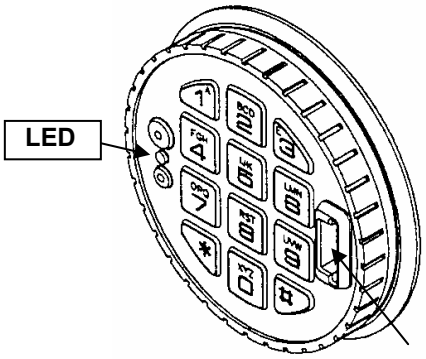
CRYPTO-GARD 66E BR 11 Systembeschreibung

Tastatur 3123

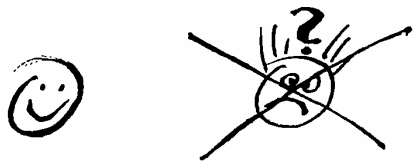


Dieses Schloss integriert 2 unabhängige Code-Systeme, die parallel genutzt werden können.

A) Das Banksystem mit 3 Öffnungscodes im 4-Augen-Prinzip, (Öffnungsverzögerung und Überfallalarm zuschaltbar).

B) Das CRYPTO-System mit einem einmalig nutzbaren, PC-generierten Öffnungscode

Hervorzuheben ist die einfache Bedienung in beiden Systemen und die leichte Montage des Schlosses.



System A) Es stehen 2 Öffnungscodes, 1 Managercode, 1 Master-/Kontroll-Code, zur Verfügung. Jeder Code kann manuell geändert werden. Flexible Programmgestaltung: Einzelcode-Betrieb oder Doppelcode-Betrieb, Öffnungsverzögerung, Überfallalarm. Dieses System kann abgeschaltet werden.

System B) Das CRYPTO-System arbeitet mit einem vom PC der Zentrale generierten Code (7-stellig), der nur für eine einmalige Öffnung und nur in einem definierten Zeitfenster für einen bestimmten Benutzer (mit PIN 4-stellig) gültig ist.
Keine Kabelverbindung zur Zentrale.

⇨ Die unabhängige Nutzung beider Systeme ermöglicht der Bank eine flexible Organisation der Geldversorgung. Das System B kann z.B. später zugeschaltet werden – ohne eine Änderung am Schloss vorzunehmen. Die Zuschaltung erfolgt über die Schloss-Tastatur mit dem Kontroll-/Master-Code und einem PC-generierten Aktivierungscode.

⇨ Im Zentralcomputer (PC) wird das Programm „BR11 CRYPTO“ geladen und eine Hierarchie der PC-Bediener festgelegt. Ferner werden alle zu bedienenden Schlösser mit Nummer und Standort festgelegt, sowie die Schloss-Benutzer mit Namen und 4-stelligem PIN-Code eingegeben.

⇨ Der Schlossbenutzer (Geldtransporteur) meldet sich per Funk bei der Zentrale an und erfragt für das entsprechende Schloss einen Öffnungscode. Der PC-Bediener ruft den Benutzer am PC auf, wählt das Schloss aus und erhält einen 7-stelligen Code angezeigt, der an den Benutzer übermittelt wird. Der Benutzer gibt an der Schlosstastatur seinen PIN und den übermittelten Code ein und kann öffnen. Die Öffnung oder Nichtöffnung wird der Zentrale bestätigt (positiv/negativ) . Der übermittelte Code ist nur ca. 15 min. gültig.

PROTOKOLL: Der Zentralcomputer speichert alle Vorgänge (Benutzer, Schloss-Nummer mit Zeit und Datum), so dass eine Verifikation aller Vorgänge sowohl von der Zentrale als auch in jedem einzelnen Schloss gegeben ist.
Die Protokollierung im Schloss zeichnet sowohl die Vorgänge des A-Systems als auch die Vorgänge des B-Systems auf.

Hardware: Das CRYPTO-GARD arbeitet in allen Schlössern mit 66E-Elektronik und BR 11-Software: COMBOGARD 6040-BR11, SAFEGARD-SWINGBOLT 6260-BR11 und SAFEGARD-OVERRIDE 6441-M-BR11 und hat die Tastatur 3125 oder 3090K.

Alarmanlagenanschluss über Sperreinrichtung „SP“ inklusive Stromversorgung (12V) aus EMA.

1. Factory-Mode: Schloss öffnet mit „1“ und sendet Alarm. In diesem Zustand kann das Schloss montiert werden (Endmontage).

