IBB Ingenieur-Büro Bergmann, Sonnenweg 3, 15537 Grünheide, info@ibbergmann.org

Software für PRG-Applikationen
Version 2.5

Autor: **Frank Bergmann**
Letzte Änderung: **05.02.2017 10:13**

1 Inhaltsverzeichnis

2 Allgemeines

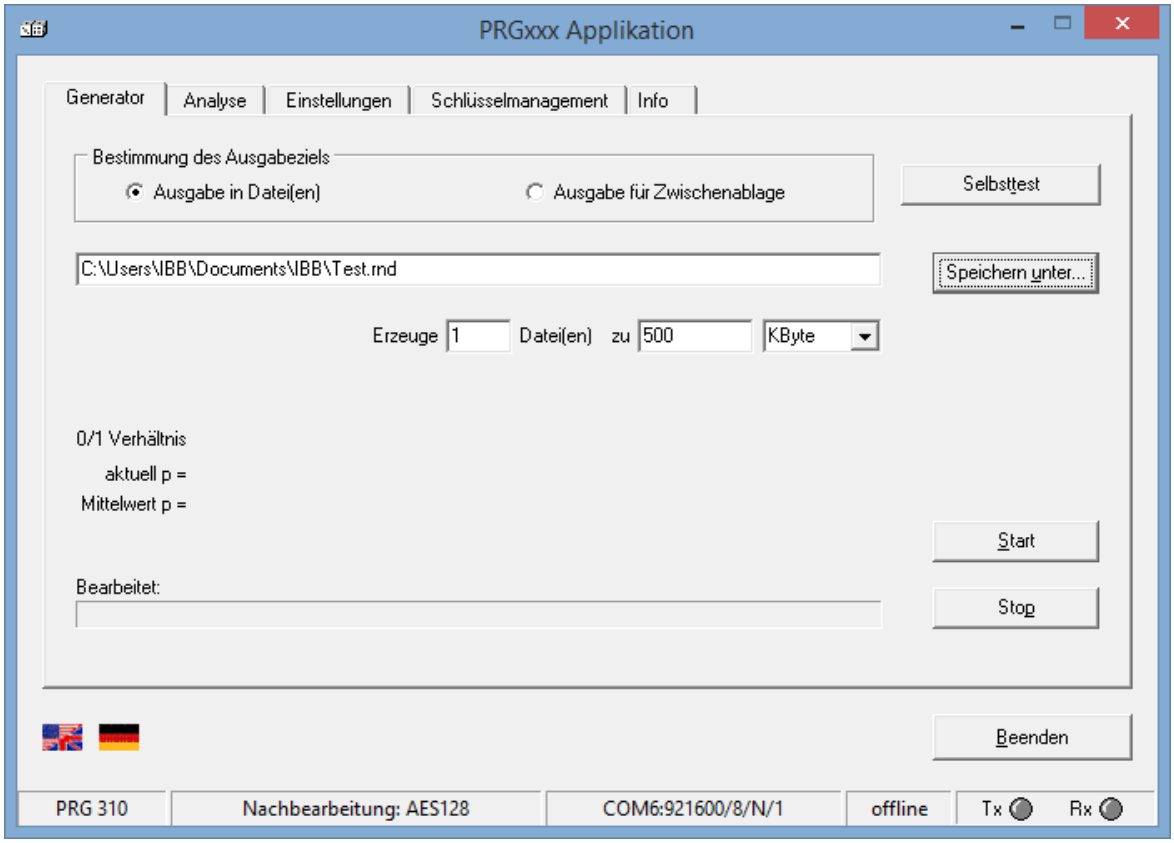
Diese Software dient der Erfassung und grafischen Auswertung von Zufallszahlen mittels verschiedener Applikationen von Zufallsgeneratoren des IBB. Die statistische Bewertung von Zufallszahlen ist mit den bekannten internationalen Analyseprogrammen (NIST-Test-Suite, Diehard-Test, AIS31-Test, usw.) meist nur mit entsprechenden Fachkenntnissen möglich. Die PRG100-Software visualisiert verschiedene Arten der statistischen Verteilung von Zufallszahlen in einfachen, aussagekräftigen Darstellungen.

Weiterhin sind Vorgehensweisen zu einem Schlüssel- und PIN-Management implementiert, dass vollkommen unabhängig von der Zufallsgenerierung genutzt werden kann.

Steuerung und Informationen dieser WINDOWS-Software sind für die deutsche und englische Sprache einstellbar.

3 Installation und Programmaufruf

Die Installation wird durch Aufruf der Datei „PRG100Setup.exe" durchgeführt. Das Programm wird nach der erfolgreichen Installation mit der Datei „PRG100.exe" gestartet und zeigt sich mit folgendem Menü:

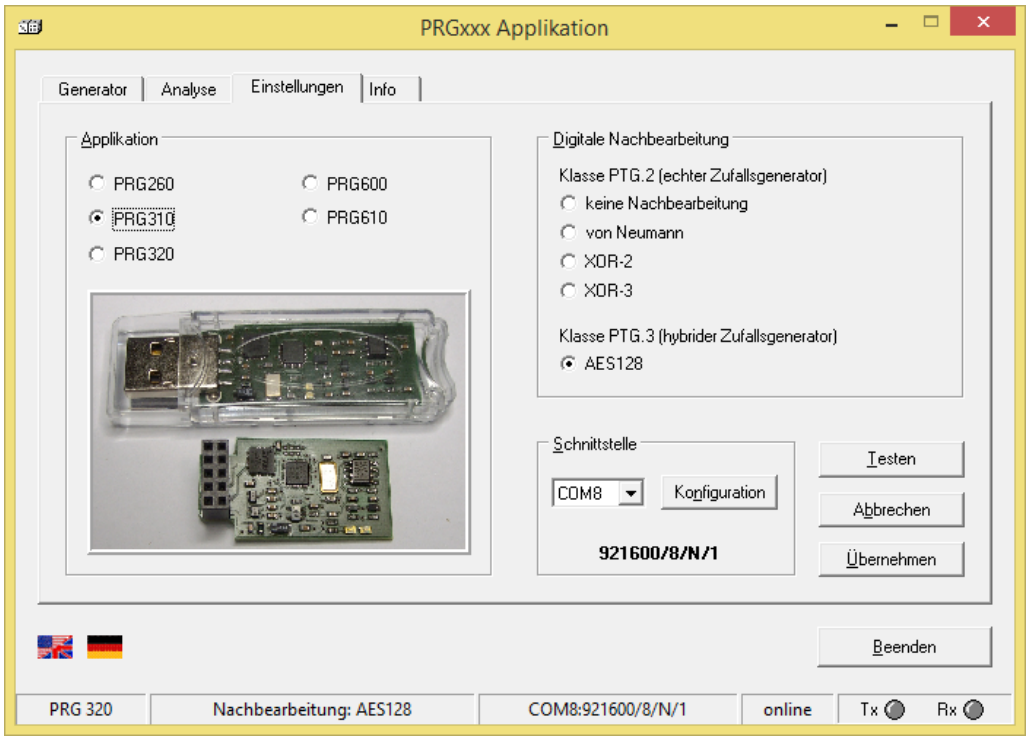


4 Einstellungen

Falls erforderlich, wählen Sie das Menü „Einstellungen" aus. Beim Verlassen des Programms werden die aktuellen Einstellungen gespeichert.

