



CLAVIS Deutschland GmbH  
Grüner Weg 38  
34117 Kassel

Telefon: +49 (0)561 988 499-0  
E-Mail: info@tresore.eu  
Internet: www.tresore.eu  
www.tresorschloss.de

**INSYS**  
MICROELECTRONICS  
*Security*

# TwinLock 7220 / 7260 BioPIN

## Basis- und Komfortsysteme

### Handbuch



DIN EN 1300

M 109319 Hochsicherheitsschloss – Klasse 3 (TwinLock 7220 BioPIN)

M 109317 Hochsicherheitsschloss – Klasse 2 (TwinLock 7260 BioPIN)

G 108061 Überfallmelder – Klasse C

G 108062 Überfallmelder – Klasse C

G 106016 / G 106015 Sperreinrichtung - Klasse C

G 105133 / G 102013 Schalteinrichtung - Klasse C

## Impressum

Copyright © März 2010 INSYS MICROELECTRONICS GmbH  
Jede Vervielfältigung dieses Handbuchs ist nicht erlaubt. Für Kritik und Anregungen sind wir jederzeit dankbar. Alle Rechte an dieser Dokumentation und an den Geräten liegen bei INSYS MICROELECTRONICS GmbH Regensburg.

### *Warenzeichen und Firmenzeichen*

Die Verwendung eines hier nicht aufgeführten Waren- oder Firmenzeichens ist kein Hinweis auf die freie Verwendbarkeit desselben.

INSYS® ist ein eingetragenes Warenzeichen der INSYS MICROELECTRONICS GmbH.

Windows™ ist ein Warenzeichen von Microsoft Corporation.

### *Herausgeber*

INSYS MICROELECTRONICS GmbH  
Waffnergasse 8  
93047 Regensburg, Deutschland



### **Kundendienst**

CLAVIS Deutschland GmbH  
Grüner Weg 38  
34117 Kassel

Telefon: +49 (0)561 988 499-0

E-Mail: [info@tresore.eu](mailto:info@tresore.eu)

Internet: [www.tresore.eu](http://www.tresore.eu)  
[www.tresorschloss.de](http://www.tresorschloss.de)

# Inhaltsverzeichnis

<b>1</b>	<b>Zu dieser Dokumentation .....</b>	<b>6</b>
<b>1.1</b>	<b>Inhalte und Nutzung .....</b>	<b>6</b>
<b>1.2</b>	<b>Benutzerqualifikation .....</b>	<b>6</b>
<b>1.3</b>	<b>Textauszeichnungen und Formatierung .....</b>	<b>7</b>
1.3.1	Sicherheitshinweise.....	7
1.3.2	Symbolbedeutungen .....	7
1.3.3	Handlungsanweisungen.....	8
<b>2</b>	<b>Systembeschreibung.....</b>	<b>9</b>
<b>2.1</b>	<b>System .....</b>	<b>9</b>
2.1.1	Systemaufbau .....	10
2.1.2	Systemkomponenten .....	17
2.1.2.1	Bedieneinheit FlatControl BioPIN.....	17
2.1.2.2	Schloss TwinLock .....	17
2.1.2.3	Busverteiler TwinConnect.....	17
2.1.2.4	Sperreinrichtung TwinXT .....	18
2.1.2.5	Schalteinrichtung TwinAlarm .....	18
2.1.2.6	Optionales Zubehör: Chipkarten TwinCard.....	19
2.1.3	Übersicht: Codes im System .....	20
<b>2.2</b>	<b>Funktionsübersicht.....</b>	<b>21</b>
2.2.1	Allgemeine Funktionen.....	21
2.2.2	Mit Software TwinComm einstellbare Funktionen .....	23
<b>2.3</b>	<b>Bestimmungsgemäßer Gebrauch.....</b>	<b>23</b>
<b>3</b>	<b>Bedienung.....</b>	<b>23</b>
<b>3.1</b>	<b>Allgemein .....</b>	<b>23</b>
3.1.1	Der Systemzustand .....	23
<b>3.2</b>	<b>Bedienung mit optionaler Software TwinComm .....</b>	<b>23</b>
<b>3.3</b>	<b>Benutzer autorisieren.....</b>	<b>23</b>
3.3.1	Kontrollkästchen der Benutzermatrix.....	23
<b>3.4</b>	<b>Menüführung in Bedieneinheit FlatControl .....</b>	<b>23</b>
<b>3.5</b>	<b>PIN-Codes .....</b>	<b>23</b>
3.5.1	Arten und Anzahl von PIN-Codes in jedem Schloss .....	23
3.5.2	PIN-Code eingeben.....	23
<b>3.6</b>	<b>Codekarten .....</b>	<b>23</b>
3.6.1	Codekarte TwinCard code access .....	23
3.6.2	Chipkarte in Bedieneinheit einlegen .....	23
<b>3.7</b>	<b>Fingerprint-Codes.....</b>	<b>23</b>
<b>3.8</b>	<b>Bedienung bei aktivierter WTU-Funktion .....</b>	<b>23</b>
<b>3.9</b>	<b>Öffnen und Schließen.....</b>	<b>23</b>
3.9.1	Schloss mit PIN-Code öffnen .....	23
3.9.2	Schloss mit Codekarte öffnen .....	23
3.9.3	Vor dem Öffnen Fingerprint-Code eingeben.....	23
3.9.4	Beim Öffnen Stillen Alarm auslösen.....	23

3.9.5	Schloss mit Codeverknüpfung öffnen.....	23
3.9.6	Schloss mit Öffnungszeitverzögerung öffnen .....	23
3.9.7	Mit Öffnungszeitverzögerung / Freigabezeit öffnen ....	23
3.9.8	Schlösser mit Parallelcode öffnen .....	23
3.9.9	Einbruchmeldeanlage (EMA) unscharf schalten .....	23
3.9.10	Schloss schließen.....	23
3.9.11	Schloss mit Code-Eingabe schließen .....	23
3.9.12	Schloss mit Türschalter automatisch schließen .....	23
3.9.13	Einbruchmeldeanlage (EMA) scharf schalten .....	23
<b>3.10</b>	<b>System einrichten.....</b>	<b>23</b>
3.10.1	Datum und Uhrzeit einstellen.....	23
3.10.2	TwinXT / TwinAlarm ein- / ausschalten .....	23
3.10.3	WTU-Funktion aktivieren .....	23
3.10.4	Protokoll exportieren (TwinComm) .....	23
3.10.5	Protokoll anzeigen / drucken (TwinComm) .....	23
3.10.6	Konfiguration importieren.....	23
3.10.7	Meldungen beim Import der Konfiguration.....	23
3.10.8	Konfiguration exportieren (TwinComm).....	23
3.10.9	Sprache wählen.....	23
3.10.10	Sprache importieren .....	23
<b>3.11</b>	<b>Benutzer verwalten .....</b>	<b>23</b>
3.11.1	Systemmanagercode ändern.....	23
3.11.2	Mastercode / WTU-Mastercode ändern .....	23
3.11.3	PIN-Code für Benutzer anmelden.....	23
3.11.4	PIN-Code ändern.....	23
3.11.5	PIN-Code abmelden .....	23
3.11.6	PIN-Code Benutzer-Anzeige.....	23
3.11.7	Codekarte anmelden .....	23
3.11.8	Codekarte abmelden .....	23
3.11.9	Codekarte Benutzer-Anzeige .....	23
3.11.10	Fingerprint: Überblick.....	23
3.11.11	Fingerprint-Scan testen .....	23
3.11.12	Fingerprint: Min. Minuten festlegen .....	23
3.11.13	Fingerprint: Schwellwert für Bildqualität festlegen.....	23
3.11.14	Fingerprint: Sicherheitsstufe festlegen .....	23
3.11.15	Fingerprint-Code anmelden.....	23
3.11.16	Fingerprint-Code abmelden.....	23
3.11.17	Fingerprint: Benutzer-Anzeige .....	23
<b>3.12</b>	<b>Service .....</b>	<b>23</b>
3.12.1	System bei Netzausfall mit Spannung versorgen .....	23
3.12.2	Status / Info des Systems anzeigen .....	23
3.12.3	Service Reset .....	23
3.12.4	Motor-Service .....	23
3.12.5	Schloss anmelden.....	23
3.12.5.1	Schloss neu .....	23
3.12.5.2	Schloss wechseln.....	23
3.12.6	System bei defektem Riegelwerkskontakt schließen....	23
3.12.7	Fingerprint Status / Info .....	23
3.12.8	Fingerprint: Temperatur anzeigen / ändern.....	23
<b>4</b>	<b>Reinigung.....</b>	<b>23</b>

<b>5</b>	<b>Störungsabhilfe .....</b>	<b>23</b>
	5.1 Fehlermeldungen .....	23
<b>6</b>	<b>Technische Unterstützung .....</b>	<b>23</b>
<b>7</b>	<b>Entsorgung.....</b>	<b>23</b>
<b>8</b>	<b>Glossar .....</b>	<b>23</b>
<b>9</b>	<b>Anhang.....</b>	<b>23</b>
	9.1 Stichwortverzeichnis .....	23
	9.2 Abbildungsverzeichnis .....	23
	9.3 Änderungshistorie des Dokuments .....	23
	9.4 Notizen .....	23

# 1 Zu dieser Dokumentation

## 1.1 Inhalte und Nutzung

Dieses Handbuch enthält Informationen zu Betrieb, Konfiguration und Pflege des Hochsicherheitsschlosssystems TwinLock 7220 / 7260 BioPIN und soll Sie im Umgang mit ihm unterstützen. Es beschreibt die Bedienvorgänge für System TwinLock BioPIN der VdS-Klasse 2 (TwinLock 7260 BioPIN) und der VdS-Klasse 3 (TwinLock 7220 BioPIN) und bietet Informationen zu den Einstellungen. VdS Schadenverhütung GmbH ist ein Institut der deutschen Versicherungswirtschaft, das unter anderem Produkte der Sicherheitstechnik evaluiert.

Informationen zur Montage und Inbetriebnahme von TwinLock BioPIN finden Sie in der Montageanleitung des Systems.

Anleitungen zu Öffnungs- und Schließvorgängen enthält die Kurzbedienungsanleitung.

## 1.2 Benutzerqualifikation

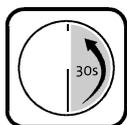
Dieses Handbuch richtet sich vor allem an qualifizierte und geschulte Fachkräfte. Einrichter und Verwalter des Systems TwinLock BioPIN müssen fähig und auch sprachlich in der Lage sein, dieses Handbuch zu lesen und zu verstehen, um sich mit den Einrichtungs-, Verwaltungs- und Bedienvorgängen vertraut machen, das System richtig konfigurieren sowie Störungen beheben und so den sicheren Betrieb von TwinLock BioPIN gewährleisten zu können.

## 1.3 Textauszeichnungen und Formatierung

### 1.3.1 Sicherheitshinweise

	<b>Gefahr</b>
	<b>Unmittelbare Lebensgefahr / Gefahr der schweren Körperverschädigung und von Gesundheitsschäden. Folgen, die sich aus der Missachtung ergeben können.</b> Anleitung zur Vermeidung oder Behebung der Gefahr
	<b>Warnung</b>
	<b>Mittelbare Lebensgefahr / Gefahr der schweren Körperverschädigung und von Gesundheitsschäden. Folgen, die sich aus der Missachtung ergeben können.</b> Anleitung zur Vermeidung oder Behebung der Gefahr
	<b>Vorsicht</b>
	<b>Verletzungsgefahr. Folgen, die sich aus der Missachtung ergeben können</b> Anleitung zur Vermeidung oder Behebung der Gefahr
	<b>Vorsicht</b>
	<b>Gefahr eines Sachschadens</b> <b>Folgen, die sich aus der Missachtung ergeben können</b> Anleitung zur Vermeidung oder Behebung der Gefahr
	<b>Hinweis</b>
	Keine Gefahrenmeldung, sondern Zusatzinformation. Hintergrundinformation / Tipps.

### 1.3.2 Symbolbedeutungen



Benutzen Sie Eingabeeinheit FlatControl.  
Nach 30 Sekunden ohne Eingabe begibt sich diese in den Ruhezustand.



Für die folgenden Schritte benötigen Sie Werkzeug.



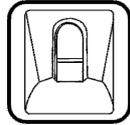
Für die folgenden Schritte benötigen Sie einen PIN-Code für Benutzer.



Für die folgenden Schritte benötigen Sie einen Mastercode.



Für die folgenden Schritte benötigen Sie den Systemmanagercode (Managercode des ersten Schlosses) oder einen anderen Managercode.



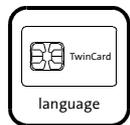
Die folgenden Schritte können nur von einem (auch) durch Fingerabdruck (Fingerprint) identifizierbaren Benutzer ausgeführt werden.



Für die folgenden Schritte benötigen Sie eine optionale Chipkarte TwinCard code access.



Für die folgenden Schritte benötigen Sie eine optionale Chipkarte TwinCard configuration II.



Für die folgenden Schritte benötigen Sie eine optionale Chipkarte TwinCard language.



Symbole für ungesicherten / gesicherten Bereich in Abbildungen.

### 1.3.3 Handlungsanweisungen

Text ohne besondere Formatierung gleich nach der Überschrift einer Handlungsanweisung enthält nicht sicherheitsrelevante Hinweise auf Umstände, die bei der Ausführung der Handlung zu beachten sind.

**Sie benötigen** Text, dem 'Sie benötigen' vorangestellt ist, enthält Hinweise zu Werkzeugen oder anderen Mitteln, die Sie für die erfolgreiche Durchführung der Handlungsschritte benötigen. Achten Sie auch auf die abgebildeten Symbole.

**Vorbedingung** Text, dem 'Vorbedingung(en)' vorangestellt ist, enthält Bedingungen, die erfüllt sein müssen, bevor Sie die Handlungsschritte ausführen können.

1. So formatierter Text fordert Sie auf, etwas zu tun. Er kann die Namen von Tasten und Menüpunkten enthalten.  
*So formatierter Text enthält Resultate, die die Folge davon sind, dass Sie einen Handlungsschritt ausgeführt haben.*

So formatierter Text am Ende einer Handlungsanweisung zeigt Ihnen, dass Sie das Ziel Ihrer Handlung erreicht haben.

## 2 Systembeschreibung

### 2.1 System

TwinLock BioPIN ist ein modular aufgebautes elektronisches Hochsicherheitsschlosssystem, bei denen die sicherheitsrelevanten Systemkomponenten voll redundant ausgeführt sind.

Sein Einsatzgebiet ist die Verwaltung, Steuerung und Ausführung von Öffnungs- und Schließvorgängen vor allem von Türen von Geldschränken im Bankenbereich.

Durch den Einsatz von TwinLock BioPIN wird die Sicherheit des Inhalts von Wertbehältnissen gewährleistet.

Befugte Personen können die Wertbehältnisse im täglichen Betrieb gemäß definierbaren Regeln öffnen und schließen. Das System kann zwei Benutzerkreise jeweils eigenständig verwalten, beispielsweise Personal einer Bank und Personal eines Werttransportunternehmens.

Es gibt die Systemvarianten:

Basissystem 1.1, 2.1 und 3.2 (mit TwinXT)  
Komfortsystem 1 und 2 (mit TwinAlarm)

Die erste Ziffer hinter der Systembezeichnung gibt die Zahl der Schlösser im System an, die zweite Ziffer die Zahl der Sperreinrichtungen TwinXT, die es nur in Basissystemen gibt.

Beispiele:

Basissystem 2.1 enthält 2 Schlösser und 1 Sperreinrichtung TwinXT.  
Komfortsystem 1 enthält 1 Schloss und 1 Schalteinrichtung TwinAlarm.

Jedes Basis- oder Komfortsystem enthält eine Bedieneinheit FlatControl BioPIN, mindestens ein Schloss TwinLock und einen Busverteiler TwinConnect, der die Komponenten verbindet. Alle Systeme enthalten außerdem ein Bedienungsanleitungsset.

Komfortsysteme enthalten 1 Schalteinrichtung TwinAlarm.

Basissysteme enthalten bis zu 2 Sperreinrichtungen TwinXT.