2. Schloss-SETUP: Programm „BR11 –SETUP“ installieren:
Betriebssystem Windows 95/98 sowie 4 MB Speicherplatz auf Festplatte erforderlich.
Port COM: 1200 bauds, no parity, 8 data bits, 1 stop bit festlegen.
Programm-Diskette laden, mit SETUP.EXE (englisch) oder INSTALL.EXE (französisch)

   Vorgegebene Codes: Master, Manager und 2 Benutzer
   Programmauswahl: Einzelcode-Betrieb
   Dual Combo (Doppelcode-Betrieb)
   Duress Alarm: (Überfallalarm)
   Time Delay: (Öffnungsverzögerung)
   Programmierung: Interface-Kabel mit Leserschlitz der Schlosstastatur verbinden, auf dem PC-Display Stecker-Symbol anklicken und an der Schlosstastatur „0“ drücken – auf PC-Display erscheint „Communication in progress“ und „DONE“, die Programmierung ist beendet. Der vorgegebene Master-Code muss zur Aktivierung geändert werden.

   ⇨ Master-/Kontroll-Code ändern: „0“ gedrückt halten bis zum nochmaligen Doppelsignal (Master-Code-Erkennung), alten, 8-stelligen Code eingeben und letzte Zahl gedrückt halten bis LED an bleibt. Funktion „0“ (=Code ändern) drücken und neuen Code 2 x eingeben (LED aus).

a) Manager-Funktion: Manager kann Benutzer zulassen (Funktion „1“); zeitweilig sperren (Funktion „2“) oder löschen (Funktion „3“), Protokoll auslesen (Funktion „7“), Öffnungsverzögerung einstellen (Funktion „9“), Seite 5.
   Bei Doppelcode-Betrieb muss zur Programmierung ein zugelassener Benutzercode vor dem Managercode eingegeben werden.
   Öffnen: Bei Doppelcode-Betrieb Manager-Code als ersten Code eingeben.
   Alarm auslösen: Letzte Code-Zahl +1/-1 eingeben.
   Beim Einzelcode-Betrieb kann der Manager nicht öffnen.

b) Benutzer-Funktion: Code ändern: Alten Code eingeben und letzte Zahl gedrückt halten bis LED an bleibt, Funktion „0“ drücken und neuen Code 2 x eingeben (LED aus).
Öffnen: Bei Einzelcodebetrieb, Code eingeben (Doppelton) und innerhalb 3 sec. öffnen.
Bei Doppelcodebetrieb werden 2 gültige Codes eingegeben.
Alarm auslösen: letzte Code-Zahl +1 oder -1 eingeben.

c) Master-/Kontroll -Funktion: (kann nicht öffnen), Protokoll auslesen, (Funktion 7) CRYPTO-System zuschalten (Funktion 6), Software-Reset (Funktion 8).
Protokoll auslesen: „0“ gedrückt halten bis zum nochmaligen Doppelsignal, 8-stelligen Code eingeben und letzte Zahl gedrückt halten (LED an), Funktion „7“ drücken (PC-Programm LG VIEW muss aufgerufen und Safe-Symbol angeklickt sein sowie Interface-Kabelverbindung zur Schlosseingabe hergestellt sein.)
   ⇨ Aktivierung des CRYPTO-Systems mit Funktion „6“.
   „0“ gedrückt halten bis zum nochmaligen Doppelton, Master-/Kontroll-Code eingeben und letzte Zahl gedrückt halten bis LED an bleibt, „6“ drücken und 12-stelligen AKTIVIERUNGS-Code (vom PC generiert) eingeben.
   Das CRYPTO-System ist zugeschaltet.
   (Positive Aktivierung der Zentrale melden und dort „Pos. Ack“ anklicken).
   Die Aktivierung synchronisiert auch die Zeit vom PC zum Schloss.
   Der Aktivierungscode soll deshalb unmittelbar nach dem Aufrufen am Schlosse eingegeben werden.

a) **Set-Up**: „BR11 CRYPTO“ ist eine Code-Generator-Software für BR11-Schlösser. Der PC der Zentrale wird mit dieser Software (2 Disketten) geladen (Set-Up. EXE) und arbeitet mit Windows 95/98.