In diesem Menü wählen Sie die am PC angeschlossene Applikation, die Schnittstelle und die gewünschte Nachbearbeitung der generierten Zufallszahlen (hängt von der jeweiligen Applikation ab) aus.

In der Statuszeile (unten) werden die aktuellen Einstellungen abgebildet. Eine Umschaltung zwischen deutscher und englischer Dialogsprache ist in jedem Menü jederzeit möglich.



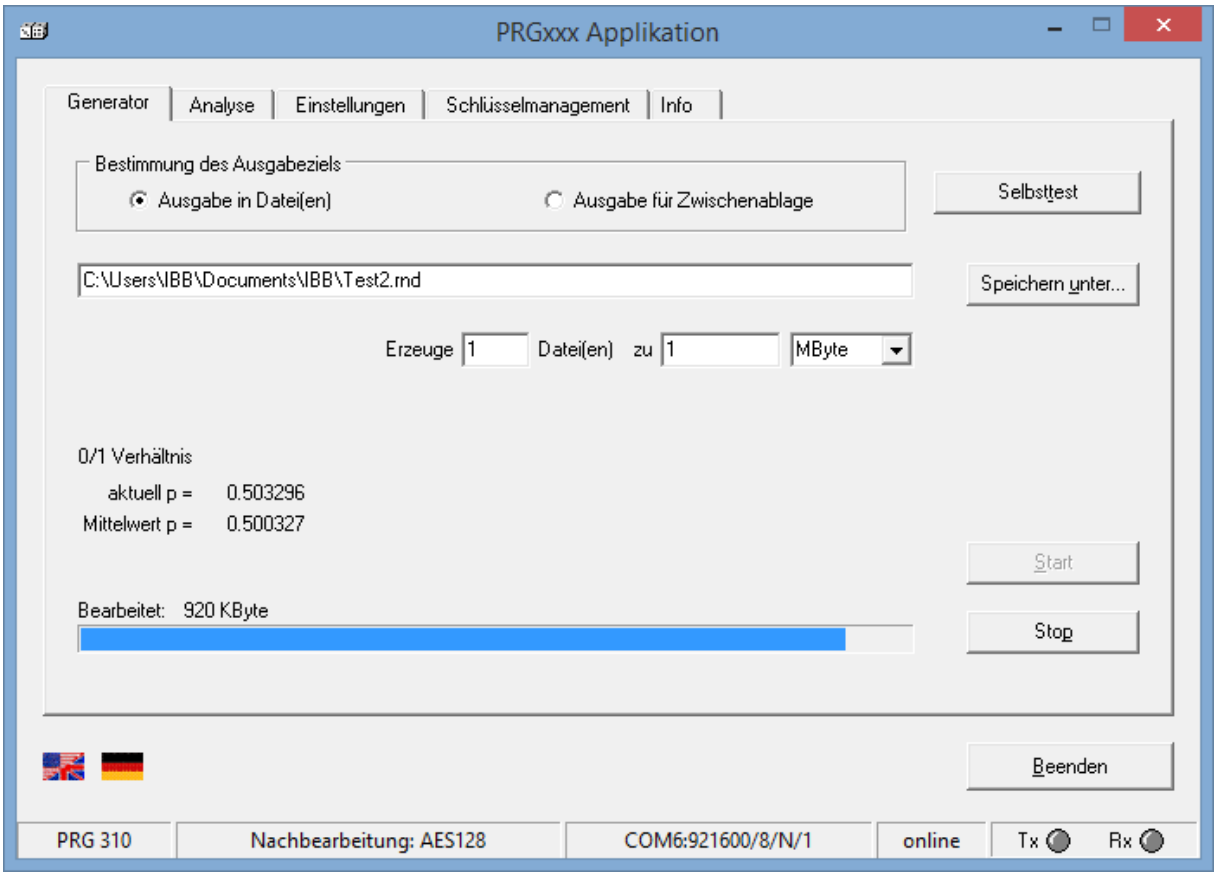
Die Parameter der Kommunikationsschnittstelle werden dem Handbuch der jeweiligen Applikation entnommen. Hier ein Beispiel für den PRG310-Zufallsgenerator:

5 Generator und Ausgabeziel

Auf der Seite „Generator" erfolgt die Generierung der Zufallsdaten. Die Schalttaste „Selbsttest" bewirkt einen intensiven Test des Zufallsgenerators auf Basis der erzeugten Rohdaten.