### 2.1.1 Systemaufbau

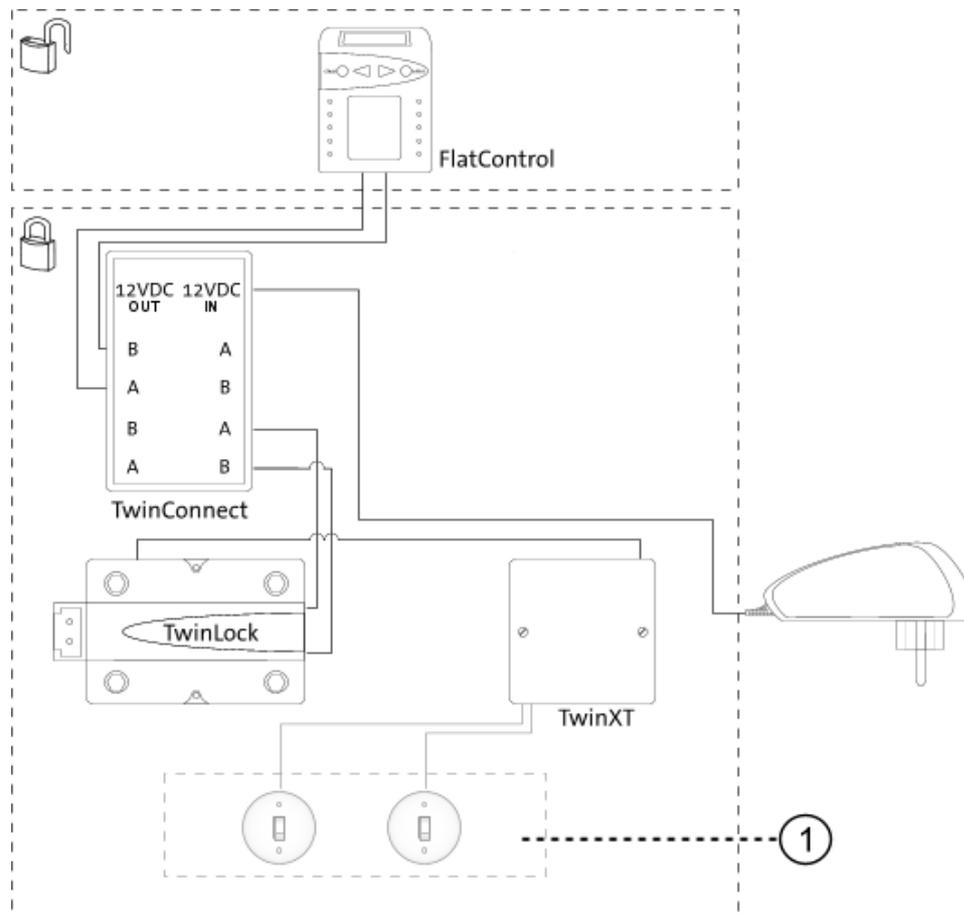


Abbildung 1 Systemaufbau von Basissystem 1.1

- 1) Zustandsanzeige, Stiller Alarm, Riegelwerksschalter und Schalter für die Freigabe für das Schloss TwinLock

Das Basissystem 1.1 besteht aus einer Bedieneinheit FlatControl und einem Netzteil im ungesicherten Bereich und einem Schloss TwinLock, einem Busverteiler TwinConnect und der Erweiterungseinheit TwinXT im gesicherten Bereich.

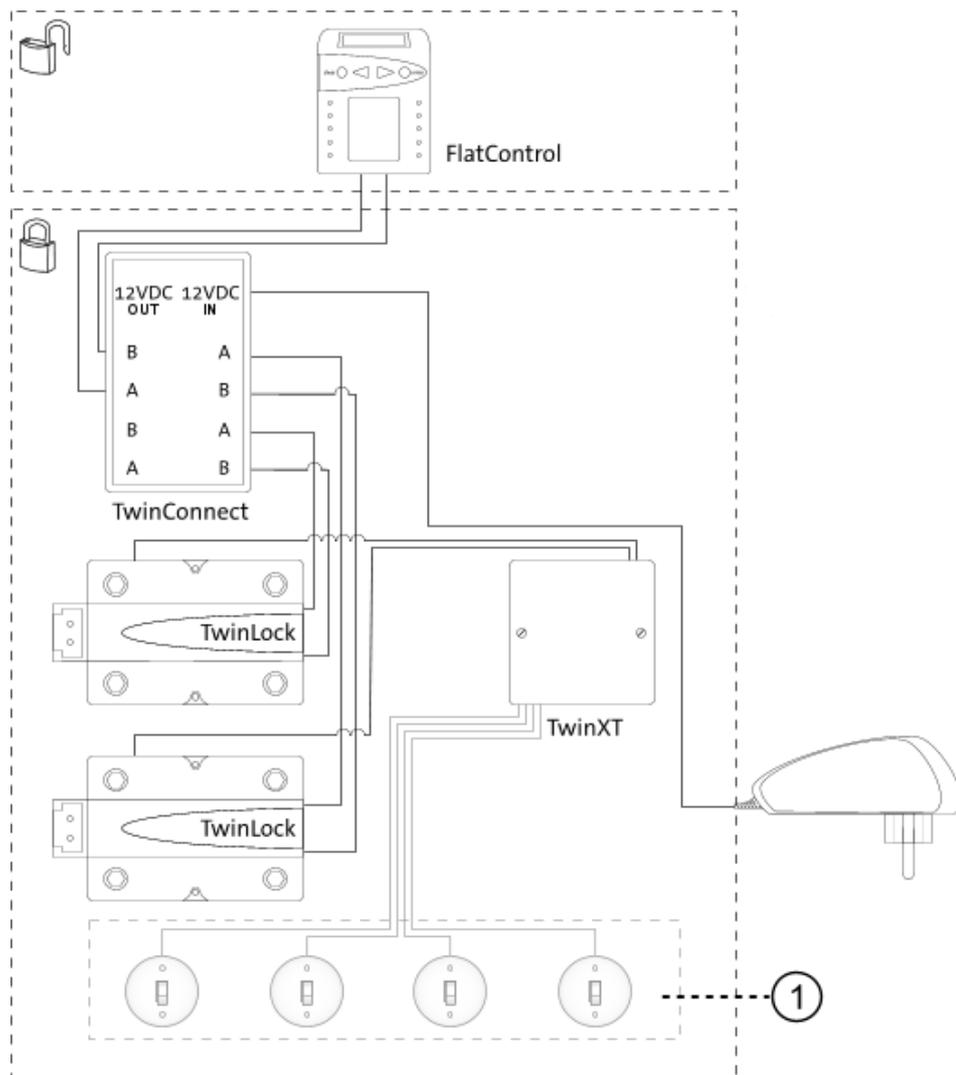


Abbildung 2 Systemaufbau von Basissystem 2.1

- 1) Zustandsanzeige, Stiller Alarm, Riegelwerksschalter und Schalter für die Freigabe der Schlösser TwinLock

Das Basissystem 2.1 besteht aus einer Bedieneinheit FlatControl und aus einem Netzteil im ungesicherten Bereich, und aus zwei Schlössern TwinLock, einem Busverteiler TwinConnect und einer Erweiterungseinheit TwinXT im gesicherten Bereich.



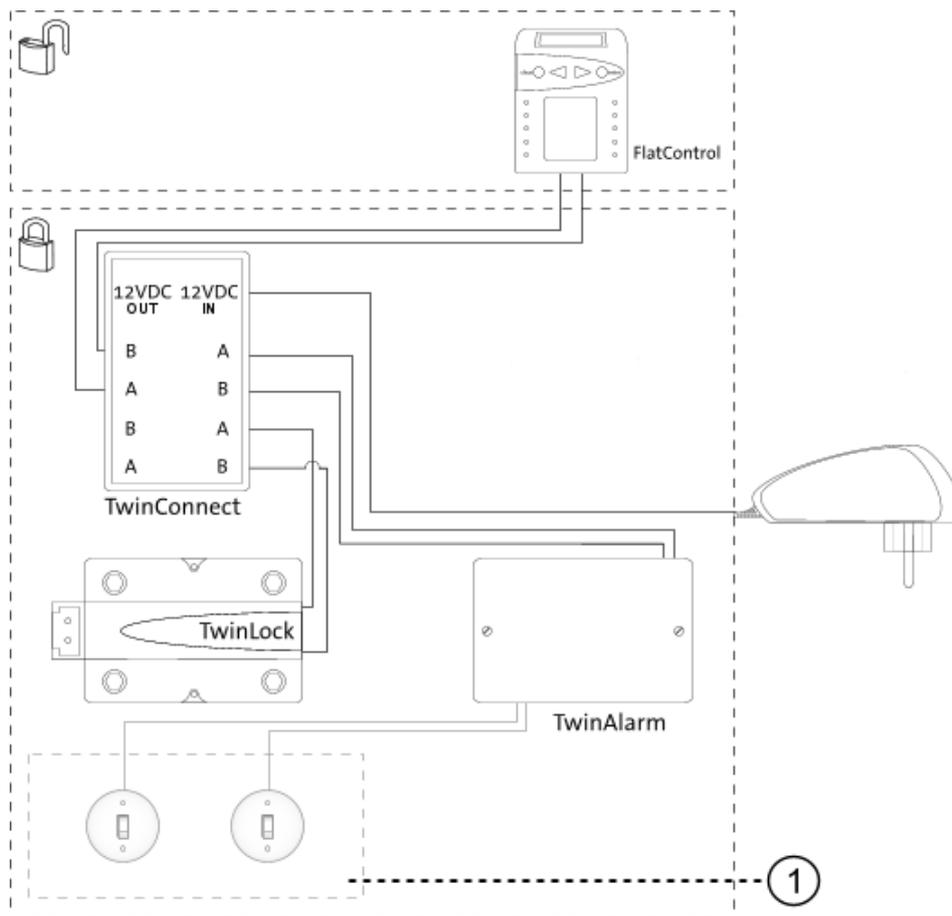


Abbildung 4 Systemaufbau von Komfortsystem 1 ohne EMA

- 1) Zustandsanzeige, Stiller Alarm, Riegelwerkszentralschalter und Schalter für die Zeitprogramm Sperre für das Schloss TwinLock

Das Komfortsystem 1 besteht aus einer Bedieneinheit FlatControl und aus einem Netzteil im ungesicherten Bereich, einem Schloss TwinLock, einem Busverteiler TwinConnect und der Schalteinrichtung TwinAlarm im gesicherten Bereich.

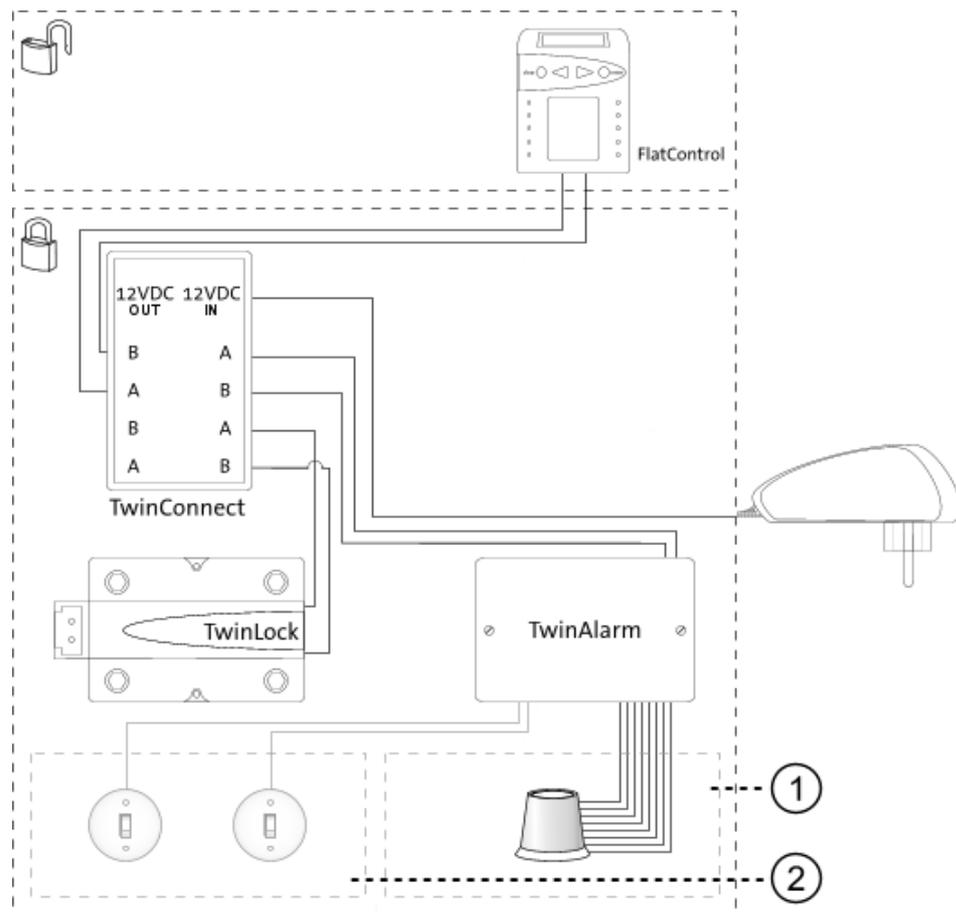


Abbildung 5 Systemaufbau von Komfortsystem 1 mit EMA

- 1) Einbruchmeldeanlage (EMA) mit Eingängen (Alarmkontakt, Zustandskontakt, Scharfschaltung) aus Richtung der Schalteinrichtung TwinAlarm und Ausgängen (EMA-Bereit, Unscharf-Sperre, Quittierung, Freigabe-Sperre, Spannungsversorgung) zur Schalteinrichtung TwinAlarm
- 2) Zustandsanzeige, Stiller Alarm, Riegelwerkszentralschalter und Schalter für die Zeitprogramm Sperre für das Schloss TwinLock

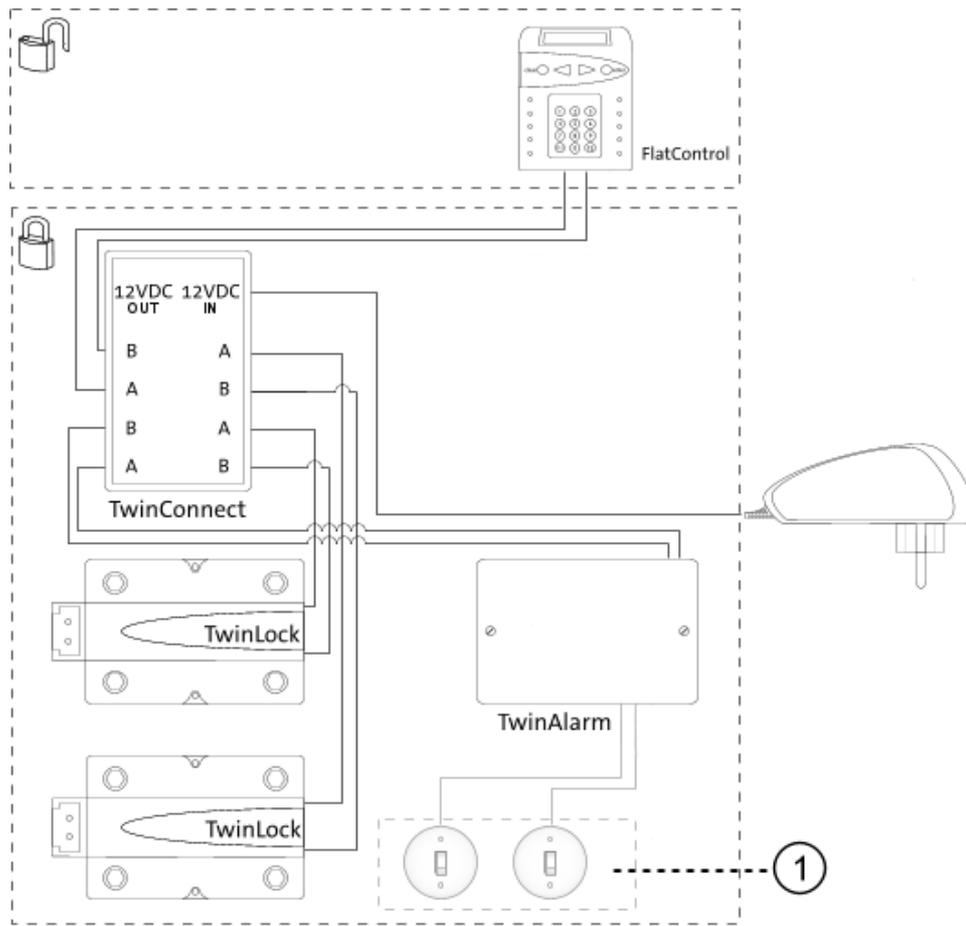


Abbildung 6 Systemaufbau von Komfortsystem 2 ohne EMA

- 1) Zustandsanzeige, Stiller Alarm, Riegelwerkszentralschalter und Schalter für die Zeitprogramm Sperre für die Schlösser TwinLock

Das Komfortsystem 2 enthält zwei Schlösser TwinLock. Alle anderen Komponenten sind die gleichen wie bei Komfortsystem 1.