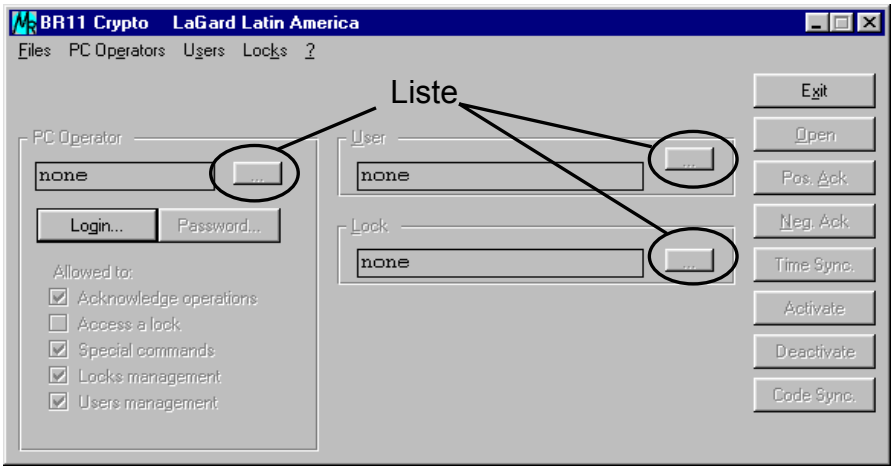
1. Beim ersten Aufrufen des BR11 CRYPTO-Programms erscheint: „INITIALIZE DATA BASE“, „OK“ anklicken.
2. PC-Master-Name mit Password eingeben (ENTER).
3. Es wird nach Sommer-/Winterzeit (DST) gefragt. Entsprechende Daten anklicken (letzter Sonntag, Mrz/Okt.) und „OK“. (Später aufrufbar unter „Files“).
   Die Schaltzeiten sind wichtig, da der später errechnete Code nur 15 Minuten gültig ist.

b) Bediener-Hierarchie: Der PC-Master kann PC-Manager und PC-Bediener zulassen, sperren und jedem verschiedene Operationsfelder zuweisen.

Operationsfelder:

Acknowledge Operations	=	Bestätigung der positiven oder negativen Öffnung
Access a Lock	=	Aufrufen des Öffnungscodes
Special Commands	=	Aktivierung, Deaktivierung, Synchronisation der Schlösser
Locks Managements	=	Schloss zulassen, Löschen, Standortbeschreibung
User Managements	=	Schloss-Benutzer zulassen oder löschen

c) Arbeitsdisplay: Nachdem sich ein PC-Bediener durch Eingabe des Namens (ENTER) und Password „eingeloggt“ hat, erscheint das Haupt-Arbeitsdisplay.



d) PC-Bediener zulassen: Im PC-Operator-Kasten rechts vom Namen das Feld (...) anklicken. Es erscheint die Liste der Bediener: „NEW“ anklicken. Es erscheint „PC-OPERATOR-FOR“. Hier wird der Name eingegeben (ENTER) und die Operationsfelder angeklickt, dann „OK“.

e) Schloss-Benutzer: (Geldtransporteure) Jeder mögliche Benutzer wird mit Namen, Rufnamen, interner ID#, Geburtsdatum, Rufname unter Bedrohung und einem 4-stelligen, persönlichen PIN (Password) eingegeben. Der PIN-Code wird später zur Öffnung des Schlosses benötigt: Rechts im USER-Feld (...) anklicken. Es erscheint die Liste der Benutzer. „NEW“ anklicken und Benutzer eingeben (ENTER) und „OK“ anklicken.

f) Schloss-Datei: Jedes Schloss wird mit Seriennummer und Standortangabe in die Schlossliste eingegeben. Rechts im LOCK-Feld (...) anklicken. Es erscheint die Liste der Schlösser „NEW“ anklicken, Daten eingeben und „OK“ anklicken.

A) Der PC-Bediener ruft „BR11 CRYPTO“ auf und meldet sich an, indem er seinen Namen (mit Password) im „LOG-IN“ Fenster einschreibt (ENTER).
Es erscheint das Arbeitsdisplay.

B) Der Schloss-Benutzer meldet sich per Funk mit Ort und Namen. Beim PC-Bediener. Der klickt das Feld (...) neben „USER“ an und erhält die Liste der Schloss-Benutzer, wählt den Namen aus und sieht unten persönliche Daten. Es wird der Rufname (Nickname) abgefragt und klickt auf „OK“ (oder rechter Mausklick).