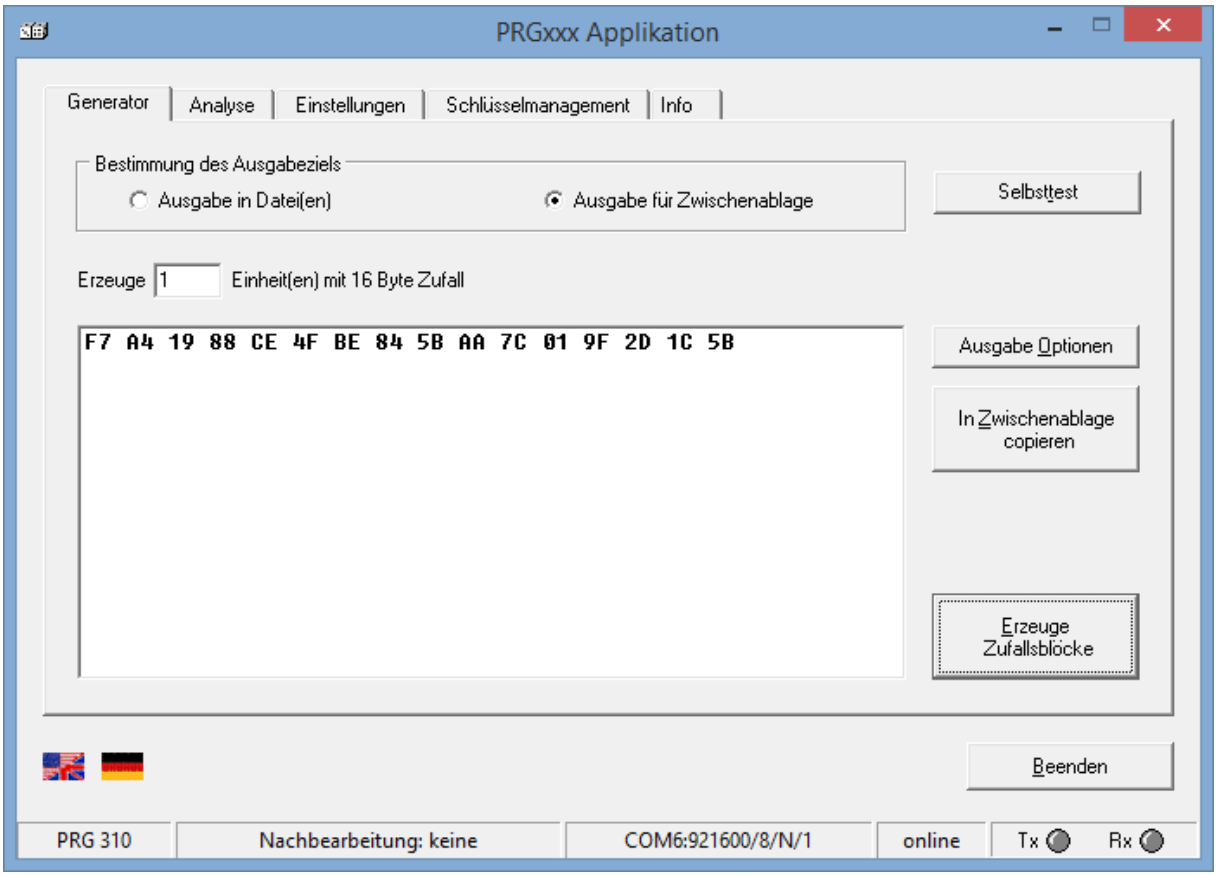
5.1 Ausgabe in Datei

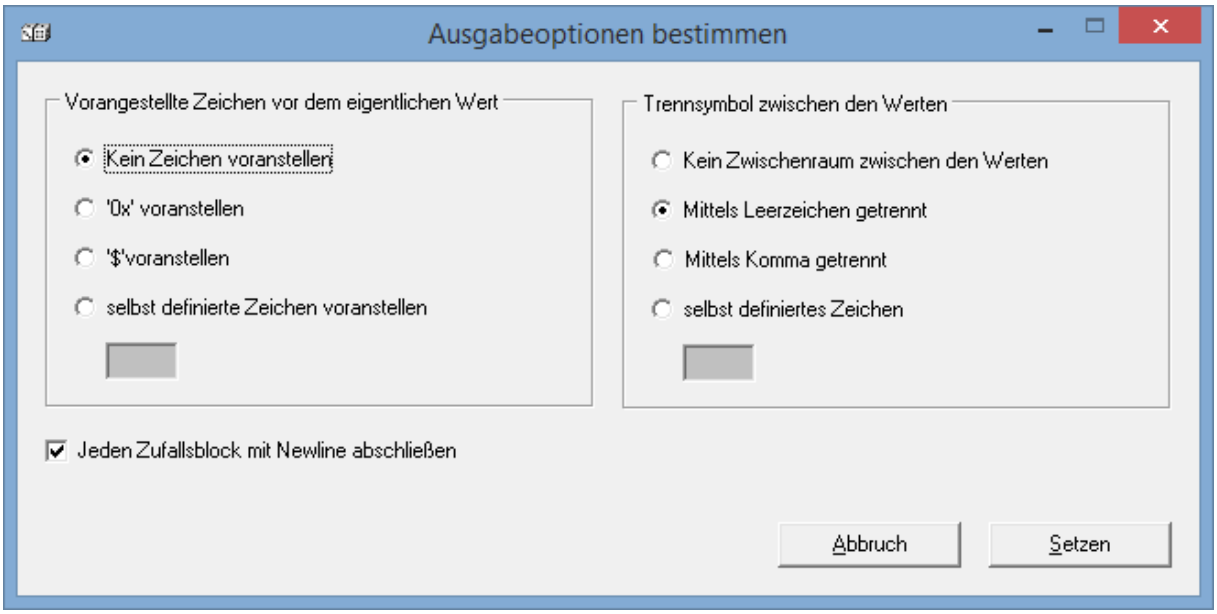
Die Generierung der Zufallszahlen kann durch Auswahl des Ausgabeziels variabel genutzt werden. Die folgende Abbildung zeigt die Generierung von Zufallszahlen und deren Abspeicherung in Dateien:



5.2 Ausgabe in Zwischenablage

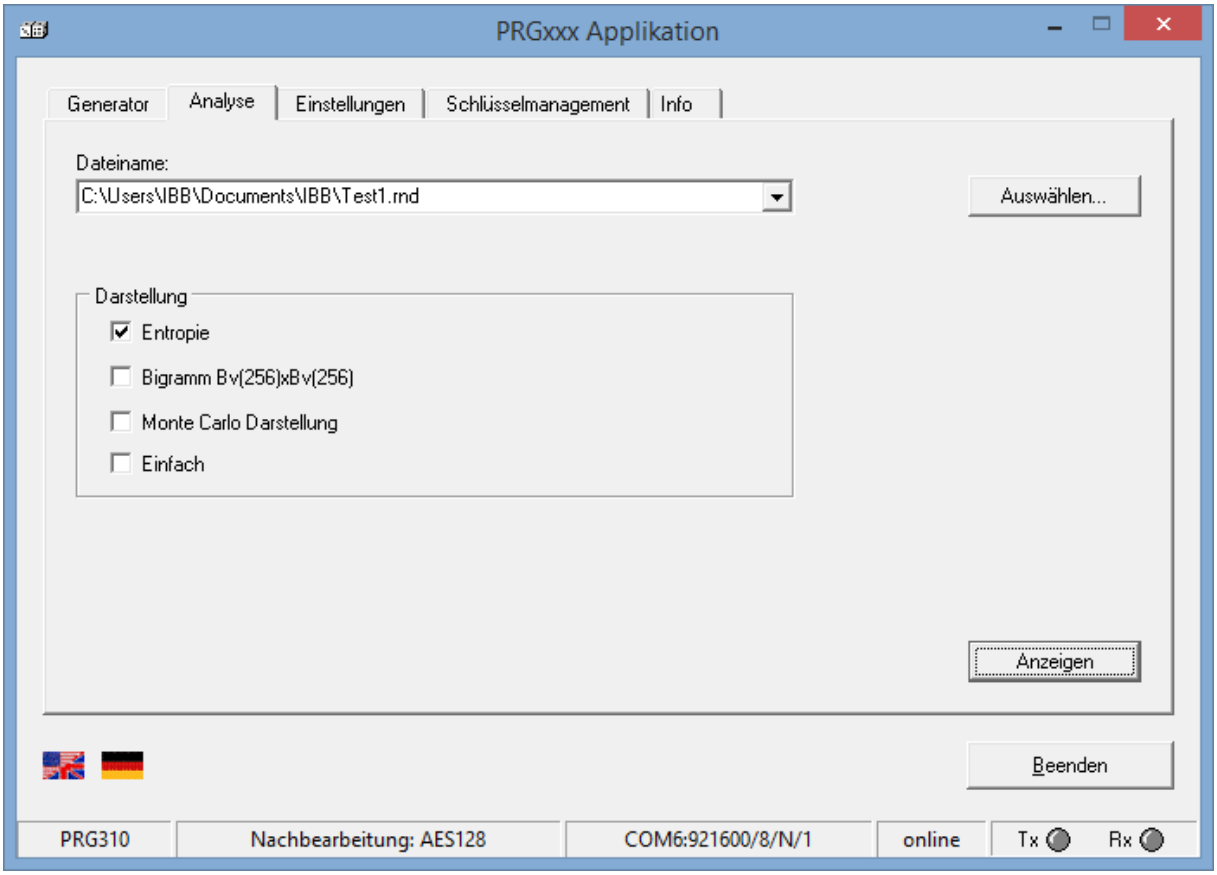
Eine weitere Variante der Zufallserzeugung kann für die Parametrisierung von Kryptosystemen genutzt werden. Die erzeugten Zufallszahlen können angezeigt und per Button in die Zwischenablage kopiert werden. Die generierten Zufallszahlen sind in variablen Formaten darstellbar und werden nicht durch die PRG-Applikation gespeichert.