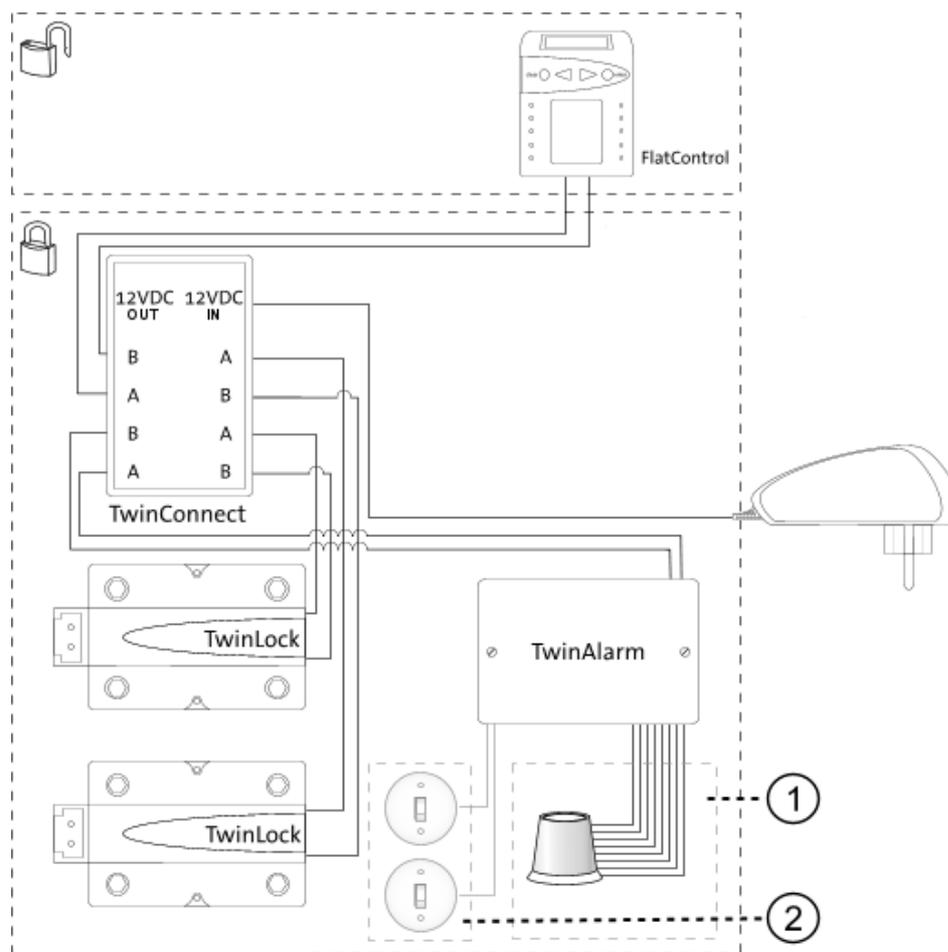


Abbildung 7 Systemaufbau von Komfortsystem 2 mit EMA

- 1) Einbruchmeldeanlage (EMA) mit Eingängen (Alarmkontakt, Zustandskontakt, Scharfschaltung) aus Richtung der Schalteinrichtung TwinAlarm und Ausgängen (EMA-Bereit, Unscharf-Sperre, Quittierung, Freigabe-Sperre, Spannungsversorgung) zur Schalteinrichtung TwinAlarm
- 2) Zustandsanzeige, Stiller Alarm, Riegelwerkszentralschalter und Schalter für die Zeitprogramm Sperre für die Schlösser TwinLock

## 2.1.2 Systemkomponenten

### 2.1.2.1 Bedieneinheit FlatControl BioPIN



Abbildung 8 Bedieneinheit FlatControl BioPIN

Mit der Bedieneinheit FlatControl BioPIN steuern und bedienen Sie das Hochsicherheitsschlosssystem TwinLock. Die Bedieneinheit befindet sich im ungesicherten Bereich des Systems. Eine Beschreibung der einzelnen Bedienelemente siehe in Kapitel 4, Bedienung.

### 2.1.2.2 Schloss TwinLock



Abbildung 9 Schloss TwinLock

Das Schloss TwinLock ver- und entriegelt das Wertbehältnis. Es befindet sich im gesicherten Bereich des Systems. Sie können bis zu 3 Schlösser TwinLock an das System anschließen.

### 2.1.2.3 Busverteiler TwinConnect



Abbildung 10 Busverteiler TwinConnect

Über ein redundantes Bussystem verbindet der Busverteiler TwinConnect die folgenden Komponenten Ihres Systems miteinander - jeweils 1 Eingabeeinheit FlatControl, bis zu 3 Schlösser TwinLock, 1 Netzteil und gegebenenfalls 1-2 Erweiterungseinheiten TwinXT oder 1 Schalteinrichtung TwinAlarm. Der Busverteiler befindet sich im gesicherten Bereich des Systems.

### 2.1.2.4 Sperreinrichtung TwinXT



Abbildung 11 Sperreinrichtung TwinXT

Die Sperreinrichtung TwinXT im gesicherten Bereich des Systems gibt es nur als Erweiterungseinheit für Basissysteme. Mit einer Einheit TwinXT können Sie das System TwinLock um 4 Ein- und 2 Ausgänge erweitern. Dadurch können bis zu zwei Schlösser einzeln gesperrt / freigegeben und mit Riegelwerkskontakt versehen werden. Zusätzlich verfügt TwinXT über einen Zustands- und einen Alarmkontakt für den Stillen Alarm.

### 2.1.2.5 Schalteinrichtung TwinAlarm



Abbildung 12 Schalteinrichtung TwinAlarm

Die optionale Schalteinrichtung TwinAlarm innerhalb des Wertbehältnisses verbindet das System mit einer optionalen Einbruchmeldeanlage (EMA). Sie dient als Verteiler für die Einbruchmeldeanlage (Riegel-, Tür- und andere Kontakte sowie Widerstandsüberwachung). In TwinAlarm werden die elektronischen Schlüssel (Chipkarten) sowie die Eingangssignale der Einbruchmeldeanlage ausgewertet.

### 2.1.2.6 Optionales Zubehör: Chipkarten TwinCard



Abbildung 13 Symbol TwinCard code access

Die Chipkarte **TwinCard code access** ist der gesicherte, mobile Codeträger für die Benutzer des TwinLock Systems. Alternativ kann der Code auch manuell eingegeben werden.

Damit Benutzer ein Schloss mit Chipkarte öffnen können, müssen sie dazu in der Benutzermatrix autorisiert worden sein und die Chipkarte muss am Schloss angemeldet worden sein.

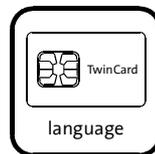


Abbildung 14 Symbol TwinCard language

**TwinCard language** ist eine optionale Chipkarte für die Konfiguration der Systemsprache (DE, EN etc).



Abbildung 15 Symbol TwinCard configuration II

**TwinCard configuration II** ist eine optionale Chipkarte für die Systemkonfiguration und das Ereignisprotokoll. Das Protokoll kann ausgelesen und ausgewertet werden. Mit der optionalen Software TwinComm können Sie das Schlosssystem via Chipkarte komfortabel konfigurieren und die Konfigurationsdaten speichern.

### 2.1.3 Übersicht: Codes im System

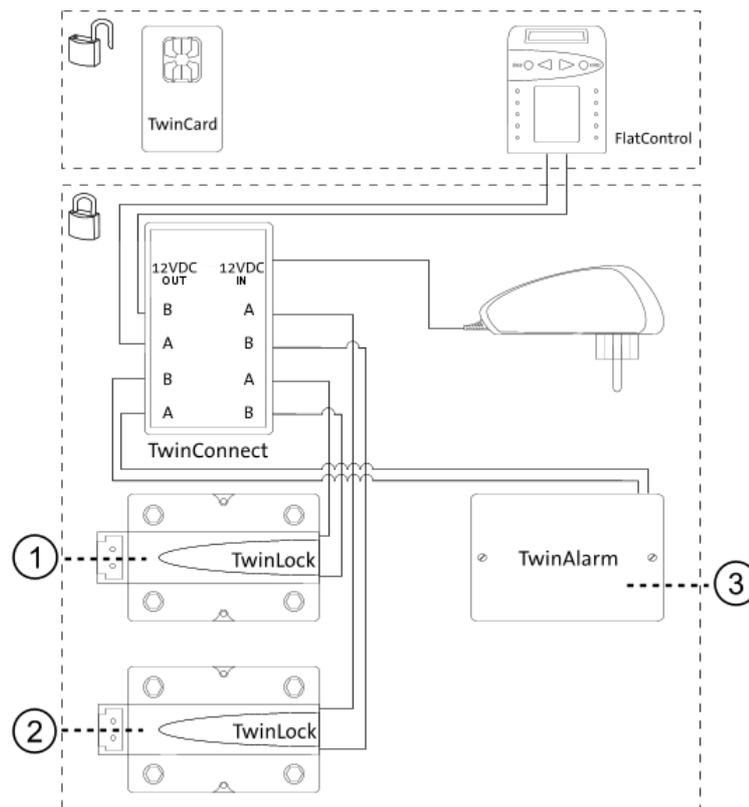


Abbildung 16 Übersicht Codes im System

- 1) **Schloss 1:** Geistige Codes:  
 1 Systemmanagercode (Managercode von Schloss 1)  
 1 Mastercode  
 99 PIN-Codes für Benutzer
- 2) **Schloss 2:** Geistige Codes:  
 1 Mastercode  
 99 PIN-Codes für Benutzer
- 3) **TwinAlarm:** Körperliche Codes:  
 1 Mastercode  
 99 PIN-Codes für Benutzer

Zusätzlich gibt es auf Chipkarten gespeicherte körperliche Codes und verschlüsselte Fingerabdrucksdaten (biometrische Codes).

#### Vorsicht

**Wenn die Benutzercodes bei Systemen mit TwinAlarm vor der Installation / der Aktivierung von TwinAlarm an Schloss 1 angemeldet werden, werden sie nicht in TwinAlarm gespeichert.**

Stellen Sie sicher, dass TwinAlarm installiert und aktiviert ist, bevor Benutzercodes an Schloss 1 angemeldet werden.

## 2.2 Funktionsübersicht

### 2.2.1 Allgemeine Funktionen

Abhängig von Ausführung und Version des Systems TwinLock BioPIN sind alle oder ein Teil der im Folgenden auszugsweise aufgeführten Funktionen vor / nach der Inbetriebnahme fest einstellbar oder mit der Bedieneinheit FlatControl BioPIN auch nachträglich änderbar.

#### Öffnen und Schließen

- Menügeführte Öffnungs- und Schließvorgänge
- Menügeführte Verwaltung und Einrichtung
- Öffnen mit Chipkarte und / oder Codeeingabe und Fingererkennung
- Öffnen mit Parallelcode (2-Schloss-Betrieb) / gemäß 4-Augen-Prinzip
- Automatisches Schließen mit Türschalter
- Schließen mit Chipkarte / Codeeingabe / Fingerprint / ohne Authentifizierung
- Schnellöffnung
- Feste Öffnungs- / Schließreihenfolge wählbar

#### Codeverwaltung

- 1 programmierbarer Systemmanagercode
- 1 programmierbarer Mastercode je Schloss
- 99 programmierbare -Codes für Benutzer je Schloss
- Für 100 Benutzer je 10 Fingerabdrücke pro Schloss speicherbar
- Anzeige Benutzerstatus
- 99 Alarmbenutzer
- Anzeige Alarmbenutzerstatus
- Parallelcode
- Schnellöffnungsberechtigung mit Code
- Programmierbare Zwangsfolge
- Codeverknüpfung (4-Augencode)
- Schutz vor Codemanipulation

#### Zeitfunktionen

- Alarm- / Sabotageverzögerungen
- Stiller Alarm
- Datums- und Uhrzeitanzeige
- Automatische Sommer- / Winterzeitumstellung
- Freigabezeit
- Öffnungsverzögerung
- Sondertage
- Teilsperzeiten
- Wochenprogramme
- Zeitprogrammunterbrechung

**Komfortfunktionen**

- Aktivierbare Displaybeleuchtung
- Ständige Selbstdiagnose
- Spannungsüberwachung

**Servicefunktionen**

- Ereignisprotokoll 3000 Ereignisse
- Im- / Export der Konfiguration per Chipkarte
- Systemsprache wählbar
- Systemstatusanzeige
- Reset der Systemkomponenten
- Versionsabfrage der Systemkomponenten
- Systemkomponenten an- / abmelden
- Motortest im Schrittbetrieb
- Systemzeile frei programmierbar
- Notbestromung bei Spannungsausfall

**TwinAlarm-Funktionen und EMA-Anbindung (optional)**

- Schalteinrichtung TwinAlarm (de-)aktivierbar
- Anschluss an Einbruchmeldeanlage (EMA)
- (Un-)Scharfschaltung der Einbruchmeldeanlage (EMA) manuell oder mit Chipkarte
- Stiller Alarm
- 1 Zustandskontakt (Relais)
- 1 Freigabekontakt (potentialfrei)
- 1 Riegelwerkskontakt (potentialfrei)
- Anschlussmöglichkeit für je 2 weitere Riegelwerks- und Türkontakte
- Erweiterbare Sabotagelinie
- Flächenschutz
- 4 Türkontakte
- Sperrzeit- / Zeitprogrammunterbrechung
- Stützpunkte für Widerstandsüberwachung

## 2.2.2 Mit Software TwinComm USB einstellbare Funktionen

TwinComm USB ist ein nicht im Lieferumfang enthaltenes Parametriereset für das System TwinLock BioPIN. Folgende Funktionen können mit der Software TwinComm USB programmiert werden:

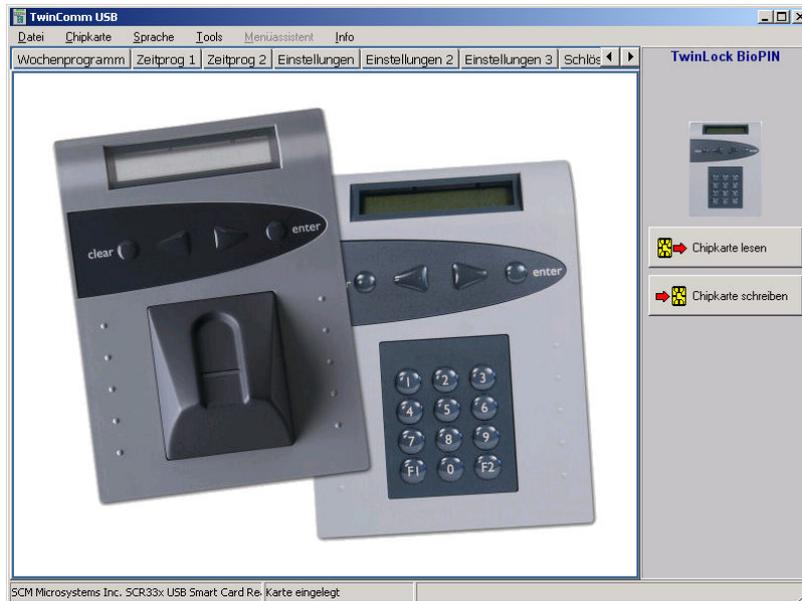


Abbildung 17 PC-Software TwinComm USB (Zubehör)