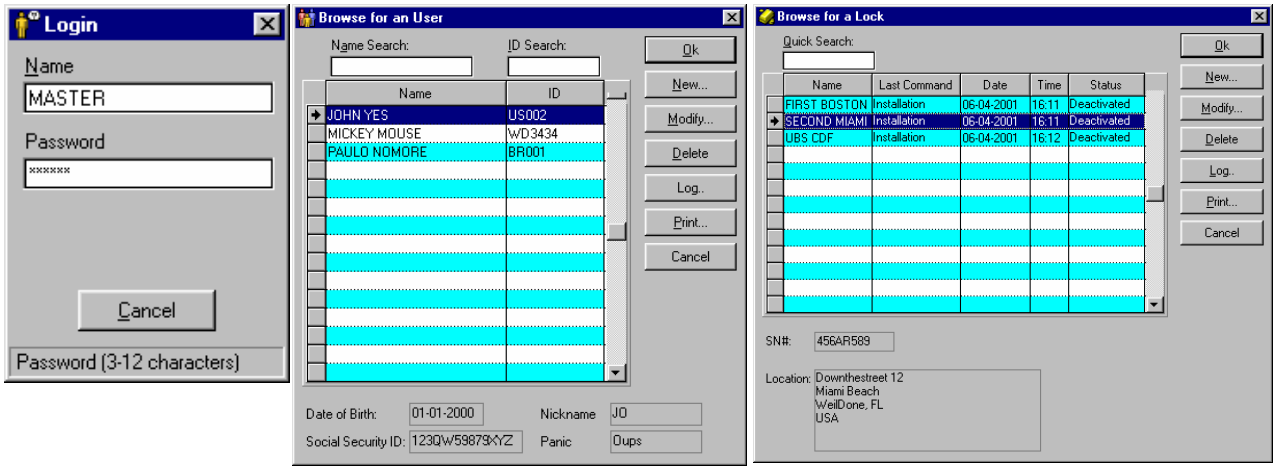
C) Dann wird das Schloss nach Ort bzw. Nummer ausgewählt, rechts neben „LOCK“Feld (...) anklicken, Liste erscheint, Schloss auswählen und „OK“ (oder rechter Mausklick.)

D) Im Arbeitsdisplay steht der Benutzer und die Schlossbezeichnung. Der PC-Bediener klickt „OPEN“ an und erhält einen 7-stelligen Code angezeigt, der dem Schloss-Benutzer durchgesagt wird und nun ca. 15 Minuten gültig ist.

E) Der Benutzer drückt an der Schloss-Tastatur „1“ bis zum nochmaligen Doppelsignal, gibt seinen persönlichen 4-stelligen PIN-Code (Doppelsignal) und den übermittelten 7-stelligen Code ein (Doppelsignal) und öffnet.
Überfallalarm: Letzte Zahl des 4-stelligen PIN +1 oder –1 eingeben.

F) Die Öffnung gibt er der Zentrale durch und der PC-Bediener klickt „Pos. Ack“ (positive Öffnung) an.

G) Sollte ein Übermittlungsfehler vorliegen und der Code nicht öffnen (3-fach-Signal), gibt der Benutzer „Negativ“ zur Zentrale und der PC-Bediener klickt „Neg. Ack“ an. Ein neuer Code für diesen Benutzer und dieses Schloss wird angezeigt, wenn „Open“ angeklickt wird.



CRYPTO-GARD 66E BR11 Kurzübersicht/System A

Das CRYPTO-GARD vereinigt zwei Code-Systeme in einem Schloss, die parallel nutzbar sind.

System A: Üblicher Mehrcodebetrieb mit manuell änderbaren Codes.
System B: Das CRYPTO-System mit einem PC-generierten Einmal-Code.

a) Programmierung: System A:
Code eingeben und letzte Zahl gedrückt halten bis LED an bleibt, dann Funktionsnummer eingeben:

FUNKTIONEN:
- „0“ = Code ändern und neuen Code 2 x eingeben.
- „1“ = Benutzer zulassen: Benutzer-Nr. eingeben und Code 2 x eingeben.
- „2“ = Benutzer sperren: Benutzer-Nr. eingeben (gesperrt bis wieder zugelassen mit „1“).
- „3“ = Benutzer löschen: Benutzer-Nr. eingeben
- „6“ = CRYPTO-System (B) aktivieren.
- „7“ = Protokoll auslesen (mit PC „LG-VIEW“ und Interface-Kabel).
- „8“ = Schloss-Reset auf Factory-Mode (dann Manager-Code eingeben).
- „9“ = Öffnungsverzögerung zuschalten. (4-stellige Zahl eingeben Stelle 1+2 Verzögerungszeit, 1-99 min. Stelle 3-4 Öffnungsfenster 1-19 min und bestätigen).