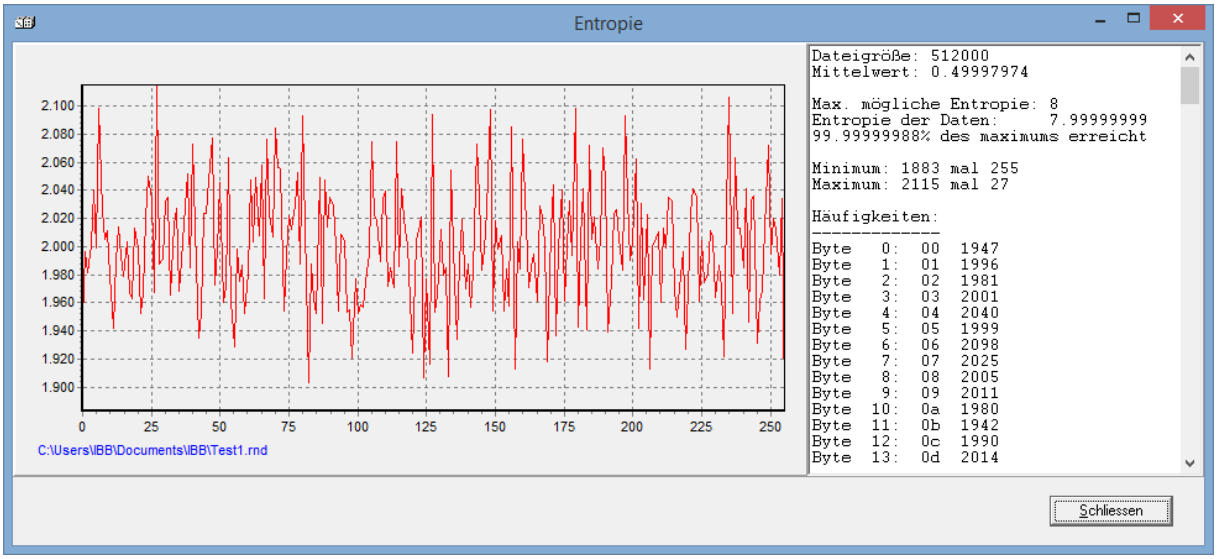
6 Analysen

Die Seite „Analyse" ermöglicht auf einfache Art und Weise numerische und grafische Auswertungen von Zufallsdaten. Es können alle Darstellungen auch gleichzeitig geöffnet werden. Die zu analysierende Datei wird ausgewählt:

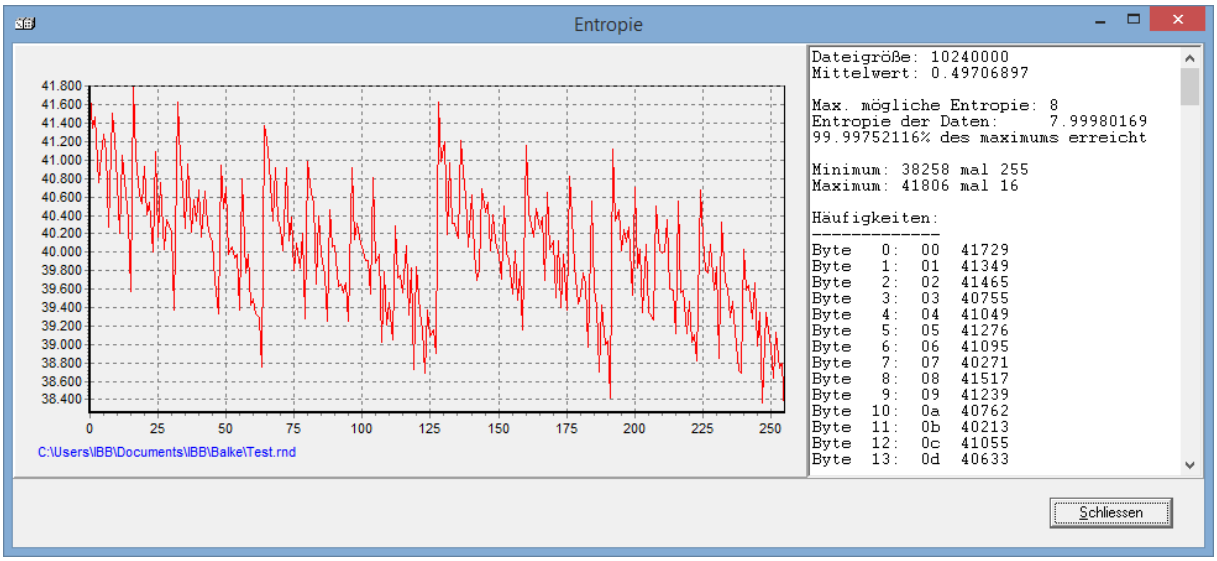


6.1 Entropie

Die Auswertung der Entropie (Berechnung nach Shannon) erfolgt numerisch. Graphisch werden alle Zufallsbytes in ihrer Häufigkeit dargestellt. Das folgende Beispiel zeigt gleichverteilte Zufallsdaten mit einer XOR3-Nachbearbeitung:



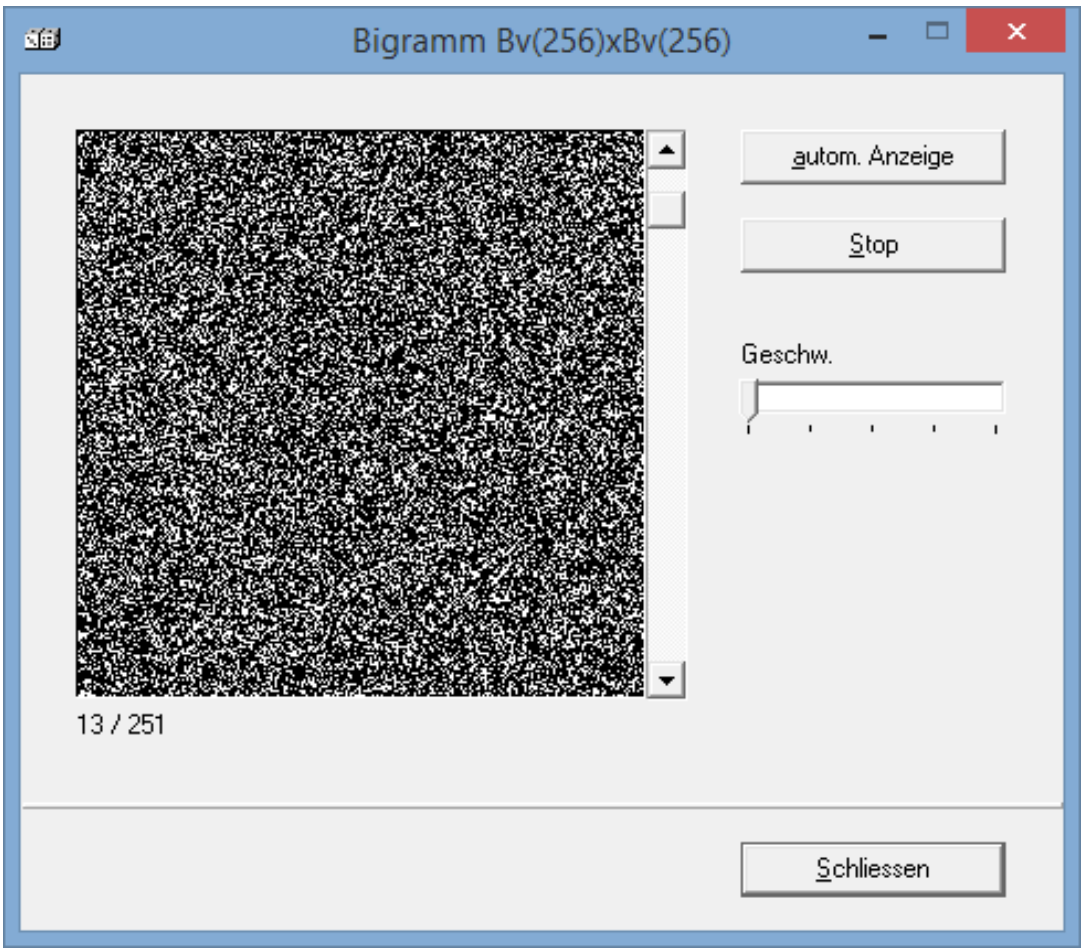
Das nächste Beispiel zeigt Zufallsdaten ohne digitale Nachbearbeitung (Rohdaten). Durch die Schiefe der 0/1-Verteilung ist eine Struktur in der Grafik zu erkennen. Diese wird durch die binäre Darstellung verursacht, keinesfalls durch deterministische Anteile der Zufallsdaten.