### Allgemeine Einstellungen

- Automatische Umstellung der Sommer-/Winterzeit (de-)aktivierbar
- Einstellung der Batteriewarngrenze (optional)
- Auswertung des Ereignisprotokolls
- Programmierung der 16-stelligen Systemzeile

### Öffnen und Schließen

- Codeverknüpfung gemäß 4-Augen-Prinzip ein- / ausschalten
- Parallelcode (de-)aktivierbar
- Berechtigung, Schloss trotz Zeitprogramm zu öffnen, für ausgewählte Benutzer einstellbar
- Zwangsfolge ein- / ausschalten
- Manuelles Schließen mit Codeabfrage ein- / ausschalten
- Automatisches Schließen mit Türschalter ein- / ausschalten
- Stiller Alarm, auch mit Öffnungsverzögerung ein- / ausschalten
- Codealterung einstellbar
- Türöffnungsüberwachung
- Öffnungsintervall Schloss 1 – Schloss 2 einstellbar
- Scharf- / Unscharfschalten einer Einbruchmeldeanlage (EMA)

### Zeitprogramme

- Öffnungsverzögerung einstellbar (0-99Min.)
- Freigabezeit einstellbar (0-99Min.)
- 5 Wochenprogramme für jeden Wochentag
- Sondertageprogramm
- 3 Teilsperzeiten pro Wochentag
- 3 Sperr- / Öffnungszeiten

### Verwaltungsfunktionen

- komfortable Systemkonfiguration
- Sperreinrichtung TwinXT (de-)aktivierbar
- Schalteneinrichtung TwinAlarm (de-)aktivierbar
- EMA-Scharfschaltungsbenutzer festlegbar
- Übersicht aller Parameter
- Protokollanzeige
- Kundendatenanzeige
- Benutzermatrix mit individuellen Autorisierungen einstellbar
- zusätzlicher WTU-Benutzerbereich mit eigener Verwaltung
- allgemeine / individuelle Mindestanforderungen Fingerprint
- Anzeige einer Servicetelefonnummer bei Fehlermeldungen

## 2.3 Bestimmungsgemäßer Gebrauch

### Warnung



**Gefahr des Einschließens von Personen.  
Lebensgefahr durch Nahrungs- / Luftmangel.**  
Stellen Sie vor dem Schließen jedes Schlosses sicher, dass sich keine Personen in dem zu verschließenden Behältnis / Raum befinden.

Verwenden Sie das Hochsicherheitsschlosssystem TwinLock BioPIN ausschließlich zum Öffnen und Schließen Ihres Wertbehältnisses sowie zur Verwaltung der Öffnungs- und Schließvorgänge.

## 3 Bedienung

### 3.1 Allgemein

Mit der Eingabeeinheit FlatControl BioPIN können Sie das System TwinLock BioPIN einstellen und bedienen.

Zusätzliche Einstellungen können gegebenenfalls mit der optionalen Software TwinComm USB vorgenommen werden. Wie diese Einstellungen gemacht werden, ist in der separaten Anleitung für das Parametrierset TwinComm beschrieben.

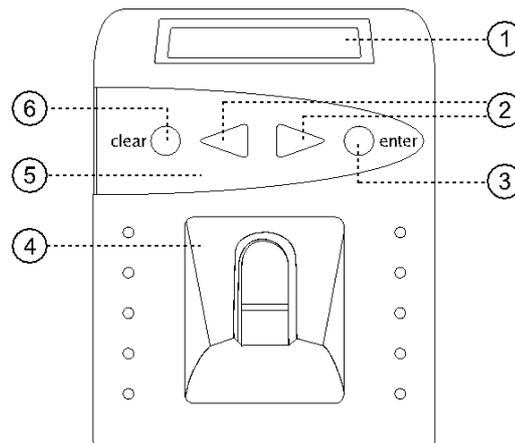


Abbildung 18 Bedieneinheit FlatControl BioPIN

- 1) 2-zeiliges Display mit Beleuchtung  
nach dem Einschalten wird das **Systemmenü** mit frei wählbarem Text in der 1. Zeile und Datum / Uhrzeit in der 2. Zeile angezeigt:

```
TwinLock BioPIN
Mo 10.02.10 08:30
```

- 2) **Menütasten** < und > **zur Navigation** zum vorhergehenden (<) / folgenden (>) Menüpunkt und zur Wahl von Eingaben
- 3) **Enter-Taste** zum Bestätigen der Wahl eines Menüpunktes / zum Bestätigen von Eingabewerten
- 4) **Fingerführung** mit Fingerabdruck-Sensor
- 5) **Menütastatur**
- 6) **Clear-Taste** zum Abbrechen:
  - kurzes Drücken ->Wahl des zuvor angezeigten Menüs
  - bei Code-Eingabe ->Löschen einer eingegebenen Ziffer
  - 3 Sek. Drücken -> Wahl des Systemmenüs

Die Anzeige wird nach 60 Sekunden ohne Eingabe automatisch ausgeschaltet. Durch Drücken einer beliebigen Taste wird sie wieder aktiviert.

Ein Chipkartenfach befindet sich an der Unterseite der Bedieneinheit.

### 3.1.1 Der Systemstatus

Systemeinstellungen sind nur bei ungesichertem, entsperrem System möglich.

Bei gesichertem System werden auf dem Display der Bedieneinheit nur die Menüs **Oeffnen**, **Schliessen** und **Status / Info** angezeigt.

Um das System zu entsperren,

- öffnen Sie Schloss 1 (wenn Option „Zwangsfolge“ [ZF] nicht gewählt) oder
- öffnen Sie alle Schlösser (wenn Option „Zwangsfolge“ [ZF] gewählt).

Wenn Option „Zwangsfolge“ bei der Konfiguration gewählt wurde, können Benutzer bei Systemen mit 2 oder 3 Schlössern nicht wählen, welche Schlösser sie öffnen oder schließen. Siehe auch das Glossar.

#### Mögliche Zustände des Systems:

- Ungesichert:** Schloss 1 (bei „Zwangsfolge“ [ZF] nicht gewählt) / alle Schlösser (bei „Zwangsfolge“ [ZF] gewählt) offen, Anzeige aller Menüs, Einstellungen sind änderbar.
- Teilgesichert:** mindestens ein Schloss offen und ein Schloss (Schloss 1) geschlossen (nur bei „Zwangsfolge“ [ZF] gewählt), Systemeinstellungen sind nicht änderbar
- Gesichert:** Schloss 1 (bei „Zwangsfolge“ [ZF] nicht gewählt) / alle Schlösser (bei „Zwangsfolge“ [ZF] gewählt) geschlossen, Menü-Anzeige eingeschränkt, Öffnungs- und Notfall-Funktionen sind ausführbar, Systemeinstellungen sind nicht änderbar.

Der Systemstatus ist abhängig davon, ob Option „Zwangsfolge“ [ZF] bei der Konfiguration aktiviert wurde oder nicht:

#### Systemstatus mit deaktivierter Option „Zwangsfolge“

Ungesichert / entsperrt, wenn Schloss 1 offen ist. Anzeige aller Menüs.

Teilgesichert gibt es in diesem Fall nicht.

Gesichert, wenn Schloss 1 verschlossen ist. Menüanzeige eingeschränkt.

#### Systemstatus mit aktivierter Option „Zwangsfolge“

Ungesichert, wenn alle Schlösser offen sind.

Teilgesichert, wenn mind. ein Schloss geschlossen und eines offen ist.

Gesichert, wenn alle Schlösser geschlossen sind.

#### Zustandskontakt von TwinAlarm/TwinXT (optional)

Nur bei Systemen mit TwinXT / TwinAlarm: Kontakt in Stellung „offen“ / „geschlossen“, wenn Schloss 1 offen / geschlossen.

#### Systemsignal von Zustandskontakt von TwinAlarm/TwinXT (optional)

Nur bei Systemen mit TwinXT / TwinAlarm: Kontakt in Stellung „offen“ / „geschlossen“, wenn Schloss 1 offen / geschlossen.

## 3.2 Bedienung mit optionaler Software TwinComm

Das System TwinLock BioPIN ist ohne Software-Unterstützung funktionsfähig. Mit Software sind zusätzliche Optionen verfügbar.

Das optionale Parametrierset TwinComm vereinfacht die Konfiguration und ermöglicht die Programmierung von Zeitprogrammen und das Auslesen des Ereignisprotokolls. Zusätzlich kann die Autorisierung für Benutzer flexibel angepaßt werden.

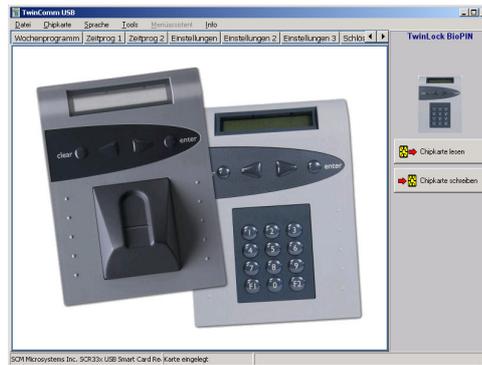


Abbildung 19 Startseite der PC-Software TwinComm USB (Zubehör)

Der Systemverwalter gibt die für die Konfiguration erforderlichen Daten über die grafische Benutzeroberfläche der Software TwinComm USB ein.

Der Datenaustausch mit dem System TwinLock erfolgt mit der Chipkarte TwinCard configuration II und der Funktion `Import / Export` an der Bedieneinheit FlatControl sowie über ein optionales Kartenlese- / -schreibgerät am PC.

## 3.3 Benutzer autorisieren

Der Systemmanager definiert die Autorisierung von Benutzern in einer Matrix, indem er für Benutzer Kontrollkästchen aktiviert (siehe Abb. unten; Beschreibung der Kontrollkästchen siehe nächstes Kapitel). Diese Autorisierung ist fest eingestellt / mit optionaler Software TwinComm USB auch änderbar.

Damit die definierten Autorisierungen im Schlosssystem gelten, importiert der Systemmanager die Konfiguration aus der Software TwinComm USB in das System TwinLock.

Ein Benutzer kann ein Schloss öffnen, wenn er dazu autorisiert wurde und der Schlossmaster (Inhaber des Mastercodes dieses Schlosses) für den Benutzer

- PIN-Code oder / und
- Codekarte oder / und
- Fingerprint-Code am Schloss angemeldet haben.

Wenn am Display der Bedieneinheit die Meldung `Autorisierung` angezeigt wird, fehlt dem aktuellen Benutzer die nötige Autorisierung. Wenn beispielsweise `Autorisierung | PIN-Code` angezeigt wird, darf er nicht PIN-Code eingeben. Der Benutzer sollte sich in diesem Fall an den Systemmanager wenden.

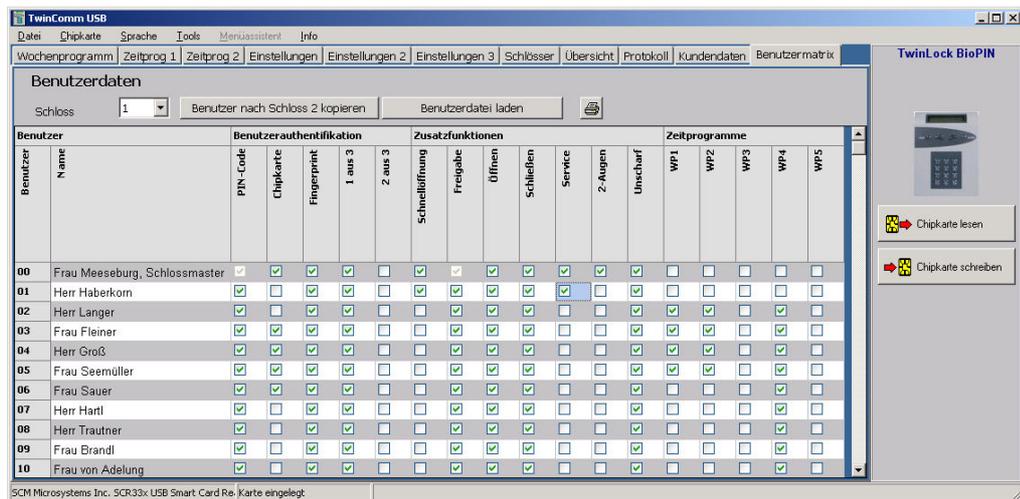


Abbildung 20 Ausschnitt Benutzermatrix in TwinComm USB

Wenn für einen Benutzer das Kontrollkästchen **Freigabe** in der Benutzermatrix nicht aktiviert ist, hat dieser Benutzer keine Rechte und ist für alle Funktionen gesperrt.

### Vorsicht

**Benutzer können kein Schloss öffnen, wenn sie nicht ausreichend autorisiert sind.**

Deaktivieren Sie die ab Werk aktivierten Kontrollkästchen zur Autorisierung in der Benutzermatrix nur nach Beratung durch eine Fachkraft für System TwinLock. Aktivieren Sie bei Bedarf weitere Kontrollkästchen wie etwa **Chipkarte** für Codekarten.

Autorisierung zum Öffnen eines Schlosses mit PIN-Code:

Der Systemmanager aktiviert für den Benutzer die Kontrollkästchen **PIN-Code**, **Freigabe** und **Öffnen**, und falls eine Einbruchmeldeanlage angeschlossen ist, auch **Unschärf**.

Autorisierung zum Öffnen eines Schlosses mit Codekarte:

Der Systemmanager aktiviert für den Benutzer alle oben aufgeführten Kästchen mit Ausnahme von **PIN-Code**, dafür aber zusätzlich **Chipkarte**.

Autorisierung zur Öffnung eines Schlosses mit Fingerprint-Code:

**Kein Benutzer kann ein Schloss allein mit Fingerprint-Code öffnen.**

Der Systemmanager aktiviert für den Benutzer die Kästchen **Fingerprint**, **Freigabe** und **Öffnen** und gegebenenfalls **Unschärf**. Zusätzlich muss der Benutzer für Chipkarte oder / und PIN-Code autorisiert sein.

Der Systemmanager legt auch fest, ob ein Benutzer zwischen PIN-Code-Eingabe und dem Einlegen der Codekarte und Fingerprint wählen kann oder nicht (siehe nächsten Abschnitt, Punkte **1 aus 3** und **2 aus 3**).

### 3.3.1 Kontrollkästchen der Benutzermatrix

Damit ein Benutzer bestimmte Bedienvorgänge ausführen kann, müssen ihm alle dafür nötigen Berechtigungen verliehen werden. Benutzer und Schlossmaster (=Benutzer 00) können vom Systemmanager, der selbst nicht öffnen kann, zur Öffnung von Schlössern autorisiert werden.

Es folgt eine Liste aller Kontrollkästchen, die der Systemmanager für jeden oder für ausgewählte Benutzer aktivieren kann:

#### Kontrollkästchen zum Freischalten der Benutzerauthentifizierung

<b>PIN-Code</b>	Berechtigung zur Eingabe von PIN-Code
<b>Chipkarte</b>	Berechtigung zur Code-Eingabe via Karte
<b>Fingerprint</b>	Berechtigung zur Eingabe biometrischer Daten (ACHTUNG: nur mit Fingerprint keine Öffnung)
<b>1 aus 3</b>	Berechtigung, die Art der Code-Eingabe wählen zu können
<b>2 aus 3</b>	Berechtigung, von drei möglichen zwei beliebige Arten der Code-Eingabe auswählen zu können

#### Kontrollkästchen zum Freischalten von Funktionen

<b>Schnellöffnung</b>	Berechtigung, Schlösser trotz aktiver Zeitprogramme (z.B. Wochenprogramme, Sperrzeit) zu öffnen
<b>Freigabe Öffnen</b>	allgemeine Freigabe zum Code-Eingeben
<b>Schließen</b>	Berechtigung zum Schloss-Öffnen
<b>Service</b>	Berechtigung zum Schloss-Schließen
<b>2-Augen</b>	Berechtigung, das Protokoll zu exportieren
	Berechtigung, trotz eingestelltem 4-Augen-Prinzip allein öffnen / schließen zu dürfen

#### Vorsicht

**Bei Systemen mit Einbruchmeldeanlage kann ein Benutzer (auch der Schlossmaster) kein Schloss öffnen, wenn er nicht zum Unscharfschalten autorisiert ist.**  
Deaktivieren Sie Kontrollkästchen **Unscharf** nicht für Benutzer, die Schlösser öffnen sollen.