b) Code-Hierarchie
Master-/Kontroll-Code: 8-stellig, kann nicht öffnen, Funktionen 0,6,7,8 möglich.
Eingabe: „0“ gedrückt halten bis nochmaliges Doppelsignal, (Mastercode-Erkennung) Code eingeben und letzte Zahl gedrückt halten bis LED an bleibt, Funktionszahl eingeben.

MANAGER-CODE: (6-stellig) verwaltet Benutzer, Funktionen 0,1,2,3,7 und 9.
Eingabe-Programmierung: Code eingeben und letzte Zahl gedrückt halten bis LED an bleibt, dann Funktionszahl eingeben. Bei Funktion 1,2 + 3 Benutzer-stelle eingeben 2. oder 3.
Bei Doppelcode-Betrieb wird der Manager-Code als zweite-Code eingegeben.
Eingabe Öffnung: Bei Doppelcode-Betrieb als 1. Code eingeben. Bei Einzel-code-Betrieb keine Öffnung.
Überfallalarm auslösen: letzte Code-Zahl +1 oder -1 eingeben.
BENUTZER-CODE: (6-stellig) kann öffnen und Code ändern. (Funktion „0“).
Eingabe Öffnung: Code eingeben. Um Überfallalarm auszulösen, letzte Zahl +1 oder -1 eingeben.
Eingabe Code ändern: Code eingeben und letzte Zahl gedrückt halten bis LED an bleibt, Funktion „0“ drücken und neuen Code 2 x eingeben.

c) Schloss SET-UP (System A) Die Konfiguration des Schlosses erfolgt per PC mit dem Programm „BR 11 SETUP“ per Interface-Kabel an der Tastatur.
Konfiguration: Mastercode, Managercode und 2 Benutzercodes
Doppelcode-Betrieb
Überfallalarm und Öffnungsverzögerung zuschaltbar.
Die Grundprogramme sind nicht ohne Reset auf Factory-Mode änderbar!

a) **PC-SETUP:** Im PC der Zentrale wird das Programm BR11 CRYPTO geladen und aufgerufen. „Initialize Database“ OK anklicken.

PC-Bediener: Der PC-„Master“ kann PC-Manager und PC-Bediener zulassen und jedem verschiedene Operationsfelder zuweisen.

Operationsfelder:

Access a Lock	=	Öffnungscode abfragen
Acknowlege Operations	=	Öffnung bestätigen (positiv/negativ)
Special Commands	=	Schlossaktivierung, Deaktivierung, Zeitsynchronisation, Codesynchronisation
Locks Management	=	Schloss zulassen, löschen, Standort-beschreibung
User Management	=	Schloss-Benutzer zulassen/löschen

Schloss-Benutzer: Neben persönlichen Kenndaten zur Verifikation wird ein PIN (Password) 4-stellig eingegeben, das bei der Öffnung verwendet wird.

Schloss-Datei: Jedes Schloss wird mit Kennnummer (SN-Nr.) und Ort eingegeben.

b) **Schloss-Aktivierung**: Die Zuschaltung des CRYPTO-System (B) im Schloss erfolgt mit dem 8-stelligen Master-/Kontroll-Code der Funktion „6“ und einem im PC generierten Aktivierungscode (12-stellig).
„0“ gedrückt ha lten bis zum nochmaligen Doppelsignal, Master-/Kontroll-Code eingeben und letzte Zahl gedrückt halten bis LED an bleibt.
„6“ drücken und 12-stelligen Aktivierungscode eingeben (Doppelsignal).
Rückmeldung: „Pos. Ack“
Das Schloss arbeitet jetzt zusätzlich mit dem CRYPTO-SYSTEM und ist mit dem PC synchronisiert.

c) **PC-Bedienung**: Der PC-Bediener ruft einen Schloss-Benutzer und das entsprechende Schloss auf, klickt „OPEN“ an und erhält einen 7-stelligen Einmal-Code, der nur für das spezifizierte Schloss und den bestimmten Benutzer gilt und ca. 15 Minuten gültig ist.

d) **Öffnung:** Schloss-Benutzer an der Schloss-Tastatur: „1“ gedrückt halten bis zum nochmaligen Doppelton (CRYPTO-Code-Erkennung) 4-stelligen PIN des Benutzers und 7-stelligen Einmal-Code eingeben (Doppelsignal) und öffnen.

e) **Rückmeldung:** Öffnung oder Nichtöffnung an Zentrale melden. PC-Bediener klickt bei Öffnun g „Pos. Acknowledge“ oder „Neg. Ack“ bei Nichtöffnung an. (Das dient dem Parallel-Lauf des Algorithmus im Schloss und PC).