6.2 Bigramm-Darstellung

Bei der Bigramm-Darstellung werden zwei aufeinanderfolgende Zufallsbytes im Fenster als Punkt dargestellt. Dabei wird das erste Byte als x-Koordinate und das zweite als y-Koordinate verwendet.

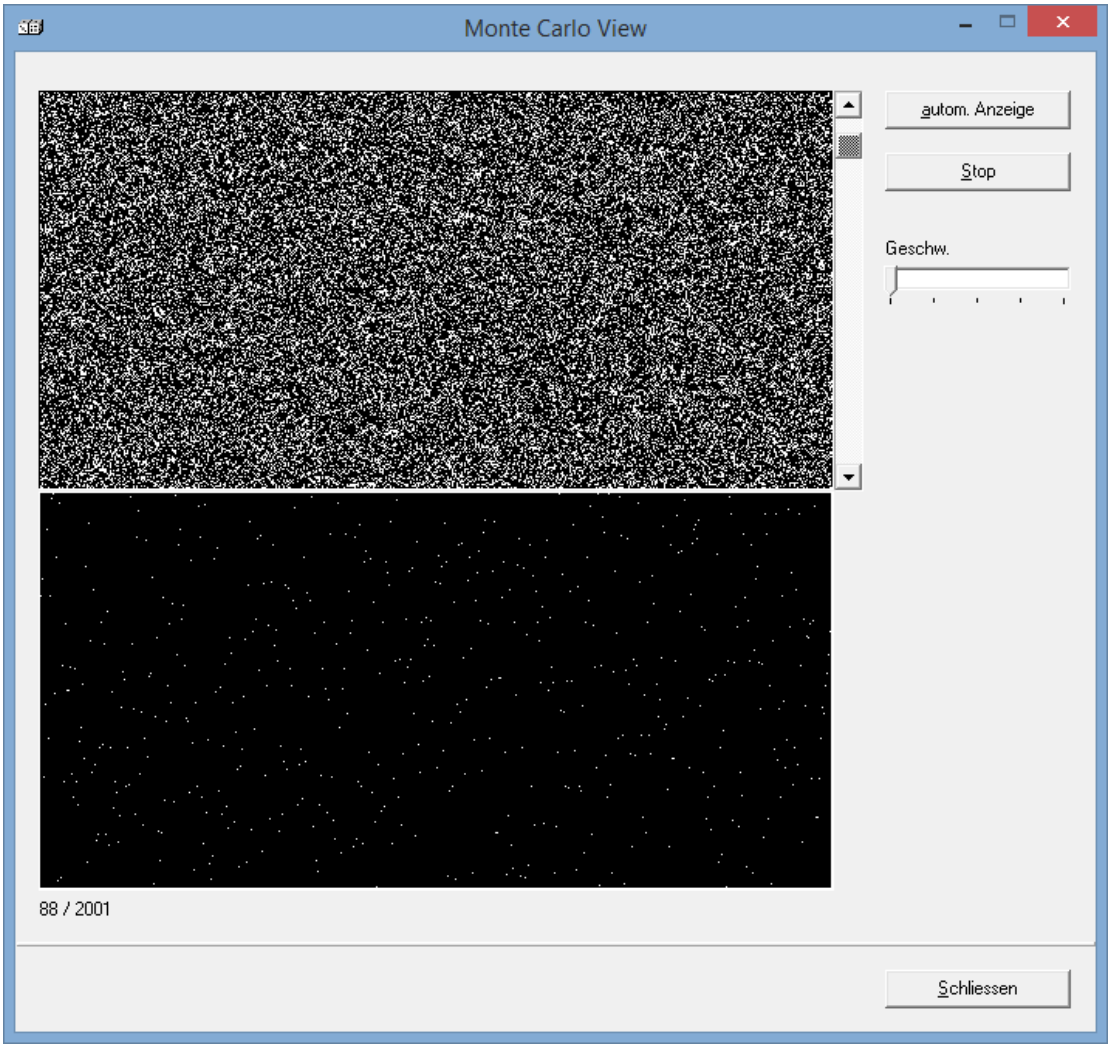
Um sich die Abschnitte (eingeblendet links unter dem Fenster) der Zufallsdatei komfortabel anzusehen, kann eine automatische Anzeige mit Wahl der Geschwindigkeit aktiviert und jederzeit angehalten werden.



6.3 Monte-Carlo-Darstellung

Bei der Monte-Carlo-Darstellung wird die x-Achse in 256 Schritte unterteilt. Im ersten Schritt der x-Achse wird der Wert des ersten Zufallsbytes in der y-Koordinate als Punkt dargestellt. Im zweiten Schritt der des zweiten Zufallsbytes. Ist der 256. Schritt als Punkt dargestellt, wird wieder mit dem ersten Schritt auf der x-Achse fortgesetzt. Das 257. Zufallsbyte wird also im ersten Schritt der x-Achse dargestellt, usw.

Das obere Fenster zeigt bereits aufaddierte Werte mehrerer Abschnitte (hier das 21. Fenster von insgesamt 19532), das untere eine aktuelle Darstellung von 256 Schritten mit ebenso vielen Zufallswerten.



6.4 Einfache Darstellung

Die Zufallsdatei wird in Abschnitte unterteilt und jeweils zwei aufeinanderfolgende Zufallswerte werden in einer y-x-Koordinate als Punkt dargestellt. In der farbigen Darstellung wird jedem Zufallswert ein Farbwert zugeordnet. Beim Aktivieren der automatischen Anzeige werden je nach gewählter Geschwindigkeit alle Abschnitte der Zufallsdatei durchlaufen und angezeigt.

7 Key-Management

Beim Key-Management handelt es sich um Funktionen zum Abspeichern von Schlüsselinformationen und PINs. Diese Funktionen können vollkommen unabhängig von den Funktionen zur Zufallserzeugung genutzt werden und ist nicht bei allen PRG-Applikationen verfügbar.