<b>Unscharf</b>	Berechtigung zum Unscharfschalten einer optionalen Einbruchmeldeanlage
-----------------	--

#### Kontrollkästchen für die Zuordnung von Zeitprogrammen

<b>WP1 – WP5</b>	Bei aktiviertem Kontrollkästchen gilt das entsprechende Wochenprogramm für den Benutzer
------------------	---

### 3.4 Menüführung in Bedieneinheit FlatControl

(bei geöffnetem System)

```

Systemmenü mit Anzeige Mo 02.01.10 8:30
  ▼
  Oeffnen
  Schliessen
  Scharfschalten (optional)
  Status / Info
  Einstellungen ▶ Mastercode
    ▼ ▶ Managercode
    ▼ ▶ PIN-Code ▶ Anmelden
    ▶ Abmelden
    ▶ Benutzer Anzeige
    ▼ ▶ Codekarte ▶ Anmelden
    ▶ Abmelden
    ▶ Benutzer Anzeige
    ▼ ▶ Fingerprint ▶ Scan Test
    ▶ Anmelden
    ▶ Abmelden
    ▶ Benutzer Anzeige
    ▶ Datum/Uhrzeit
    ▶ Alarmgeräte ▶ TwinXT
    ▼ ▶ TwinAlarm
    ▶ WTU_Funktion
  Service ▶ Reset
    ▼ ▶ Motor - Service
    ▶ Schloss anmelden
    ▶ 1x Riegelwerk
    ▶ Fingerprint ▶ Status / Info
    ▼ ▶ Min. Minutien
    ▶ Bildqualität
    ▶ Sicherheitsstufe
    ▶ Temperatur
  Import / Export ▶ Konfiguration
    ▼ ▶ Protokoll
    ▶ Sprache
  
```

## 3.5 PIN-Codes

### Vorsicht

**Mit werksseitigen Systemmanager- und Mastercodes ist das System nicht gesichert.**

**Gefahr der unberechtigten Öffnung.**

Ändern Sie werksseitige Codes aus Sicherheitsgründen sofort nach der Installation.

### Vorsicht

**Codes mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, können erraten werden.**

**Gefahr der unberechtigten Öffnung.**

Wählen Sie keine Ziffern, die jemand, der Ihre persönlichen Daten kennt, erraten könnte.

### Vorsicht

**Mit angemeldeten Codes, die nicht wiederholt werden können, ist eine Schlossöffnung nicht möglich.**

**Gefahr von erfolglosen Öffnungsversuchen.**

Testen Sie neue Öffnungscodes mehrmals bei geöffneten Wertbehältnissen und sichern Sie sie.

### 3.5.1 Arten und Anzahl von PIN-Codes in jedem Schloss

- 1 Managercode (ohne Berechtigung zur Öffnung des Schlosses)
- 1 Mastercode (mit optionaler Berechtigung zur Öffnung des Schlosses)
- 1-99 PIN-Codes für Benutzer (mit optionaler Berechtigung zur Öffnung des Schlosses, siehe auch Abschnitt „Benutzer autorisieren“)

Mit dem **Managercode** des Schlosses Nr.1 kann das gesamte System konfiguriert werden. Deshalb wird er als **Systemmanagercode**, kurz als Systemcode bezeichnet und sein Inhaber als Systemmanager.

Mit dem **Mastercode** jedes Schlosses können die Benutzercodes des Schlosses an- und abgemeldet werden. Sein Inhaber wird als Schlossmaster bezeichnet. Er kann vom Systemmanager optional zur Schloss-Öffnung autorisiert werden. Manager- und Mastercodes können nicht abgemeldet oder deaktiviert werden.

Mit jedem vom Schlossmaster am Schloss angemeldeten **PIN-Code für Benutzer** kann das Schloss geöffnet werden, wenn der Benutzer vom Systemmanager autorisiert wurde.

PIN-Codes für Benutzer sind werksseitig nicht vorprogrammiert. Über die Benutzermatrix in Software TwinComm definiert, zu welchen Aktionen sie berechtigen. Sie können vom Schlossmaster an- und abgemeldet werden. Jeder Benutzer kann seinen Code ändern und abhängig von seiner Autorisierung das Schloss öffnen und schließen.

Die Anzahl der Ziffern im PIN-Code (Benutzer-, Master-, Manager- und Systemcode) ist abhängig von der VdS-Klasse des Systems TwinLock.

Die **VdS-Klasse** von TwinLock BioPIN wird in Menü `Status / Info` auf dem Display der Bedieneinheit angezeigt.

Systeme der VdS-Klasse 2 enthalten ausschließlich Schlösser des Typs TwinLock 7260, solche der Klasse 3 Schlösser des Typs TwinLock 7220.

Bei Systemen der VdS-Klasse 3 ist jeder PIN-Code achtstellig.

Bei Systemen der VdS-Klasse 2 ist jeder PIN-Code sechstellig.

Master- und Systemmanagercodes ab Werk		
	Master	System / Manager
<b>VdS Klasse 2</b>	123456 (Benutzer 00)	111111 (Benutzer 225)
<b>VdS Klasse 3</b>	12345678 (Benutzer 00)	11111111 (Benutzer 225)

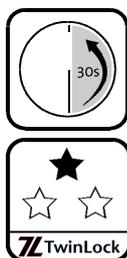
Bei Systemen 7220 der VdS Klasse 3 lautet der dem Benutzer 00 zugeordnete Mastercode eines jeden Schlosses ab Werk „1 2 3 4 5 6 7 8“. Der dem Benutzer 225 zugeordnete Managercode aller Schlösser / Systemcode des Schlosses Nr.1 ist werkseingestellt „1 1 1 1 1 1 1 1“.

Bei Systemen 7260 der VdS Klasse 2 sind die Codes ab Werk ganz ähnlich, siehe Tabelle oben.

### 3.5.2 PIN-Code eingeben

Alle Benutzer geben ihren PIN-Code mit den Menütasten ein.

**Vorbedingungen** Für Sie sind in der Benutzermatrix die Kontrollkästchen **PIN-Code**, **Freigabe** und **Öffnen** aktiviert. Ihr PIN-Code ist am Schloss angemeldet.



- Führen Sie die Schritte bis zur Code-Eingabe so aus wie in der jeweiligen Anleitung beschrieben.  
*Das Display zeigt vor der Code- Eingabe unter anderem 0123456789. Der Cursor steht vor der Eingabe jeder Ziffer bei einer beliebigen Ziffer.*
- Wählen Sie mit < und > jeweils eine Ziffer des Codes und bestätigen Sie jeweils mit `Enter`.  
*Das Display zeigt für jede eingegebene Ziffer ein Sternchen (Asterisk):  
Code: \*\*\*. Nach der Eingabe zeigt das Display die jeweils folgende Meldung wie beispielsweise Bitte warten.*
- Führen Sie gegebenenfalls weitere Schritte aus wie in der jeweiligen Anleitung beschrieben.

Sie haben den PIN-Code erfolgreich eingegeben.

## 3.6 Codekarten

### 3.6.1 Codekarte TwinCard code access

Optionale **Codekarten** (TwinCard code access) können nur vom Schlossmaster angemeldet werden. Dieser kann für bis zu 99 Benutzer pro Schloss je eine Codekarte an- und abmelden. Werksseitig sind die Kartencodes für die Benutzer 01 – 99 inaktiv. Siehe auch Abschnitt „Benutzer autorisieren“.

### 3.6.2 Chipkarte in Bedieneinheit stecken



Wenn der Systemmanager einen Benutzer dazu autorisiert hat (siehe Vorbedingungen unten), kann dieser mit der optionalen Chipkarte TwinCard code access ein Schloss öffnen (siehe „Schloss mit Chipkarte öffnen“ in diesem Kapitel). Mit der optionalen Chipkarte TwinCard configuration II kann gegebenenfalls das Protokoll exportiert werden. Mit TwinCard language kann der Systemmanager Sprachen importieren.

- Vorbedingungen** - für TwinCard code access: für den Benutzer sind in der Benutzermatrix die Kontrollkästchen **Chipkarte**, **Freigabe** und **Öffnen** aktiviert.  
 - für TwinCard configuration II: für den Benutzer sind in der Benutzermatrix die Kontrollkästchen **Freigabe** und **Service** aktiviert.

**Sie benötigen** eine optionale Chipkarte TwinCard code access / -configuration II.

1. Wenn das Display der Bedieneinheit **Karte ein** anzeigt, legen Sie die Chipkarte TwinCard des erwarteten Typs ins Kartenfach ein.  
*Die Karte rastet hörbar ein. Der Chip befindet sich in der oberen Kartenhälfte, die Kartenrückseite zeigt in Ihre Richtung.*

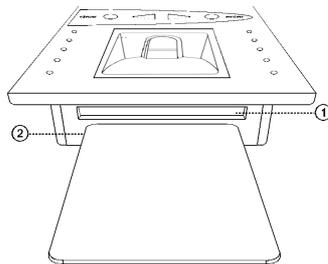


Abbildung 21 Karte und Kartenfach FlatControl BioPIN

- 1) Kartenfach der Eingabeeinheit FlatControl
  - 2) Chipkarte TwinCard (code access / configuration II / language)
2. Warten Sie, bis das Display **Karte aus** anzeigt.
  3. Entnehmen Sie die Chipkarte aus der Bedieneinheit FlatControl.
- Sie haben die Karte erfolgreich eingelegt und sie wieder entnommen.

### 3.7 Fingerprint-Codes

Fingerprint-Codes (max. 10 pro Benutzer, für 99 Benutzer und 1 Master pro Schloss) können nur gemeinsam von Schlossmaster und Benutzer angemeldet und geändert werden. Abmelden kann sie nur der Master. Anders als bei den anderen Codearten kann kein Benutzer allein durch das Einlegen eines Fingers ein Schloss öffnen. Dazu ist die Eingabe mindestens einer anderen Codeart erforderlich. Siehe auch Abschnitt „Benutzer autorisieren“.



Zu Fingerprint allgemein siehe auch die Beschreibungen in diesem Kapitel beginnend mit „Fingerprint: Übersicht“ sowie das Glossar am Ende des Handbuchs.

## 3.8 Bedienung bei aktivierter WTU-Funktion

### Vorsicht

**Ohne autorisierten WTU-Master mit angemeldetem Code kann der WTU-Benutzerbereich nicht verwaltet werden.**

Statten Sie Benutzer 99 **vor Aktivierung der WTU-Funktion** mit allen erforderlichen Rechten aus (siehe Abschnitt „Benutzer autorisieren“) und melden Sie Code für ihn am Schloss an.

Für Benutzer ändert sich die Bedienung bei aktiver WTU-Funktion nicht.

Bei aktivierter WTU-Funktion (siehe auch „WTU-Funktion aktivieren“ in diesem Kapitel) werden die Benutzer jedes Schlosses in zwei Gruppen aufgeteilt. Die Gruppengröße wird via TwinComm USB definiert (ab Werk Benutzer 01-50 bei Schlossmaster und Benutzer 51-98 bei WTU-Master). Der Schlossmaster verwaltet die erste Gruppe (Benutzer 01 bis XX-1). Benutzer 99, der zum WTU-Master wird, verwaltet die WTU-Benutzer (Benutzer XX bis 98).

Schloss- und WTU-Master wählen vor ihrer Code-Eingabe zusätzlich „Master“ beziehungsweise „WTU-Master“:

1. Führen Sie die Schritte einer Anleitung aus, bis Code-Eingabe nötig ist.

*Das Display zeigt Code-Eingabe | Benutzer: Master.*

2. Bestätigen Sie **Master** mit Taste **Enter** oder wählen Sie mit den Menütasten **<** und **>** **WTU-Master** und Taste **Enter**.

*Das Display zeigt WTU-Master oder Master, Code-Eingabe und 0123456789 | Code:.*

3. Geben Sie den zugehörigen Code ein und, falls nötig, führen Sie weitere Schritte der Anleitung aus.

Sie haben erfolgreich Master / WTU-Master gewählt.

## 3.9 Öffnen und Schließen

### Vorsicht

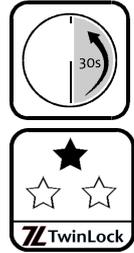
**Bei Systemen mit Einbruchmeldeanlage (EMA) kann ein Benutzer kein Schloss öffnen, wenn er nicht zum Unscharfschalten autorisiert ist.**

Aktivieren Sie für Benutzer in der Benutzermatrix von TwinComm auch Kontrollkästchen **Unscharf**, wenn eine EMA angeschlossen ist.

Um das System zu entsperren, öffnen Sie je nach Systemeinstellung alle Schlösser oder nur Schloss 1. Siehe auch Abschnitt „Der Systemstatus“.

### 3.9.1 Schloss mit PIN-Code öffnen

**Vorbedingungen** Für Sie sind in der Benutzermatrix die Kontrollkästchen **PIN-Code**, **Freigabe** und **Öffnen** und gegebenenfalls **Unscharf** aktiviert.  
Der Schlossmaster hat für Sie PIN-Code angemeldet.



1. Drücken Sie kurz die Taste `Enter`.  
*Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit.*
2. Wählen Sie mit Menütaste `<` oder Menütaste `>` `Oeffnen` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Oeffnen` und gegebenenfalls `Schloss: 1`. Falls `Oeffnen` nicht angezeigt wird, sind alle Schlösser offen.*
3. Wählen Sie gegebenenfalls das Schloss mit `<` oder `>` und `Enter`.  
*Das Display zeigt `Code-Eingabe | Benutzer: Master`*
4. Wählen Sie mit `<` und `>` Ihre Benutzernummer und `Enter`.  
*Das Display zeigt `Benutzer Nr. | PIN-Code`.*
5. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Benutzer Nr., 0123456789` und `Code:.` Siehe auch Abschnitt „PIN-Code eingeben“.*
6. Wählen Sie mit `<` und `>` die PIN-Code-Ziffern und jeweils `Enter`.  
*Das Display zeigt gegebenenfalls `Code-Eingabe | PIN-Code` und Sie können zusätzlich `Fingerprint` und / oder `Codekarte` wählen.  
Bei Benutzern mit Authentifizierung nur mit PIN-Code zeigt das Display `Oeffnen | Bitte warten.. Der Riegel des Schlosses fährt ein. Das Display zeigt Oeffnen | Schloss auf: Nr. und gegebenenfalls System entsperrt.`*

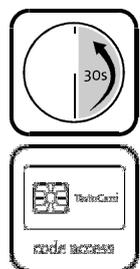
Sie haben das Schloss (gegebenenfalls nach zusätzlicher Codekarten- oder / und Fingerprint-Code-Eingabe) erfolgreich geöffnet.

### 3.9.2 Schloss mit Codekarte öffnen

**Vorbedingungen** Für Sie sind in der Benutzermatrix die Kontrollkästchen **Chipkarte**, **Freigabe**, **Öffnen** (und **Unscharf**) aktiviert. Der Schlossmaster hat Ihre Codekarte am Schloss angemeldet.