Das Schloss speichert die letzten 511 Vorgänge mit Datum, Zeit und Benutzer.
Nur Master-/Kontroller und der Manager haben Zugriff zum Schloss-Protokoll.
Der Protokollspeicher ist nicht löschbar. Stromunterbrechungen, länger als 5 Minuten, verfälschen oder löschen die registrierte Uhrzeit (letzte Spalte „?“ anstatt „OK“).
Die Reiehnfolge der Aktionen bleibt erhalten.

A) Schloss-Protokoll: Das Auslesen erfolgt im PC mit dem Programm „LG-View“.

1. Vorbereitung am PC: „LG-View laden und aufrufen. In der Kopfzeile „CONFIGURATION“ aufrufen und serial Port COM für das Interface festlegen. (1200 baud, non parity, 1 stop-bit). Ferner „Daylight saving time“ auswählen und anklicken, und Sommer-/ Winterzeit (DST-activ) aktivieren und Schaltzeiten anklicken (letzter Sonntag Mrz/Okt.).

   Safe-Symbol (start aquisition) anklicken. Der PC ist jetzt für das Auslesen vorbereitet. (Als nächste Option erscheint STOP (rot) und „QUIT“)

2. Auslesen: Interface-Stecker in den Leseschlitz an der Schloss-Tastatur stecken. Kontroll- oder Manager-Code eingeben, letzte Zahl gedrückt halten bis LED an bleibt, Funktion „7“ drücken. Die Datenübertragung beginnt und endet, wenn die LED ausgeht. Zum vorzeitigen Abbruch „STOP“ anklicken oder eine Zahl an der Schloss-Tastatur drücken.
   Im Display erscheint die Auflistung, zeitlich rückwärts.
   Öffnungen mit CRYPTO-CODE werden als Benutzer Nr. 9 protokolliert.

3. Filterfunktion: Es kann eine Auswahl nach Vorgängen, Benutzer oder Datum getroffen werden, indem ein Kriterium ausgewählt und durch rechten Mausklick ausgefiltert wird (erscheint in rot).

4. Speichern: Das Protokoll kann gespeichert werden, indem „SAVE“ angeklickt und eine Ablage (File) gewählt wird. Der Abruf erfolgt durch „LOAD“.

5. Status: Durch Anklicken „INFO“ erscheint der Schloss-Status mit SN# und Softwareversion, eingestellten Programmen, Benutzerstatus. (Kenn-Buchstaben:
   E=aktiv, B=blockiert, D=gesperrt, I=initialisiert (nicht aktiv), – Benutzerstelle frei
   1. Stelle = Master-/Kontrollcode, 2. Stelle = Manager, 3. + 4. Stelle = Benutzer 2 + 3.)

B) PC-Protokolle: Im PC der Zentrale werden alle Daten des CRYPTO-Systems gespeichert. Es stehen folgende Listen dem PC-Master und PC-Manager zur Verfügung und können gedruckt werden:

1.	PC-Bediener:	Liste aller PC-Bediener mit Status (mit „quick search“ alphabetisch)
2.	Bediener-Log:	Liste des ausgewählten PC-Bedieners mit Betriebszeit und Funktionen (Bedienerliste „LOG“ anklicken). Liste aller PC-Bediener erscheint, wenn Filterfunktion ausgeschaltet wird.
3.	Schloss-Benutzer:	Liste aller Schloss-Benutzer mit ID# (PIN nicht sichtbar)
4.	Benutzer-Log:	Liste des ausgewählten Benutzers mit Datum, Zeit Funktion, Schloss # und PC-Bediener. Liste aller Benutzer, Filter abschalten. Diese Liste wird als Tages-Logbuch verwendet und enthält alle Angaben.
5.	Schlossliste:	Aufstellung aller Schlösser mit SN# und Standort und Status.
6.	Schloss-Log:	Liste der Schlossvorgänge mit PC-Bediener, Benutzer, Schloss#, Vorgang, Datum, Zeit (Schlossliste „LOG“ anklicken).
7.	Ausdrucken:	In der jeweiligen Liste „Print“ auklicken.

