Kontinuierlicher Zufall	(3)
Firmware-Update	(4)
Userkey und PIN	(ESC)
Ihre Auswahl:	

Abbildung 8: Menü Diverses

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 15 15 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Physikalischer Zufallsgenerator

Die präzise und qualitätsgerechte Funktion des physikalischen Zufallsgenerators kann im Menüpunkt 4 des Hauptmenüs getestet werden. Es werden 10.000 Bits erzeugt und die statistische Verteilung mit der Bewertung eines Halbbyte-Tests (die Anzahl der zufällig erzeugten Halbbytes aus vier aufeinanderfolgenden Zufallsbits werden gezählt) geprüft. Der im Ergebnis gezeigte Wertebereich stellt hohe Anforderungen für einen physikalischen Zufallsgenerator dar. Statistisch können 5% aller erzeugten Tests aus einer positiven Bewertung herausfallen, ohne das ein Fehler des Zufallsgenerators vorliegt.

```
Zufallsgenerator arbeitet...
4994 1-Bit von 10000 Bits

Ergebnis des Halb-Byte Tests
Wertebereich 116...156...196
00: 145
01: 170
02: 158
03: 182
04: 166
05: 153
06: 164
07: 160
08: 131
09: 146
0A: 156
0B: 148
0C: 172
0D: 150
0E: 147
0F: 152
Zufallsgenerator ok
Bitte Taste druecken..
```

Abbildung 9: Test des physikalischen Zufallsgenerators

Synchronisation

Für die automatische Neusynchronisation sind keine Parametereingaben notwendig:

```
-----
                Synchronisation
-----
Keine Synchronisation (1)
Synchronisation aktiv (2)
Hauptmenue (ESC)
Ihre Auswahl:      -
```

Abbildung 10: Menü der automatischen Neusynchronisation

Eine automatische Synchronisation ist nur bei langsamen und fehlerhaften Datenübertagungen empfehlenswert.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 16 16 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Werkseinstellungen

Soll ein Gerät in den Auslieferungszustand gesetzt werden, wird diese Funktion aktiviert. Unter Umständen kann bei einer vergessenen PIN nur diese Funktion eine weitere Anwendung des ME100 ermöglichen. Folgende default-Werte werden programmiert:

- PIN: „0000“ (4 ASCII-Zeichen)
- Userkey: „0000000000000000“ (16 ASCII-Zeichen)
- Baudrate: automatisch
- Reports: ja
- Synchronisation: keine
- Dialogsprache: deutsch

Vor dem Setzen der Werkseinstellungen erfolgt eine Sicherheitsabfrage.

Selbsttest

Mit dieser Funktion werden aktuellen Einstellungen abgefragt und ein Zufallsgeneratortest durchgeführt. PIN und Userkey werden nicht angezeigt.

```

Selbsttest und Einstellungen

Gespeicherte Parameter : in Ordnung
Eingestellte Baudrate  : automatisch
Test Zufallsgenerator  : in Ordnung
Reports erzeugen       : ja
Synchronisation        : keine

```

Abbildung 11: Anzeigen nach Selbsttest

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 17 17 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Sprachauswahl

Es stehen die Deutsche und Englische Dialogsprachen zur Auswahl. Nach der Auswahl wird die gewünschte Sprache sofort aktiviert und bis zur erneuten Änderung angewendet.

Sprachauswahl	
Deutsch	(1)
Englisch	(2)
Hauptmenue	(ESC)
Ihre Auswahl:	

Abbildung 12: Menü der Sprachauswahl

Beenden

Mit der Taste „ESC“ kann das Hauptmenü verlassen werden. Um eine ordnungsgemäße Funktion des Gerätes zu gewährleisten, ist der AT-Befehl „at“ (Enter) zu geben. Es wird mit „OK“ quittiert.

7. Datenübertragung im Klartext

Nach dem Einschalten des Gerätes und nach Beendigung einer Verbindung wird immer automatisch in den verschlüsselten Modus geschaltet (Leuchtdiode „CRYPT“ ein). Temporär, also für die nächste Verbindungsaufnahme, kann in den Klartext-Modus geschaltet werden. Der AT-Befehl ist at#co (Enter). Optisch zeigt die ausgeschaltete Leuchtdiode „CRYPT“ die Umschaltung an. Eine Zurückschaltung ist mit dem AT-Befehl „at#cc“ möglich.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 18 18 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

8. Einsatzhinweise

Terminalprogramm

Eine typische Applikation der Kommunikation mit Modems ist mit einem Terminalprogramm gewährleistet. Initialisierung und Wählparameter können in einfacher Art getätigt werden. Für eine Protokollierung der gesendeten und empfangenen Daten ist die Mittschnittsfunktion geeignet:

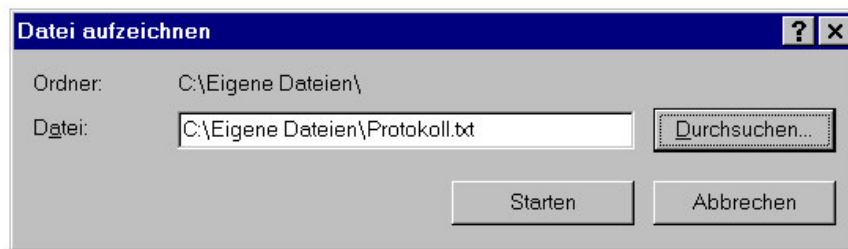


Abbildung 13: Protokollierung unter Hyperterminal

Unbemannte Station

In Remote-Applikationen (Fernwartung/Ferndiagnose) ist das Modem der unbemannten Station nach den spezifischen Bedingungen zu programmieren. Folgendes Beispiel zeigt die Reihenfolge einer möglichen Programmierung:

- `ats0=1` automatische Rufannahme nach der Meldung: ankommender Ruf (Ring)
- `atq1` keine Statusmeldungen ausgeben, („Kein Report“ im ME100 aktivieren!)
- `ate0` kein lokales Echo
- `at&w0` als Profil 0 abspeichern, wird nach jedem Einschalten geladen

Sinnvoll ist es, eine feste Baudrate im Menü Konfiguration des ME100 einzustellen, da bei automatischer Baudratenerkennung immer mindestens ein AT-Befehl zur Ermittlung der Übertragungsgeschwindigkeit von der PC-Seite erforderlich ist.

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 19 19 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Was nicht funktioniert

Internet

Das ME100 ist für verschlüsselte Punkt-zu-Punkt-Übertragungen entwickelt, d.h. alle Daten werden verschlüsselt übertragen. Dadurch ist eine Internet-Anbindung nicht möglich. Die notwendigen IP-Adressen sind nicht mehr im Klartext verfügbar.

Vernetzte Übertragungen

Es gilt das gleiche Prinzip wie beim Internet. Auch diese Applikation ist nicht möglich, da die notwendigen Adressen nicht im Klartext übertragen werden.

Fax

Die Kommunikation im FAX-Modus erfolgt im Allgemeinen im XOFF/XON-Protokoll. Dieses Protokoll wird vom Gerät nicht unterstützt. Alternativ kann natürlich die zu übertragene Datei verschlüsselt mit z.B. Z-Modem-Protokoll zur Gegenstelle versendet werden

9. Fehlermeldungen

Das Gerät verfügt über umfangreiche interne Tests und sichert die Funktionssicherheit während einer Verbindungsaufnahme. Mögliche Fehlzustände mit unterschiedlichen Ursachen werden folgendermaßen gemeldet:

- **Leuchtdioden** „CRYPT“ und „OK“ blinken
Handlung des Anwenders: Konfiguration aufrufen und Fehlermeldung ermitteln
Mögliche Fehlerursachen: Fehler im Power-on-Test, Speicherfehler, Fehler Zufallsgenerator
- **Meldungen während der Konfiguration**
Diese Meldungen sind selbsterklärend.
- **Meldungen im Terminalprogramm** bei Verbindungsaufnahme
Diese Meldungen werden nur angezeigt, wenn die Funktion „Report erzeugen“ aktiviert ist.
„Fehler Verbindungsaufnahme“

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 20 20 von 21

Modem Encryptor ME100	Handbuch	IBB Ingenieurbüro Bergmann

Die Synchronisation zwischen zwei Geräten auf logischer Ebene ist fehlerhaft. Dieser Fehler weist auf eine mögliche Manipulation oder Störungen auf der Telefon-Netzleitung hin.

„Fehler Zufallsgenerator“

Vor jeder verschlüsselten Verbindungsaufnahme werden jeweils ein neuer Sessionkey und Initialvektor durch den physikalischen Zufallsgenerator erzeugt. Werden dabei die statistischen Grenzen überschritten, wird diese Fehlermeldung gegeben. Anschließend sind weitere Tests im Konfigurationsmenü durchzuführen. Sind mehr als 5% aller Tests negativ, ist das Gerät an den Hersteller zurück zu senden.

„Abbruch durch falschen Parameter“

Die Einstellung des Userkey muß auf beiden Seiten identisch sein. Ist das nicht der Fall, wird die Verbindung mit dieser Meldung abgebrochen.

„Keine Daten von Gegenstelle“

Sind nach einer Wartezeit von ca. 5 Sekunden noch keine Daten der Gegenstelle empfangen worden, wird die Verbindung mit dieser Meldung unterbrochen.

10. Technische Daten

- Abmessungen: 100 x 55 x 16 (mm)
- Stromversorgung: Steckernetzteil 6V/0,5A, stabilisiert oder aus dem USB-Port (ca. 70mA)
- Schnittstellen: Eingang: RS-232C oder USB1.1 (Datenendgerät),
Ausgang: RS-232C (Modem)
- Kompatibel mit: OEM-Verschlüsselungs-Modul CM200,
Analog-Verschlüsselungs-Modem ACM100
ISDN-Verschlüsselungs-Modem ICM100
GSM-Verschlüsselungs-Modem GCM100

Datum: 14.09.07		www.ibbergmann.org
Dateiname: Handbuch ME100	Version: 1.2	Seite: 21 21 von 21