**Sie benötigen** die optionale Chipkarte TwinCard code access.

1. Drücken Sie kurz die Taste `Enter`.  
*Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit*
2. Wählen Sie mit Menütaste `<` oder Menütaste `>` `Oeffnen` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Oeffnen` und gegebenenfalls `Schloss: 1`. Falls `Oeffnen` nicht angezeigt wird, sind alle Schlösser offen.*



3. Wählen Sie gegebenenfalls mit < oder > das Schloss und **Enter**.  
Das Display zeigt *Code-Eingabe | Master*.  
Falls Sie als Master öffnen wollen, bestätigen Sie mit **Enter**.
4. Wählen Sie mit < und > Ihre Benutzernummer und **Enter**.  
Das Display zeigt *Benutzer Nr. | PIN-Code*.
5. Wählen Sie mit < und > **Codekarte** und **Enter**.  
Das Display zeigt *Benutzer Nr. | Karte ein*.
6. Legen Sie die Karte TwinCard code access ins Kartenfach (siehe Abschnitt „Chipkarte in Bedieneinheit legen“).  
Das Display zeigt *Lese Daten und danach Karte aus*.
7. Entnehmen Sie die Karte.  
Das Display zeigt *Bitte warten, danach OK und gegebenenfalls Code-Eingabe | PIN-Code* und Sie können zusätzlich PIN- und / oder Fingerprint-Code eingeben.  
Bei Benutzern, die nur mit Codekarte öffnen, zeigt das Display *Oeffnen | Bitte warten*. Der Riegel des Schlosses fährt ein.  
Das Display zeigt *Oeffnen | Schloss auf: Nr.*

Sie haben das Schloss (gegebenenfalls nach zusätzlicher PIN-Code- und / oder Fingerprint-Code-Eingabe) erfolgreich geöffnet.

### 3.9.3 Fingerprint-Code eingeben und Schloss öffnen

Die Authentifizierung nur mit Fingerprint-Code allein ist zur Öffnung eines Schlosses nicht ausreichend. Siehe Abschnitt „Benutzer autorisieren“. Wenn der als „Alarmfinger“ definierte Finger gescannt wird, wird mit der Öffnung „Stiller Alarm“ ausgelöst.

**Vorbedingungen** Sie sind zum Öffnen auch mit **Fingerprint** autorisiert und haben gemeinsam mit dem Schlossmaster Ihren Fingerprint-Code angemeldet.

1. Drücken Sie kurz die Taste **Enter**.  
Der Systemstatus wird geprüft. Das Display zeigt *Datum und Uhrzeit*.
2. Wählen Sie mit Taste < oder > **Oeffnen** und Taste **Enter**.  
Das Display zeigt *Oeffnen und gegebenenfalls Schloss: 1*.
3. Wählen Sie gegebenenfalls mit < oder > das Schloss und **Enter**.  
Das Display zeigt *Code-Eingabe | Master*. Falls Sie als Master öffnen wollen, bestätigen Sie mit **Enter**.
4. Wählen Sie mit < und > Ihre Benutzernummer und **Enter**.  
Das Display zeigt *Code-Eingabe | PIN-Code*.



5. Wählen Sie mit < und > **Fingerprint** und **Enter**.  
*Das Display zeigt **re. Zeigefinger** oder einen anderen Finger.*
6. Wählen Sie mit < und > den zu scannenden Finger und **Enter**.  
*Das Display zeigt <<SCAN>>. So lang die Klammern um „SCAN“ animiert sind, kann ein Finger gescannt werden. Wenn der „Alarmfinger“ gescannt wird, wird mit der Öffnung „Stiller Alarm“ ausgelöst.*
7. Legen Sie einen am Schloss registrierten Finger in die Führung und ziehen Sie ihn gleichmäßig ohne Abstand zur Führung nach unten.  
*Das Display zeigt **Bitte warten**, danach **OK** und gegebenenfalls **Code-Eingabe | PIN-Code** und Sie können PIN-Code eingeben und / oder Codekarte einlegen.*  
*Falls Fingerprint-Code die letzte Stufe Ihrer Authentifizierung war, zeigt das Display **Oeffnen | Bitte warten**. Der Schlossriegel fährt ein. Das Display zeigt **Oeffnen | Schloss auf: Nr.***

Sie haben die Öffnung des Schlosses eingeleitet / es erfolgreich geöffnet.

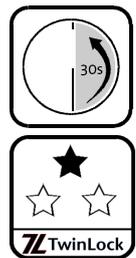
### 3.9.4 Beim Öffnen Stillen Alarm auslösen

So können Sie im Fall einer Bedrohung unauffällig Hilfe verständigen. Der Alarm kann **nicht via Codekarte** aktiviert werden. Bei Fingerprint wird er durch Wahl des „Alarmfingers“ (siehe „Fingerprint-Code eingeben und Schloss öffnen“) aktiviert und bei PIN-Code wie unten beschrieben.

**Vorbedingungen** Für Sie sind in der Benutzermatrix **PIN-Code, Öffnen, Freigabe** und **Unscharf** aktiviert. Ihr PIN-Code ist am Schloss angemeldet. Option „Stiller Alarm“ ist via Parametrierset TwinComm USB aktiviert.

**Sie benötigen** Eine aktivierte Einheit TwinXT / TwinAlarm sowie eine Einbruchmeldeanlage (EMA).

1. Drücken Sie kurz die Taste **Enter**.  
*Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit.*
2. Wählen Sie mit den Tasten < und > **Oeffnen** und danach **Enter**.  
*Das Display zeigt **Oeffnen** und gegebenenfalls **Schloss 1**.*
3. Wählen Sie mit < und > gegebenenfalls das Schloss und **Enter**.  
*Das Display zeigt **Code-Eingabe | Master**.*
4. Wählen Sie mit < und > Ihre Benutzernummer und **Enter**.  
*Das Display zeigt **Benutzer Nr. | PIN-Code***
5. Bestätigen Sie mit **Enter**.  
*Das Display zeigt **Benutzer Nr., 0123456789** und **Code:***
6. Wählen Sie mit < und > alle Ziffern Ihres Codes außer der letzten. Bestätigen Sie jeweils mit **Enter**.



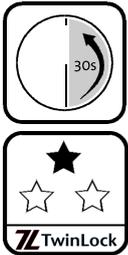
7. Wählen Sie mit < und > statt der letzten Ziffer (z.B. 8) deren Wert plus dem in TwinComm eingestellten Wert für Stillen Alarm (ab Werk „1“, Wertebereich 1-9) und bestätigen Sie mit `Enter`.  
*Falls der letzte Wert zweistellig würde, wählen Sie für die Summe „11“ 1, für „12“ 2, für „13“ 3 und so weiter.*  
*Die Display-Anzeige und gegebenenfalls auch der weitere Öffnungsvorgang ist genau so wie bei einer „normalen“ Öffnung.*

Sie haben erfolgreich Stillen Alarm ausgelöst.

### 3.9.5 Schloss mit Codeverknüpfung öffnen

Nur wenn jeder der zwei beteiligten Benutzer alle ihm zugeteilten Authentifizierungsarten durchführt, öffnet sich das Schloss.

**Vorbedingungen** Auf Registerkarte „Einstellungen“ in TwinComm USB ist die Option „4-Augen-Prinzip (Öffnung)“ aktiviert. Für Sie sind in der Benutzermatrix **Freigabe, Öffnen, PIN-Code** und / oder **Chipkarte** (und **Unschärf**) aktiviert. **2-Augen-Code** ist nicht aktiviert. Der Schlossmaster hat Ihren PIN-Code am Schloss angemeldet.

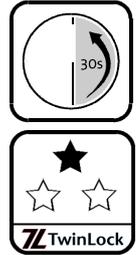


1. Drücken Sie kurz die Taste `Enter`.  
*Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit.*
2. Wählen Sie mit den Tasten < und > `Oeffnen` und danach `Enter`.  
*Das Display zeigt `Oeffnen | Schloss: 1`.*
3. Wählen Sie gegebenenfalls mit < und > das Schloss und `Enter`.  
*Das Display zeigt `Code-Eingabe &1 | Benutzer: Master`.*
4. Wählen Sie mit < und > Ihre Benutzernummer und `Enter`.  
*Das Display zeigt `Benutzer Nr. | PIN-Code`.*
5. Wählen Sie gemäß Ihrer Autorisierung `PIN-Code`, `Codekarte` oder `Fingerprint` und verfahren Sie so wie beim normalen Öffnen eines Schlosses.  
*Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels. Den nächsten Schritt führt eine zweite Person aus.*  
*Das Display zeigt `Code-Eingabe &2 | Master`.*
6. Ein zweiter Benutzer authentifiziert sich am Schloss.  
*Siehe Schritte 3-5.*  
*Das Display zeigt `Oeffnen | Bitte warten`. Der Riegel fährt ein. Das Display zeigt `Oeffnen | Schloss auf: Nr.`*

Sie haben das Schloss erfolgreich mit Codeverknüpfung geöffnet.

### 3.9.6 Schloss mit Öffnungszeitverzögerung öffnen

**Vorbedingungen** Auf Registerkarte „Schlösser“ der optionalen Software TwinComm USB ist ein Wert größer als „0“ für „Öffnungsverzögerung“ gesetzt. Für Sie sind in der Benutzermatrix **Freigabe, Öffnen, PIN-Code / Chipkarte** und / oder **Fingerprint** (und **Unschärf**) aktiviert. Code ist am Schloss angemeldet.



1. Drücken Sie kurz die Taste `Enter`.  
*Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit.*
2. Wählen Sie mit den Tasten `<` und `>` `Oeffnen` und danach `Enter`.  
*Das Display zeigt `Oeffnen` und gegebenenfalls `Schloss 1`.*
3. Wählen Sie mit `<` und `>` gegebenenfalls das Schloss und `Enter`.  
*Das Display zeigt `Code-Eingabe | Benutzer: Master`.*
4. Wählen Sie mit `<` und `>` Ihre Benutzernummer und danach `Enter`.  
*Das Display zeigt `Benutzer Nr. | PIN-Code`.*
5. Wählen Sie gemäß Ihrer Autorisierung `PIN-Code`, `Codekarte` oder `Fingerprint` und verfahren Sie so wie beim „normalen“ Öffnen.  
*Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels. Das Display zeigt `Oeffnen | Zeit: 00:00`. Die ersten 2 Ziffern stehen für die Anzahl der Minuten, die letzten 2 für die der Sekunden.*
6. Warten Sie, bis die Zeit der Öffnungsverzögerung abgelaufen ist.  
*Ein akustisches Signal zeigt den Ablauf der Verzögerungszeit an. Das Display zeigt `Oeffnen | Bitte warten.. Der Riegel fährt ein. Das Display zeigt Oeffnen | Schloss auf: Nr..`*

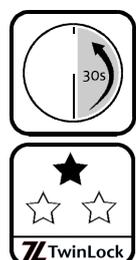
Sie haben das das Schloss erfolgreich geöffnet.

### 3.9.7 Mit Öffnungsverzögerung und Freigabezeit öffnen

Diese Anleitung ist eine Weiterführung der vorhergehenden.

**Vorbedingungen** Siehe vorhergehenden Abschnitt. Zusätzlich ist Option „Freigabezeit“ in TwinComm USB aktiviert.

1. Führen Sie Schritte 1-6 der vorhergehenden Handlungsanleitung aus und bereiten Sie sich darauf vor, eingeben zu können.  
*Ein akustisches Signal zeigt den Ablauf der Verzögerungszeit an. Während der folgenden Freigabezeit ertönt alle 2 Sekunden ein akustisches Signal. Das Display zeigt im Fall eines Systems mit mehreren Schlössern `Code-Eingabe | Schloss Nr.` Falls Sie bis zum Ablauf der Freigabezeit keine Eingabe machen, wird die Öffnung abgebrochen.*
2. Wählen Sie gegebenenfalls mit `<` und `>` das Schloss und `Enter`.  
*Das Display zeigt `Code-Eingabe | Benutzer: Master`.*



3. Wählen Sie mit < und > Ihre Benutzernummer und danach **Enter**.  
*Das Display zeigt Benutzer Nr | PIN-Code.*
4. Geben Sie Ihre(n) Code(s) ein.  
*Siehe Schritt 5 der vorhergehenden Anleitung. Das Display zeigt Oeffnen | Bitte warten. Der Riegel fährt ein. Das Display zeigt Oeffnen | Schloss auf: Nr.*

Sie haben das Schloss erfolgreich geöffnet.

### 3.9.8 Schlösser mit Parallelcode öffnen

Ein Benutzer öffnet Schloss 1, ein zweiter Schloss 2 und ein dritter gegebenenfalls Schloss 3. Alle öffnen dabei gemäß ihrer Autorisierung.

**Vorbedingungen** Option“ Parallelcode“ (nur für Systeme mit mindestens 2 Schlössern) ist über die optionale Software TwinComm eingestellt.  
Für die Benutzer sind in der Benutzermatrix **Freigabe, Öffnen, PIN-Code / Chipkarte** und / oder **Fingerprint** (und **Unschärf**) aktiviert. Code ist am Schloss angemeldet.



1. Drücken Sie kurz die Taste **Enter**.  
*Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit.*
2. Wählen Sie mit den Tasten < und > **Oeffnen** und danach **Enter**.  
*Das Display zeigt Oeffnen | Bitte warten und gegebenenfalls Oeffnen und gegebenenfalls Schloss 1.*
3. Wählen Sie die Nummer des Schlosses und danach **Enter**.  
*Das Display zeigt Code-Eingabe | Benutzer: Master.*
4. Wählen Sie mit < und > Ihre Benutzernummer und danach **Enter**.  
*Das Display zeigt Benutzer Nr | PIN-Code:*
5. Wählen Sie **PIN-Code, Codekarte oder Fingerprint** und öffnen Sie das Schloss gemäß Ihrer Autorisierung.  
*Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels. Schloss 1 öffnet sich.*  
*Das Display zeigt Oeffnen | Schloss auf: 1.*
6. Ein anderer, zweiter Benutzer wiederholt die Schritte 1 bis 5 an Schloss 2 und gegebenenfalls tut dies ein dritter an Schloss 3.  
*Das Display zeigt Oeffnen | Bitte warten. Der Riegel fährt ein. Das Display zeigt Oeffnen | Schloss auf: 2/3.*

Sie haben die Schlösser in Ihrem System erfolgreich geöffnet.

### 3.9.9 Einbruchmeldeanlage (EMA) unscharf schalten

Wenn ein Benutzer nicht zum Unscharfschalten autorisiert ist, kann er bei angeschlossener und scharf geschalteter EMA kein Schloss öffnen. Das Unscharfschalten erfolgt automatisch mit dem Öffnen.

**Vorbedingungen** Für Sie sind in der Benutzermatrix **PIN-Code**, **Freigabe**, **Öffnen** und **Unscharf** sowie **Fingerprint** oder **Chipkarte** aktiviert.

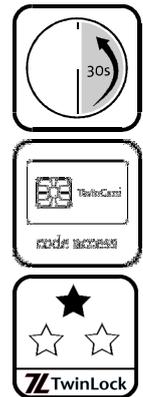
TwinAlarm und EMA sind angeschlossen, TwinAlarm ist aktiviert, EMA ist scharf und alle Schlösser sind geschlossen.

**Sie benötigen** gegebenenfalls Chipkarte TwinCard code access.

- Geben Sie Ihren PIN-Code sowie zusätzlich Codekarte oder Fingerprint-Code ein.

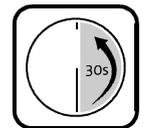
*Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels.*

Sie haben geöffnet und die EMA erfolgreich unscharf geschaltet.



### 3.9.10 Schloss schließen

**Vorbedingungen** Der Riegelwerkskontakt ist nicht so eingerichtet, dass er ein Schließen des Schlosses verhindert. Über Software TwinComm USB ist nicht eingestellt, dass die Schlösser automatisch schließen / nur mit Code-Eingabe geschlossen werden können.



1. Drücken Sie kurz die Taste `Enter`.  
*Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit.*
2. Wählen Sie mit Taste `<` oder `>` `Schliessen` und danach `Enter`.  
*Das Display zeigt `Schliessen` und gegebenenfalls `Schloss 1`. Falls `Schliessen` nicht angezeigt wird, sind die Schlösser geschlossen.*
3. Wählen Sie mit `<` und `>` gegebenenfalls das Schloss und `Enter`.  
*Das Display zeigt `Schliessen | Bitte warten`. Der Riegel fährt aus. Das Display zeigt `Schliessen | Schloss zu: Nr.`*

Sie haben das Schloss erfolgreich geschlossen.

### 3.9.11 Schloss mit Code-Eingabe schließen



Für das Schließen mit Code-Eingabe reicht es aus, entweder PIN- oder Karten- oder Fingerprint-Code einzugeben.

**Vorbedingungen** In TwinComm USB ist auf Seite „Einstellungen“ die Option „Manuelles Schliessen mit Code-Eingabe“ aktiviert.