Die Schlüsselverwaltung umfasst folgende Funktionen:

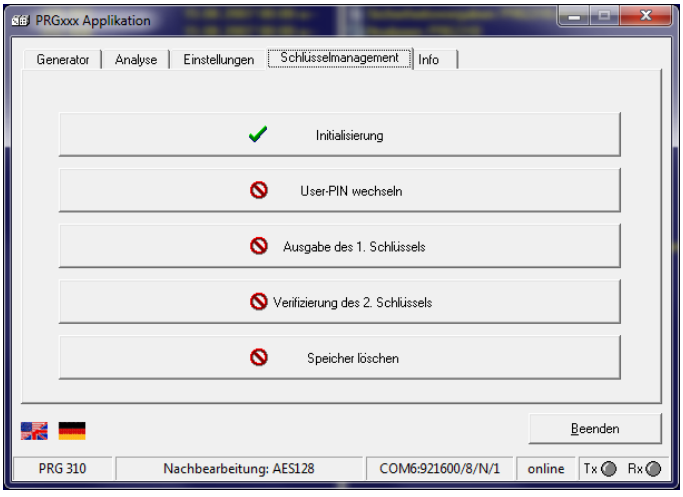
- Initialisierung in gesicherter Umgebung von:
  - 192 Byte Schlüssel 1
  - 192 Byte Schlüssel 2
  - 8 Byte User-PIN
  - 8 Byte Master-PIN
- Neueingabe (Ändern) der User-Pin
- Ausgabe von Schlüssel 1
- Verifizieren von Schlüssel 2
- Zustandsabfrage
- Löschen des Speichers nach Eingabe der Master-Pin

Für alle Funktionen gilt: der vollständige Datentransfer zur PRG-Applikation muss innerhalb von 10 Sekunden abgeschlossen sein. Wird das nicht realisiert, wird mit einer Fehlermeldung und der Inkrementierung eines Fehlerzählers abgebrochen.

Der Fehlerzähler wird bei jeder Fehlfunktion (falsche Pin, falsch verifizierter Schlüssel 2, Zeitüberschreitung) inkrementiert. Sind 5 Fehlerereignisse registriert, werden alle weiteren Handlungen, auch bei richtiger Eingabe, mit einer Fehlermeldung quittiert. Der Fehlerzähler kann danach nur noch durch PON gelöscht werden. Damit soll ein Ausprobieren der vertraulichen Informationen verhindert bzw. sehr erschwert werden.

Die Initialisierung sollte in einer gesicherten Umgebung durchgeführt werden. Angewendet werden kann das Key-Management zur Authentisierung, zur Authentisierung eines Administrators oder zur Authentisierung von Applikationen.

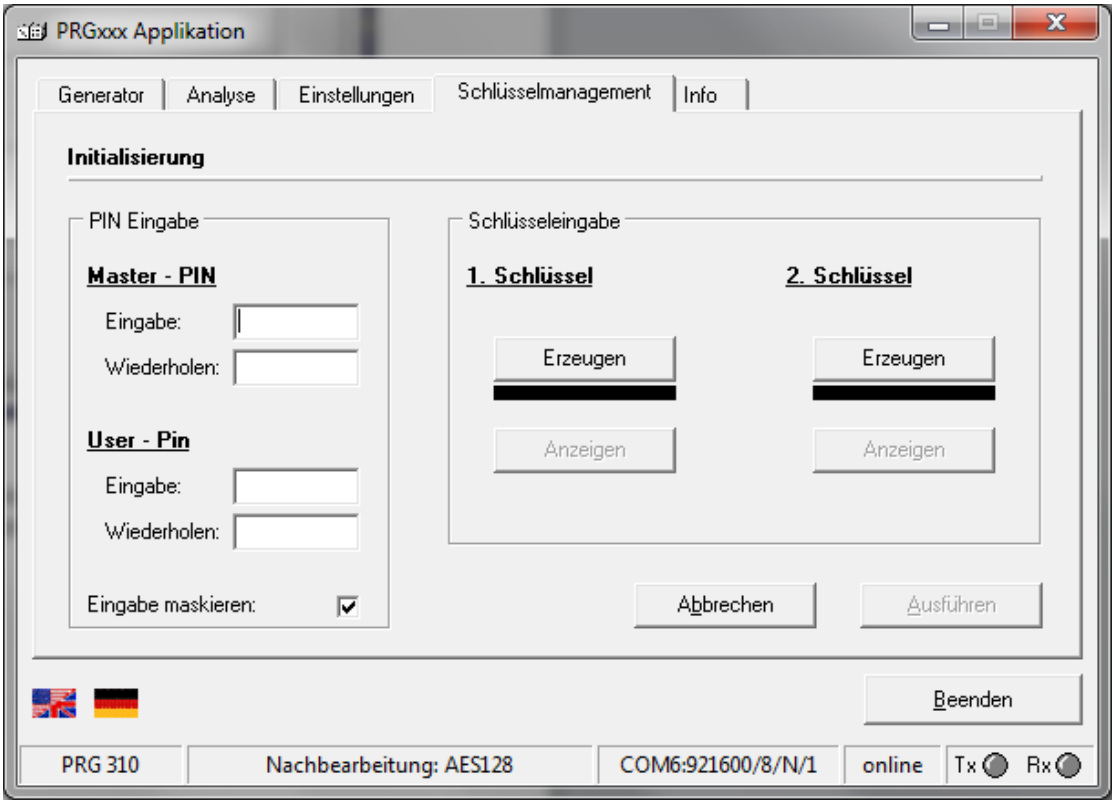
Die den Applikationen beiliegende Software PRG100 ermöglicht die vollständige Anwendung des Key-Managements. Im Folgenden sollen alle Funktionen demonstriert werden:



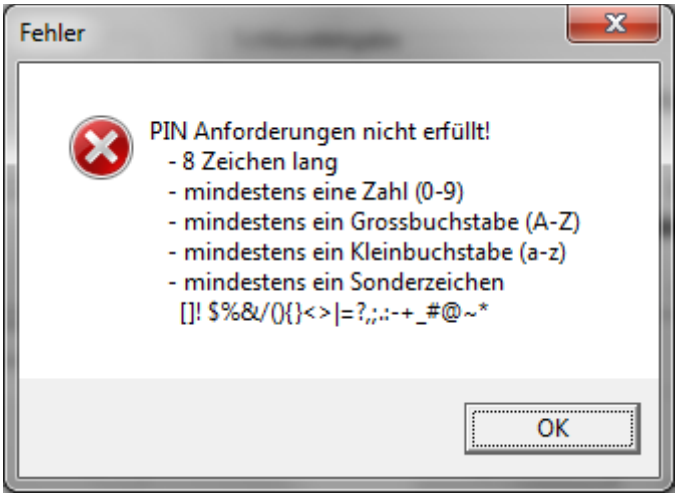
Die Seite Schlüsselmanagement zeigt Status und Möglichkeiten. Beim Aufruf wird automatisch der Status der angeschlossenen PRG-Applikation geprüft und angezeigt, welche Funktionen möglich ist.

7.1 Initialisierung

Die Maske vor der Initialisierung zeigt alle einzugebenden Parameter:

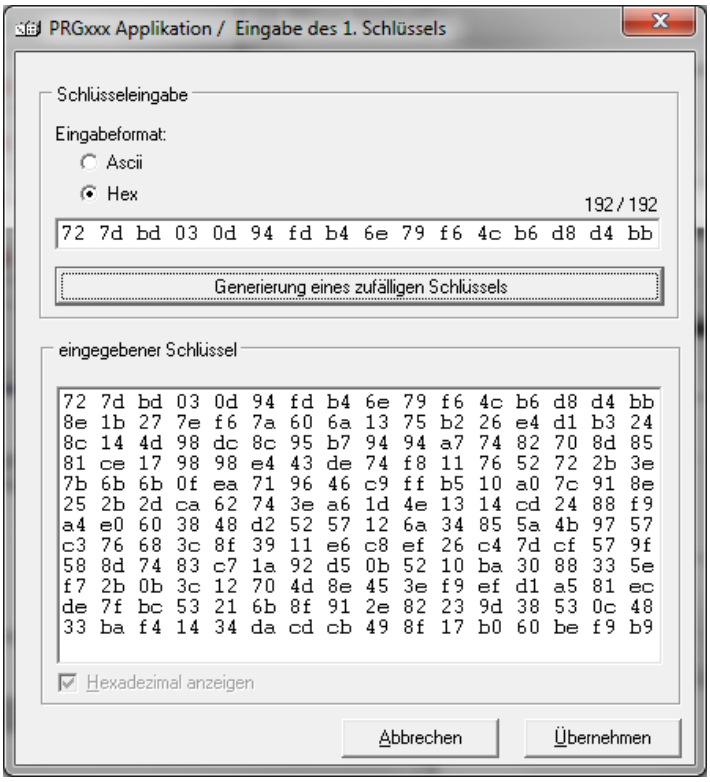


Die User- und Master-Pin kann maskiert oder unmaskiert eingegeben werden und muss folgende Bedingungen erfüllen:

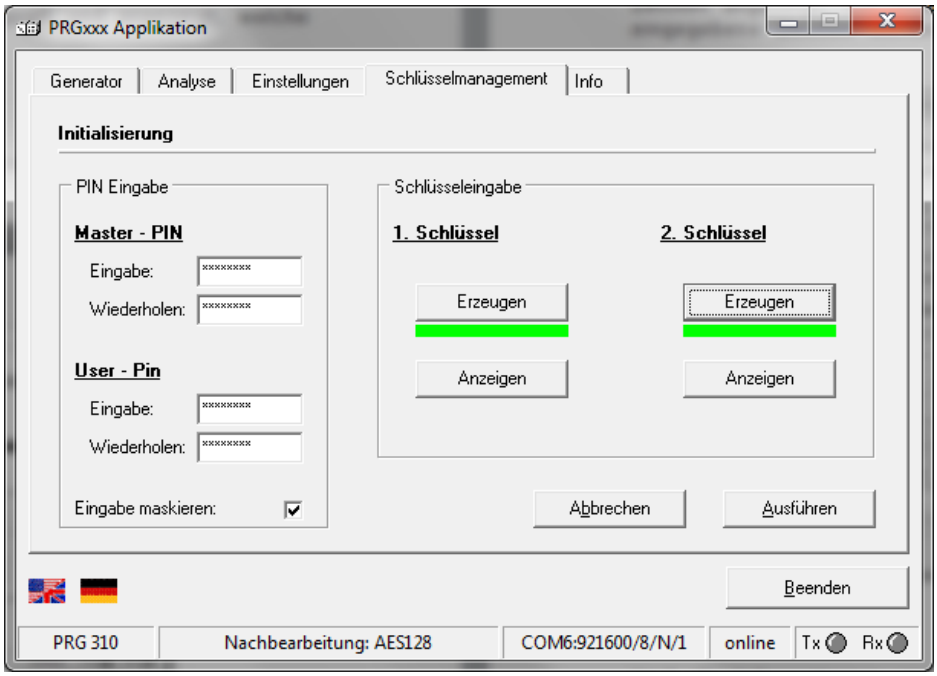


Die Schlüsseleingabe kann im ASCII-Code oder hexadezimal erfolgen. Die Software kann auch einen zufälligen Schlüssel generieren. Im unteren Feld werden alle 192

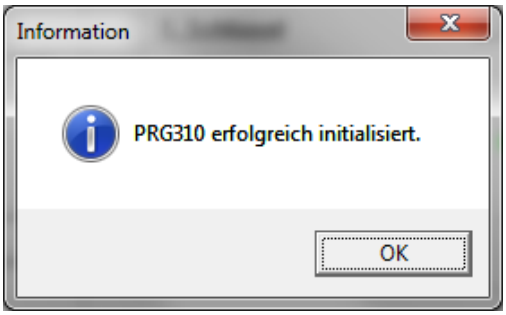
Zeichen angezeigt. Die Anzahl der ein zugebenen Zeichen ist beliebig. Nicht eingegebene Zeichen werden mit „Space" (0x20) hinterlegt.



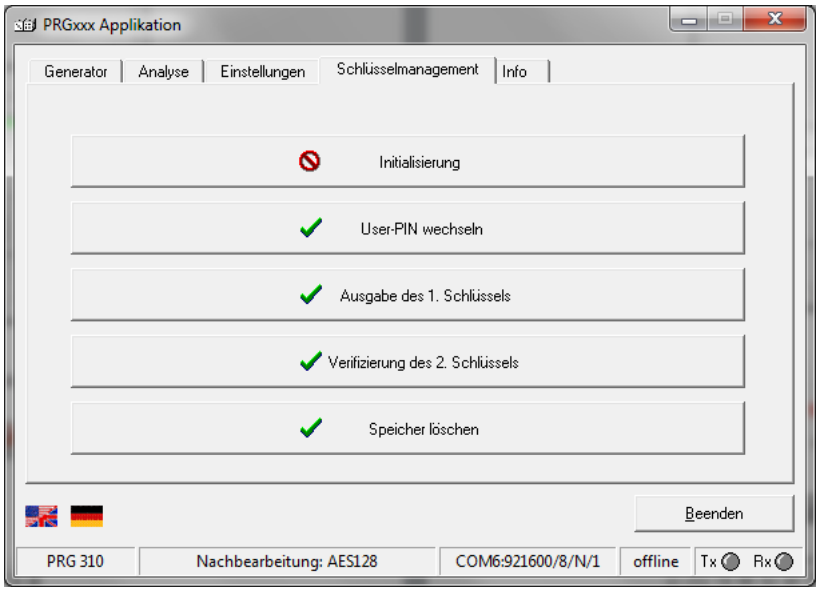
Sind alle Informationen eingeben, werden die Daten zur PRG-Applikation übertragen.



Alle Informationen sind vollständig eingegeben und werden mit „Ausführen" zur PRG-Applikation übertragen.

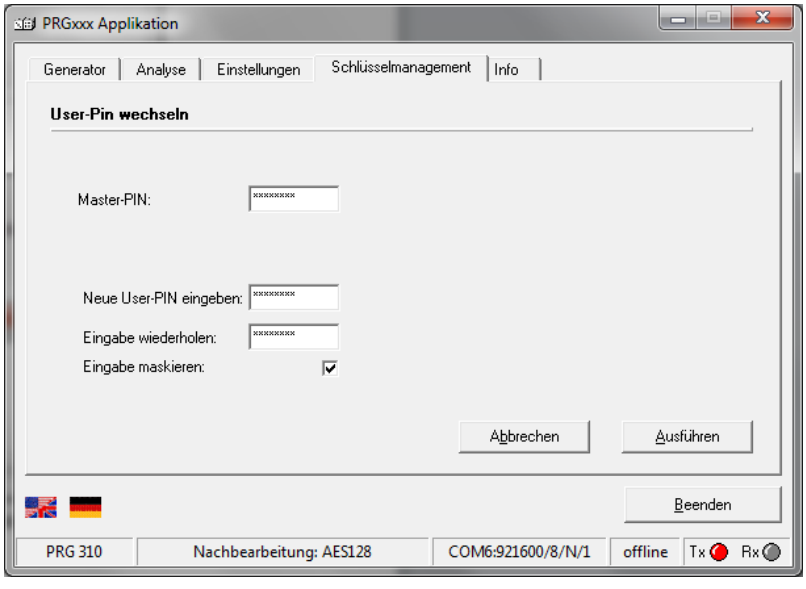


Das Menü-Bild des Key-Managers zeigt nun die sich aus der Initialisierung ergebenden Möglichkeiten:



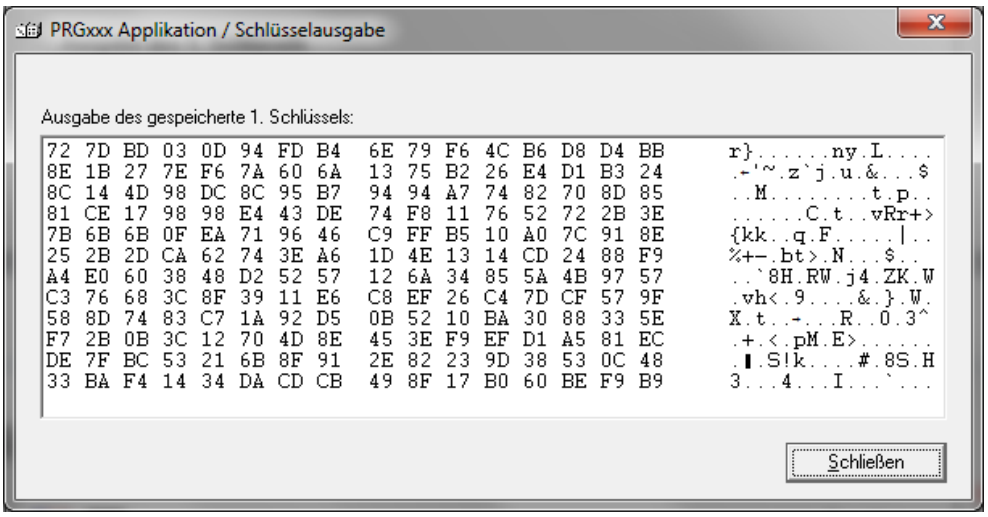
7.2 User-Pin wechseln

Aus Sicherheitsgründen kann ein Wechsel der User-Pin erforderlich sein:



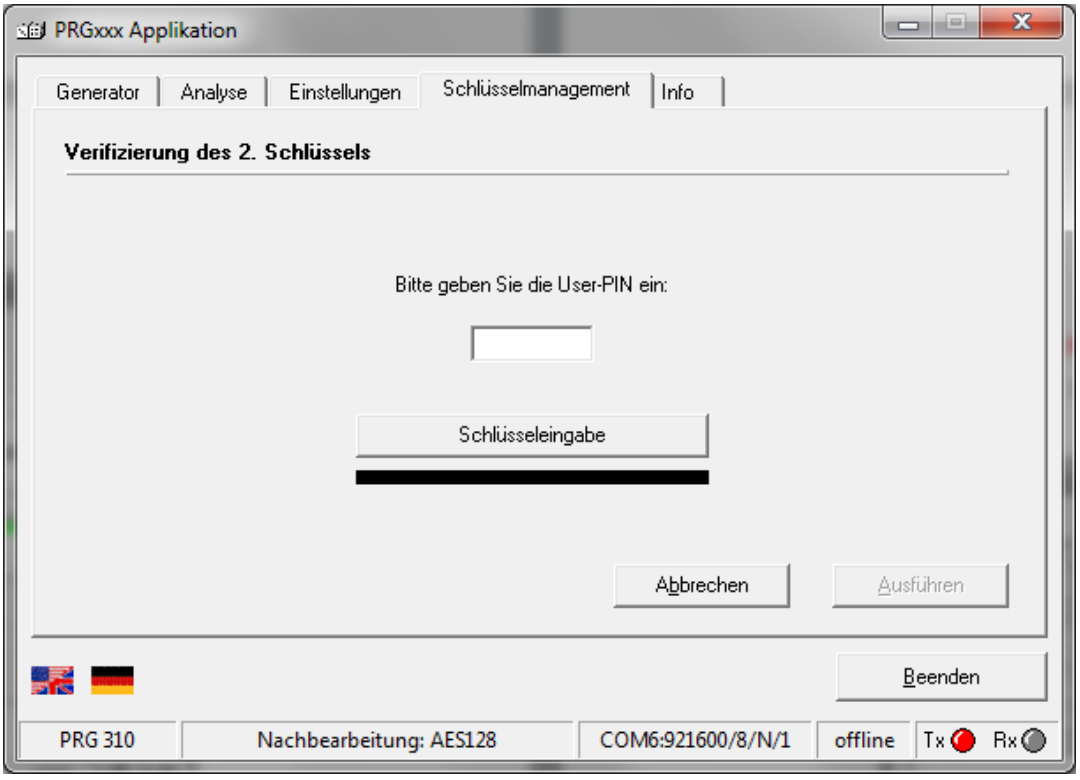
7.3 Ausgabe Schlüssel 1

Nach Eingabe der User-Pin wird der Schlüssel 1 ausgegeben und angezeigt:



7.4 Verifizieren Schlüssel 2

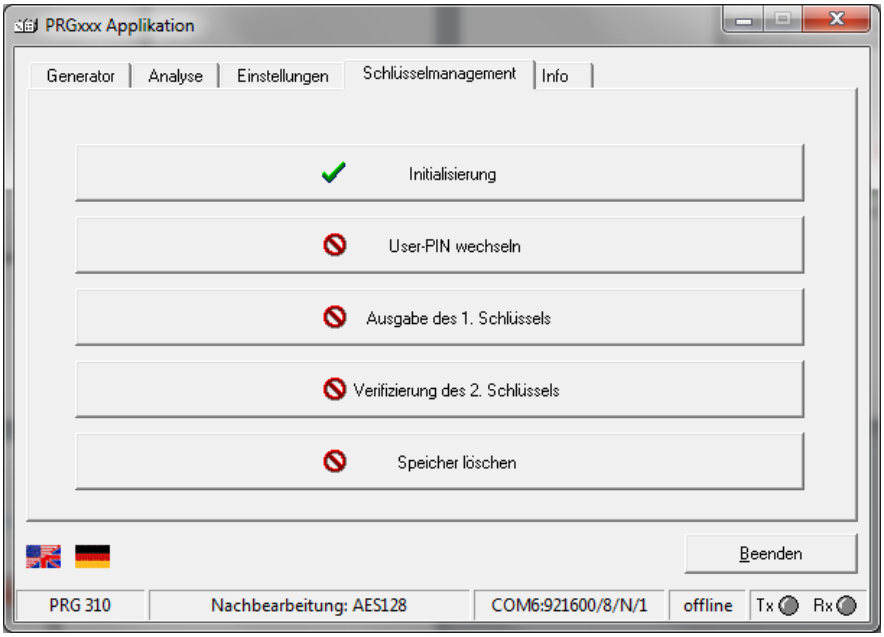
Schlüssel 2 kann nicht mehr ausgegeben, sondern nur indirekt bestätigt werden. Hierzu muss die User-Pin und der identische Schlüssel 2 eingeben werden:



7.5 Speicher löschen

Diese Funktion erfordert die Master-Pin. Anschließend werden alle Parameter im Speicher des Mikrocontrollers gelöscht:

Danach stellt sich wieder der Auslieferzustand des Key-Managers ein:



7.6 Sicherheitshinweise

Ist die Master-Pin nicht mehr bekannt, gibt es keine Möglichkeit durch den Nutzer, den Speicher zu löschen. Die PRG-Applikation ist in diesem Fall zum Hersteller zu sende. Der Programm- und Datenspeicher wird vollständig gelöscht und neu programmiert. Auch der Hersteller hat keine Möglichkeiten Informationen des Key-Managers auszulesen!