MASTER-/KONTROLL-CODE

A) Abschaltung „System A“

1. Crypto-System deaktivieren: Am Schloss Master-/Kontroll-Code, Funktion „6“ und PC generierten Deaktivierungs-Code eingeben (Doppelsignal) und „Positiv“ der Zentrale melden (Pos. Ack anklicken).

2. Software-Reset am Schloss: Master-/Kontroll-Code, Funktion „8“ und Manager-Code eingeben (1 langes Signal). Der Master-/Kontroll-Code ist auf 8 x „5“ gesetzt, alle Codes und Programme sind gelöscht. Das Protokoll ist nicht gelöscht.

3. Factory-Mode: Nach dem Reset ist das Schloss im Factory-Mode. „1“ öffnet und sendet Alarm.

4. Programmierung manuell (anstelle des PC-SETUP). Solange der Master-/Kontroll-Code nicht umgestellt wird, kann dieser Manager- und 2 Benutzer-Codes zulassen (Funktion „1“ und Benutzerstelle), zeitweilig sperren (Funktion „2“ und Benutzerstelle) oder löschen (Funktion „3“ und Benutzerstelle) und die Programme wählen (Funktion „8“ und Programm-Nr.- siehe unten B3). Jeder Programmschnitt wird einzeln vorgenommen.

5. Abschaltung: Master-/Kontroll-Code lässt nur den Manager zu (kann nicht öffnen): „0“ gedrückt halten bis nochmaliges Doppelsignal, 8 x „5“ eingeben und letzte Zahl gedrückt halten bis LED an bleibt, Funktion „1“ und Stelle für Manager „1“ eingeben und 2 x 6-stelligen Manager-Code eingeben.
   Master-/Kontroll-Code ändern mit Funktion „0“ und 2 x neuen 8-stelligen Code eingeben. Die Konfiguration ist durch Code-Änderung „eingefroren“ Da kein Öffnungscode programmiert wurde, ist System A ausgeschaltet.

6. CRYPTO-System aktivieren: Der umgestellte Master-/Kontroll-Code aktiviert mit Funktion „6“ und dem PC-generierten Aktivierungscode (12-stellig) das CRYPTO-System und gibt die Ausführung an die PC-Zentrale durch, die „Pos. Ack“ anklickt. Das Schloss ist im CRYPTO-System synchronisiert und arbeitsfähig.

B) Zuschaltung „System A“

1. CRYPTO-System deaktivieren: - siehe oben A1-

2. Software-Reset am Schloss mit Master-/Kontroll-Code, „8“ und Manager-Code - siehe oben A2-

3. Managercode und Benutzercodes zulassen – siehe oben A4–
   Programm mit Master-/Kontroll-Code 8 x „5“: Funktion „8“ und Programmversion festlegen:

Einzelcode-Betrieb (Benutzer 2 + 3 öffnen einzeln)	„0“
Doppelcode-Betrieb	„2“
Einzelcode-Betrieb mit Alarm	„4“
Doppeldode-Betrieb mit Alarm	„6“

   „0“ gedrückt halten bis nochmaliges Doppelsignal, 8 x „5“ eingeben und letzte Zahl gedrückt halten bis LED an bleibt, Funktion „8“ und Programm-Nr. z.B. „4“ eingeben und bestätigen (noch einmal „4“ eingeben).
   Nach Änderung des Master-/Kontroll-Codes kann der Manager einen gelöschten Benutzer nur durch erneuten Reset wieder zulassen. Im Doppelcode-Betrieb kann der Benutzer-Code, der vor dem Manager-Code eingegeben wurde, nicht gesperrt oder gelöscht werden.

C) Hardware-Reset

Falls der Master-/Kontrollcode und/oder der Manager-Code nicht bekannt ist, muss ein Hardware-Reset erfolgen. Bei geöffneter Tür wird eine RESET-BOX an den BAT-Anschluss des Schlosses gesteckt. Das Schloss ist dann ebenfalls im Factory-Mode und kann manuell oder per PC-SETUP programmiert werden (Anleitung auf der RESET-Box beachten).