Für Sie sind in der Benutzermatrix **Freigabe, PIN-Code, Schliessen, Fingerprint** oder **Chipkarte** aktiviert.

1. Drücken Sie kurz die Taste `Enter`.  
*Der Systemstatus wird geprüft. Das Display zeigt Uhrzeit und Datum.*
2. Wählen Sie mit den Tasten `<` und `>` `Schliessen` und `Enter`.  
*Das Display zeigt `Schliessen` und gegebenenfalls `Schloss 1`.*
3. Wählen Sie mit `<` und `>` gegebenenfalls das Schloss und `Enter`.  
*Das Display zeigt `Code-Eingabe | Benutzer: Master`*
4. Wählen Sie mit `<` und `>` Ihre Benutzernummer und danach `Enter`.  
*Das Display zeigt `Benutzer Nr | PIN-Code`.*
5. Wählen Sie `PIN-Code` oder `Codekarte` oder `Fingerprint` und geben Sie den entsprechenden Code ein.  
*Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels.  
Das Display zeigt `Schliessen | Bitte warten`.  
Der Schlossriegel fährt aus.  
Das Display zeigt `Schliessen | Schloss zu: Nr`.*

Sie haben das Schloss erfolgreich geschlossen.

### 3.9.12 Schloss mit Türschalter automatisch schließen

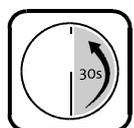
Diese Funktion kann mit Software TwinComm USB eingestellt werden.

**Vorbedingungen** TwinXT oder TwinAlarm sind angeschlossen und aktiviert. In TwinComm ist auf Seite „Einstellungen“ Option „Automatisches Schliessen mit Türschalter“ aktiviert. Der Riegelwerkskontakt ist nicht so eingerichtet, dass er automatisches Schließen verhindert.

- Schließen Sie die Tür des Wertbehältnisses.  
*Über Tür- und Riegelwerksschalter, deren Zustand regelmäßig geprüft wird, registriert das System das Schließen der Tür des Behältnisses und schließt das Schloss / die Schlösser automatisch.*

Das Schloss hat sich automatisch geschlossen.

### 3.9.13 Einbruchmeldeanlage (EMA) scharf schalten



Abhängig von der Einstellung in TwinComm USB („Einstellungen / TwinAlarm / Scharfschalten mit Code“ ein / aus) müssen Benutzer zum Scharf-Schalten PIN- oder Karten- oder Fingerprint-Code eingeben oder nicht.

**Vorbedingungen** TwinAlarm und EMA sind angeschlossen, TwinAlarm ist aktiviert, EMA unscharf und alle Schlösser sind geschlossen. Nur dann wird Menü **Scharfschalten** zum Scharfschalten der EMA angezeigt.  
In **Einstellungen Alarmgeräte** hat der Systemmanager **TwinAlarm** auf **aktiv** gestellt. Für Sie hat er in der Benutzermatrix **Freigabe, PIN-Code** und / oder **Chipkarte** und / oder **Fingerprint** aktiviert.

1. Sperren Sie das System, indem Sie Schloss 1 oder alle Schlösser schließen.  
*Siehe „Der Systemstatus“ in diesem Kapitel. Das System ist gesichert.*
2. Drücken Sie kurz die Taste **Enter**.  
*Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit.*
3. Wählen Sie mit **<** und **>** **Scharfschalten** und danach **Enter**.  
*Falls ! EMA scharf ! angezeigt wird, haben Sie die Aufgabe erfolgreich ausgeführt. Springen Sie zum Ende dieser Beschreibung. Bei aktivierter Option „Scharfschalten mit Code“ zeigt das Display **Code-Eingabe | Benutzer: Master und PIN-Code**.*
  - Wählen Sie Ihre Benutzernummer und **Enter** und **PIN-Code** / **Codekarte** oder **Fingerprint** und **Enter**.  
*Je nach Ihrer Wahl geht es unterschiedlich weiter. Die Code-Eingabe entspricht der beim Öffnen. Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels.*  
*Das Display zeigt **Benutzer: Nr. | Bitte warten**.*  
*Die Bedieneinheit gibt ein akustisches Signal aus.*  
*Das Display zeigt **Benutzer: Nr. | ! EMA Scharf !**.*

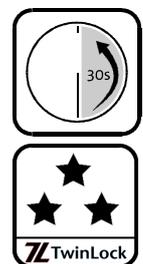
Sie haben die Einbruchmeldeanlage erfolgreich scharf geschaltet.

## 3.10 System einrichten

### 3.10.1 Datum und Uhrzeit einstellen

Von der richtigen Einstellung von Datum und Uhrzeit sind alle Zeitfunktionen des Systems abhängig, ebenso das Ereignisprotokoll. Die Sommer- / Winter-Zeitungstellung erfolgt automatisch, wenn die Option „automatische Umstellung Sommerzeit / Winterzeit“ auf Registerkarte „Einstellungen“ in TwinComm aktiviert ist (Werkseinstellung).

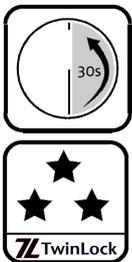
1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit Taste **<** oder Taste **>** **Einstellungen** und bestätigen Sie mit Taste **Enter**.  
*Das Display zeigt **Einstellungen | Mastercodes**.*
3. Wählen Sie mit **<** oder **>** **Datum/Uhrzeit** und danach **Enter**.  
*Das Display zeigt **Code-Eingabe | Systemmanager und 0123456789 | Code:.***



4. Wählen Sie mit < und > die Ziffern des Systemmanagercodes und bestätigen Sie jeweils mit **Enter**.  
*Im Display blinkt die erste Ziffer der aktuell eingestellten Uhrzeit. Wenn Sie 2x **Clear** drücken, behält das System die bisherige Zeiteinstellung.*
5. Geben Sie die aktuelle Uhrzeit mit < und > ein. Drücken Sie jeweils **Enter**, um Ziffern zu bestätigen.  
*Der Cursor „>“ blinkt links vom aktuell eingestellten Wochentag.*
6. Wählen Sie mit < und > die beiden ersten Buchstaben des aktuellen Wochentags und bestätigen Sie mit **Enter**.  
*Die erste Ziffer des Datums blinkt.*
7. Geben Sie Tag, Monat und Jahr so ein wie die Uhrzeit.  
*Das Display zeigt **Datum/Uhrzeit | Gespeichert**.*

Sie haben Datum und Uhrzeit erfolgreich eingestellt.

### 3.10.2 TwinXT / TwinAlarm ein- / ausschalten



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Menütasten < und > **Einstellungen** und bestätigen Sie mit **Enter**.  
*Das Display zeigt **Einstellungen | Mastercodes**.*
3. Wählen Sie mit < und > **Alarmgeräte** und wieder **Enter**.  
*Das Display zeigt **Code-Eingabe, Systemmanager, 0123456789 und Code :.***
4. Geben Sie mit < und > die Ziffern des Systemmanagercodes ein und bestätigen Sie jeweils mit **Enter**.  
*Das Display zeigt **Alarmgeräte | TwinXT**.*
5. Bestätigen Sie **TwinXT** mit **Enter** oder wählen Sie mit < und > **TwinAlarm** und bestätigen Sie mit **Enter**.  
*Das Display zeigt das gewählte Gerät, **aktiv und \*=JA \*=NEIN**.*
6. Wählen Sie zum Aktivieren mit < und > **\*=JA** und **Enter**, zum Deaktivieren mit < und > **\*=NEIN** und **Enter**.  
*Das Display zeigt das gewählte Gerät und **aktiv | Geloescht oder aktiv | Gespeichert**.*

Sie haben TwinAlarm / TwinXT erfolgreich aktiviert / deaktiviert.

### 3.10.3 WTU-Funktion aktivieren

Siehe auch Abschnitt „Bedienung bei aktivierter WTU-Funktion“ am Anfang dieses Kapitels.

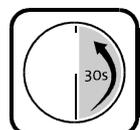
1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Menütasten < und > **Einstellungen** und bestätigen Sie mit **Enter**.  
*Das Display zeigt **Einstellungen** | **Mastercodes**.*
3. Wählen Sie mit < und > **WTU-Funktion** und wieder **Enter**.  
*Das Display zeigt **Code-Eingabe**, **Systemmanager**, **gegebenfalls 0123456789** und **Code** .:*
4. Wählen Sie mit < und > die Ziffern des Systemmanagercodes und bestätigen Sie jeweils mit **Enter**.  
*Vor jeder Eingabe steht der Cursor bei einer anderen Ziffer.  
Das Display zeigt **WTU-Funktion** | **\*=JA** **\*=NEIN**.*
5. Wählen Sie mit < und > zum Aktivieren **\*=JA**, zum Deaktivieren **\*=NEIN** und erneut **Enter**.  
*Das Display zeigt **WTU-Funktion** | **Geloescht** oder **WTU-Funktion** | **Gespeichert**.*

Sie haben die WTU-Funktion erfolgreich ein- oder ausgeschaltet.

### 3.10.4 Protokoll exportieren (TwinComm USB)

**Vorbedingungen** Für Sie sind in der Benutzermatrix **Freigabe** und **Service** und **PIN-Code** oder **Chipkarte** aktiviert.  
**Sie benötigen** das optionale Parametrierset TwinComm USB und die optionale TwinCard configuration II.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Menütasten < und > **Import / Export** und bestätigen Sie mit Taste **Enter**.  
*Das Display zeigt **Import / Export** | **Konfiguration**.*
3. Wählen Sie mit < und > **Protokoll** und **Enter**.  
*Das Display zeigt **Code-Eingabe** | **Manager**.*
4. Bestätigen Sie mit **Enter** oder wählen Sie mit < und > **Master** oder Ihre Benutzernummer und bestätigen Sie mit **Enter**.  
*Das Display zeigt **Systemmanager**, **Master** / **Benutzer Nr.** und **PIN-Code**. Die Eingabe einer Art von Code ist ausreichend.*
5. Bestätigen Sie mit **Enter** und geben Sie PIN-Code ein oder wählen Sie mit < und > **Codekarte** oder **Fingerprint** und **Enter**.  
*Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels.  
Das Display zeigt **Bitte warten** und danach **Protokoll Export** | **Karte ein**.*



6. Legen Sie Chipkarte TwinCard configuration II in die Bedieneinheit. *Siehe Abschnitt „Chipkarte in Bedieneinheit einlegen“. Das Display zeigt `Protokoll -Export | >>>`. Die Anzahl der Pfeile zeigt den Fortschritt. Die Daten werden auf die Karte geschrieben. Das Display zeigt `Daten-Export | Karte aus`.*
7. Nehmen Sie die Chipkarte aus der Bedieneinheit. *Das Display zeigt `OK` und danach `Import / Export`.*

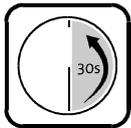
Sie haben das Protokoll erfolgreich auf die Chipkarte gespielt.

### 3.10.5 Protokoll anzeigen / drucken (TwinComm USB)

Öffnungs- und Schließvorgänge, Codeeingaben, Konfigurationsvorgänge und Manipulationsversuche werden protokolliert.

**Vorbedingung** Protokolldaten wurden auf Chipkarte gespeichert.

**Sie benötigen** das optionale Parametrierset TwinComm USB und die optionale Chipkarte TwinCard configuration II.



1. Starten Sie das Programm TwinComm USB an Ihrem Computer und wählen Sie die Schaltfläche `Protokoll`. *Registerkarte „Protokoll“ wird angezeigt.*
2. Legen Sie die Karte TwinCard configuration II mit dem Chip voraus in den Kartenleser.
3. Wählen Sie im Fenster TwinComm USB die Schaltfläche `Chipkarte lesen`. *Am Bildschirm werden die Protokolldaten angezeigt.*
4. Falls sich Benutzerdaten seit dem letzten Laden der Karte geändert haben, wählen Sie Schaltfläche `Benutzer aktualisieren`. *Das Protokoll und die aktuellen Benutzerdaten werden angezeigt.*
5. Wählen Sie die Schaltfläche mit dem Druckersymbol und die gewünschten Einstellungen, um das Protokoll zu drucken. *Die Protokolldaten werden gedruckt.*
6. Wählen Sie Schaltfläche `Protokoll speichern` und vergeben Sie einen Dateinamen, um das Protokoll zu speichern. *Die Daten werden in das Programm Excel exportiert und als CSV-Datei gespeichert.*
7. Entnehmen Sie die Chipkarte aus dem Kartenlesegerät.

Sie haben die Protokolldaten erfolgreich angezeigt und gedruckt.

### 3.10.6 Konfiguration importieren

**Vorbedingung** Mit Parametrierset TwinComm USB ist eine gültige Konfiguration erstellt (und gespeichert) worden.

**Sie benötigen** das optionale Parametrierset TwinComm und die optionale TwinCard configuration II.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit < und > `Import / Export` und `Enter`.  
*Das Display zeigt `Import / Export | Konfiguration`.*
3. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Import / Export | Import`.*
4. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Code-Eingabe, Systemmanager, gegebenenfalls 0123456789 und Code:`. Siehe Abschnitt „PIN-Code eingeben“.*
5. Wählen Sie mit < und > jeweils eine Ziffer des Systemmanager-codes und bestätigen Sie jede Eingabe mit `Enter`.  
*Das Display zeigt `Bitte warten und Daten - Import | Karte ein`.*
6. Legen Sie die Karte TwinCard configuration II in die Bedieneinheit.  
*Siehe Abschnitt „Chipkarte in Bedieneinheit einlegen“. Das Display zeigt `1 >>> 5`. Die Konfiguration wird importiert. Falls sie nicht zulässige Parameter enthält, werden Fehlermeldungen angezeigt. Siehe die folgende Meldungsliste. Das Display zeigt `5 >>> 5 und Daten - Import | Karte aus`.*
7. Nehmen Sie die Chipkarte aus der Bedieneinheit FlatControl.

Sie haben das System TwinLock erfolgreich konfiguriert.

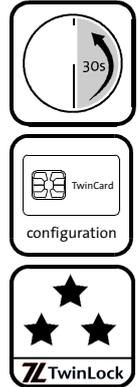
### 3.10.7 Meldungen beim Import der Konfiguration

Beim Import einer Konfiguration können die im Folgenden aufgelisteten Meldungen zweizeilig an der Bedieneinheit angezeigt werden.

- Ändern Sie ungültige Parameter mit der Software TwinComm USB und lesen Sie die Konfiguration erneut ein.

#### In der ersten Zeile des Displays anzeigbarer Text:

`Fehler Konfig.` bei einem Parameter mit ungültigem Wert und  
`Schlosssystem` bei nicht zum System passender Konfiguration



**In der zweiten Zeile des Displays anzeigbarer Text:****Alarm-Verzoeg.**

- ! Alarmverzögerung bei stillem Alarm liegt nicht im zulässigen Wertebereich von 0-99 Minuten.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Alter Code**

- ! Der Wert für „Codealterung“ liegt nicht im zulässigen Wertebereich von 0-99 Monaten.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Bildqualität**

- ! Der untere Grenzwert für „Bildqualität“ liegt nicht im zulässigen Wertebereich von 20-99.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Min. Minutien**

- ! Der untere Grenzwert für Minutien liegt nicht im zulässigen Wertebereich von 09-50.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Öffnen**

- ! Der bei Parameter „Öffnung Schloss 1 -> 2“ eingegebene Wert liegt nicht im zulässigen Wertebereich von 00-99 Minuten.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Parallelcode**

- ! „Parallelcode“ und „4-Augen-Prinzip (Öffnung)“ sind gleichzeitig aktiviert.
- ✓ *Deaktivieren Sie eine der Optionen.*

**PIN-Codes**

- ! Zu wenig PIN-Codes im System. Falls die Konfiguration importiert würde, könnte das System nicht geöffnet werden.
- ✓ *Erhöhen Sie die Anzahl berechtigter Benutzer im System und melden Sie PIN-Codes für sie an.*

**Schliessen&Code**

- ! „Schliessen mit Code“ und „Automatisches Schliessen“ / „Öffnung Schloss 1 -> 2“ sind aktiviert.
- ✓ *Deaktivieren Sie eine der Optionen.*

**Sicherheitsstufe**

- ! Der Wert der Mindestanforderung für „Sicherheitsstufe“ liegt nicht im zulässigen Wertebereich von 30-99.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Sondertage**

- ! Für mindestens einen „Sondertag“ wurde ein ungültiges Datum eingetragen.
- ✓ *Berichtigen Sie die Daten für „Sondertage“.*

**Sperrzeit**

- ! Für Zeitprogramm „Sperrzeit“ wurde mindestens ein ungültiges Datum eingetragen.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Stiller Alarm**

- ! Der Wert für „Alarmziffer“ in TwinComm liegt nicht im zulässigen Wertebereich von 01-09.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Teilsperzeit**

- ! Für Zeitprogramm „Teilsperzeit“ wurde mindestens eine ungültige Uhrzeit eingetragen.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Temperatur**

- ! Der Wert für „Sensortemperatur“ liegt nicht im zulässigen Wertebereich von „00“ oder „18-50 °C“.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Tuer offen**

- ! Der Wert für „Türöffnungsüberwachung“ liegt nicht im zulässigen Wertebereich von 00-99 Minuten.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**TwinAlarm**

- ! Sowohl TwinXT als auch TwinAlarm sind aktiviert.
- ✓ *Deaktivieren Sie das Gerät, das nicht im System ist.*

**Wochenprogramm**

- ! Für Zeitprogramm „Wochenprogramm“ wurde mindestens eine ungültige Uhrzeit eingetragen.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**WTU-Benutzer**

- ! Die Benutzernummer des ersten „WTU-Benutzers“ liegt nicht im zulässigen Wertebereich von „01-99“.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**Zeitverzögerung**

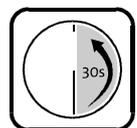
- ! Der Wert für „Öffnungsverzögerung“ eines Schlosses liegt nicht im zulässigen Wertebereich von 00-99.
- ✓ *Tragen Sie einen zulässigen Wert ein.*

**3.10.8 Konfiguration exportieren (TwinComm USB)**

Sie können die Konfiguration des Schlosssystems über Chipkarte in die Parametriersoftware TwinComm USB exportieren.

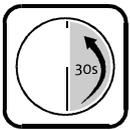
**Sie benötigen** das optionale Parametrierset TwinComm USB und die optionale Chipkarte TwinCard configuration II.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Menütasten < und > **Import / Export** und bestätigen Sie mit **Enter**.  
*Das Display zeigt **Import / Export | Konfiguration**.*



3. Bestätigen Sie mit **Enter**.  
*Das Display zeigt Import / Export | Import.*
4. Wählen Sie mit **<** und **>** **Export** und **Enter**.  
*Das Display zeigt Code-Eingabe, Systemmanager, 0123456789 und Code:.*
5. Wählen Sie mit **<** und **>** jeweils eine Ziffer des Systemmanager-codes und bestätigen Sie jeweils mit **Enter**.  
*Danach zeigt das Display Bitte warten und Daten - Export | Karte ein.*
6. Legen Sie Karte TwinCard configuration II in die Bedieneinheit.  
*Siehe auch Abschnitt „Chipkarte in Bedieneinheit einlegen“.*  
  
*Das Display zeigt >>>. Die Anzahl der Pfeile zeigt den Fortschritt. Die Daten werden auf die Chipkarte geschrieben.*  
*Das Display zeigt Daten - Export | Karte aus.*
7. Nehmen Sie Ihre Chipkarte aus der Eingabeeinheit FlatControl.  
  
Sie haben die Konfiguration erfolgreich auf die Chipkarte gespielt.

### 3.10.9 Sprache wählen



Jeder Benutzer kann zwischen drei Sprachen wählen, wenn diese vorher in FlatControl gespeichert wurden. Siehe auch „Sprache einlesen“.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Menütasten **Import / Export** und bestätigen Sie mit **Enter**.  
*Sie befinden sich im Menü Import / Export.*  
*Das Display zeigt Import / Export | Konfiguration.*
3. Wählen Sie mit **<** und **>** **Sprache** und bestätigen Sie mit **Enter**.  
*Das Display zeigt beispielsweise Sprache | 1 Deutsch. Sie können die Sprache auf Sprachplatz 1, 2 oder 3 wählen. Die gewählte Sprache wird im Folgenden mit gewählte Sprache bezeichnet.*
4. Wählen Sie eine Sprache mit **<** und **>** und Taste **Enter**.  
*Das Display zeigt gewählte Sprache | Gespeichert, und danach OK. Die gewählte Sprache wird sofort angezeigt.*

Sie haben die Sprache des Displays von FlatControl erfolgreich geändert.

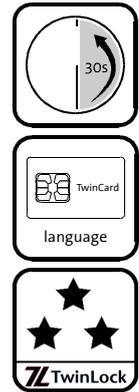
### 3.10.10 Sprache importieren

Die Bedieneinheit verfügt über drei Sprachplätze, auf denen drei Sprachen gespeichert werden können.

**Sie benötigen** die optionale Chipkarte TwinCard language.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Menütasten `Import / Export` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Import / Export | Konfiguration`.*
3. Wählen Sie mit `<` und `>` `Sprache` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Sprache | 1 Deutsch`.*
4. Wählen Sie mit `<` und `>` `Daten-Import` und `Enter`.  
*Das Display zeigt `Sprache | Daten-Import`, danach `Code-Eingabe`, `Systemmanager`, `0123456789` und `Code`.*
5. Wählen Sie mit `<` und `>` jeweils eine Ziffer des Systemmanagercodes und bestätigen Sie jeweils mit `Enter`.  
*Nach der Eingabe zeigt das Display `Sprache | Bitte warten` und `Sprache | Sprachplatz 1<`. Der Cursor blinkt.*
6. Wählen Sie mit `<` und `>` den Sprachplatz und danach `Enter`.  
*Eine dem Sprachplatz eventuell vorher zugeordnete Sprache wird gelöscht. Das Display zeigt `Sprache Import | Karte ein`.*
7. Stecken Sie die Chipkarte TwinCard language in die Bedieneinheit.  
*Siehe Abschnitt „Chipkarte in Bedieneinheit einlegen“.*  
*Das Display zeigt `Daten - Import | Sprache`.*  
*Das Display zeigt `>>>>`. Die Anzahl der Pfeile zeigt den Fortschritt.*  
*Die Konfigurationsdaten werden von der Karte importiert.*  
*Das Display zeigt `Daten - Import | Karte aus`.*
8. Nehmen Sie die Chipkarte aus der Bedieneinheit.

Sie haben die Sprache erfolgreich importiert.



## 3.11 Benutzer verwalten

### 3.11.1 Systemmanagercode ändern

Der Systemmanagercode (=Managercode von Schloss 1) berechtigt nicht zur Schlossöffnung, sondern zur Systemkonfiguration.

#### Vorsicht

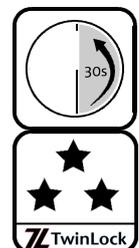
**Mit werksseitigem Systemmanagercode ist Ihr System nicht gesichert.**

Ändern Sie werksseitigen Code so bald wie möglich.  
Verwenden Sie keine persönlichen Daten.

#### Vorsicht

**Ohne Systemmanagercode können Sie Ihr System nicht mehr konfigurieren.**

Speichern Sie den Systemmanagercode an einem sicheren, nur dem Systemmanager zugänglichen Ort.

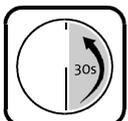


1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Menütasten < und > **Einstellungen** und drücken Sie **Enter**.  
*Das Display zeigt **Einstellungen | Mastercode**.*
3. Wählen Sie mit den Tasten < und > **Managercode** und **Enter**.  
*Das Display zeigt **Code-Eingabe | Schloss 1<**.*
4. Bei 2 oder 3 Schlössern im System wählen Sie **Schloss 1** mit **Enter**.  
*Das Display zeigt **Code-Eingabe, Systemmanager, 0123456789 und Code:.***
5. Wählen Sie mit < und > jeweils eine Ziffer des Systemmanagercodes und bestätigen Sie jeweils mit **Enter**.  
*Das Display zeigt **Managercode | Bitte warten** sowie **Managercode neu und 0123456789 | Code:.***
6. Geben Sie den neuen Systemmanagercode ein.  
*Das Display zeigt **Code bestaetigen | Code:.***
7. Wiederholen Sie die Eingabe des neuen Systemmanagercodes.  
*Das Display zeigt **Managercode neu | Bitte warten** und danach **Managercode neu | Gespeichert**.*

Sie haben den Systemmanagercode erfolgreich geändert.

### 3.11.2 Mastercode / WTU-Mastercode ändern

Der Master- sowie gegebenenfalls der WTU-Mastercode eines Schlosses berechtigen zum Verwalten der Benutzer des Schlosses sowie optional auch zum Öffnen des Schlosses.



#### Vorsicht

**Mit werksseitigen Mastercodes ist Ihr System nicht gesichert.**

Ändern Sie werksseitige Codes so bald wie möglich. Verwenden Sie keine persönliche Daten.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.“.*
2. Wählen Sie mit den Menütasten < und > **Einstellungen** und bestätigen Sie mit **Enter**.  
*Das Display zeigt **Einstellungen | Mastercode**.*
3. Bestätigen Sie **Mastercode** mit **Enter**.  
*Das Display zeigt **Code-Eingabe | Schloss 1<**.*
4. Wählen Sie mit < und > gegebenenfalls das Schloss, dessen Mastercode Sie ändern möchten, und wieder **Enter**.

*Das Display zeigt Mastercode | Code-Eingabe und  
0123456789 | Code:.*

*Bei WTU-Betrieb zeigt das Display Code-Eingabe und Benutzer:  
Master. Sie können mit < und >  
WTU-Master wählen. Bis auf den Zusatz WTU entspricht diese  
Codeänderung sonst derjenigen des Mastercodes.*

5. Wählen Sie die Ziffern des Master- oder des WTU-Mastercodes mit < und > und bestätigen Sie mit Enter.

*Das Display zeigt Mastercode | Bitte warten, dann  
Mastercode neu | Code: und 0123456789 | Code:.*

6. Geben Sie den neuen (WTU-)Mastercode ein.

*Das Display zeigt Code bestätigen und  
0123456789 | Code:.*

7. Wiederholen Sie Ihre Eingabe des neuen (WTU-)Mastercodes.

*Das Display zeigt Mastercode neu | Bitte warten  
und Mastercode neu | Gespeichert.*

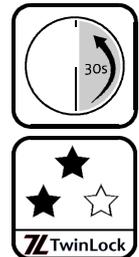
Sie haben den Master- oder den WTU-Mastercode erfolgreich geändert.

### 3.11.3 PIN-Code für Benutzer anmelden

Der Schlossmaster und gegebenenfalls auch der WTU-Master können PIN-Codes für Benutzer am Schloss anmelden. Damit ein Benutzer mit PIN-Code öffnen kann, muss er dafür in der Benutzermatrix von TwinComm USB autorisiert worden sein.

#### Vorsicht

**Wenn bei Systemen mit TwinAlarm die PIN-Codes vor der Installation und der Aktivierung von TwinAlarm angemeldet werden, werden die PIN-Codes der Benutzer nicht in TwinAlarm gespeichert.** Stellen Sie sicher, dass TwinAlarm installiert und aktiviert (siehe „TwinXT / TwinAlarm ... einschalten“) ist, bevor Sie PIN-Codes am Schloss anmelden.



**Vorbedingungen** Wenn eine Einbruchmeldeanlage Teil des Systems ist, muss TwinAlarm installiert und aktiviert sein.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Tasten < und > Einstellungen und Enter.  
*Das Display zeigt Einstellungen | Mastercode.*
3. Wählen Sie mit < und > PIN-Code und danach Enter.  
*Das Display zeigt PIN-Code | Anmelden.*
4. Bestätigen Sie Anmelden mit Enter.  
*Das Display zeigt Anmelden | Code aendern.*
5. Wählen Sie mit < und > Benutzer neu und danach Enter.

Das Display zeigt *Code-Eingabe | Schloss 1.*

6. Wählen Sie mit < und > gegebenenfalls das Schloss und Enter.  
Das Display zeigt bei WTU-Betrieb:  
*Code-Eingabe | Benutzer: Master. Mit < und > können Sie WTU-Master wählen und Enter drücken.*  
*Ohne aktivierte WTU-Funktion zeigt das Display Code-Eingabe, Master, 0123456789 und Code:.*
7. Wählen Sie mit < und > die Ziffern des (WTU-)Mastercodes und drücken Sie jeweils Enter.  
Das Display zeigt *(WTU-)Mastercode | Bitte warten und danach Anmelden | Benutzer 01.*
8. Wählen Sie mit < und > den Benutzer und wieder Enter.  
Das Display zeigt *Benutzercode neu | Code:.*
9. Geben Sie den neuen PIN-Code ein.  
Das Display zeigt *Code bestaetigen | Code:.*
10. Wiederholen Sie die Eingabe des neuen Benutzercodes.  
Das Display zeigt *PIN-Code | Bitte warten und danach Benutzer Nr. | Gespeichert. Danach zeigt das Display Weiterer Code? | \*=JA | \*=Nein.*
11. Wählen Sie *\*=JA*, wenn Sie weitere PIN-Codes anmelden wollen. Für jede weitere Anmeldung wiederholen Sie die Schritte 8 bis 11. Wählen Sie *\*=Nein*, wenn Sie das Anmelden beenden wollen.

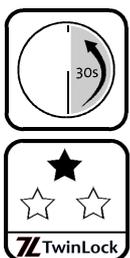
Sie haben erfolgreich PIN-Code für Benutzer angemeldet.

### 3.11.4 PIN-Code ändern

Jeder Benutzer kann bei entsperrem System seinen PIN-Code ändern.

**Vorbedingungen** Für Sie sind in der Benutzermatrix mindestens **PIN-Code, Öffnen** und **Freigabe** aktiviert. Der Schlossmaster hat Ihren PIN-Code am Schloss angemeldet.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.
2. Wählen Sie mit Taste < oder Taste > *Einstellungen* und Enter.  
Das Display zeigt *Einstellungen | Mastercode.*
3. Wählen Sie mit < und > *PIN-Code* und danach Enter.  
Das Display zeigt *PIN-Code | Anmelden.*
4. Wählen Sie mit < und > *Anmelden* und danach Enter.  
Das Display zeigt *Anmelden | Code aendern.*
5. Bestätigen Sie *Code aendern* mit Enter.



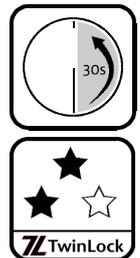
- Das Display zeigt gegebenenfalls **Alter Code | Schloss 1**.*
6. Wählen Sie mit < und > gegebenenfalls das Schloss und Enter.  
*Das Display zeigt **Alter Code | Benutzer:01**.*
  7. Wählen Sie mit < und > Ihre Benutzernummer und danach Enter.  
*Das Display zeigt **Benutzer Nr., 0123456789 und Code:**.*
  8. Wählen Sie mit < und > jeweils eine Ziffer Ihres bisherigen Codes und bestätigen Sie jeweils mit Enter.  
*Das Display zeigt **Benutzercode neu, 0123456789 und Code:**.*
  9. Geben Sie den neuen PIN-Code ein.  
*Das Display zeigt **Code bestaetigen , ... und Code:**.*
  10. Geben Sie Ihren neuen Code nochmals ein.  
*Das Display zeigt **PIN-Code | Bitte warten.***  
*Das Display zeigt **Benutzer Nr. | Gespeichert.***

Sie haben erfolgreich Ihren PIN-Code geändert.

### 3.11.5 PIN-Code abmelden

#### Vorsicht

**Gefahr eines Konfigurationsfehlers: Wertbehältnis kann möglicherweise nicht mehr geöffnet werden.**  
Schlösser mit zu wenig angemeldeten Codes können nicht geöffnet werden. Wenn Sie „Codeverknüpfung“ oder „Zwangsfolge“ eingerichtet haben, melden Sie an jedem Schloss mindestens so viele zur Öffnung autorisierte Codes an wie benötigt.



1. Wählen Sie Menü **Einstellungen | PIN-Code**.  
*Eine genaue Anleitung hierfür siehe obige Beschreibung „PIN-Code ändern“, Schritte 1-4. Das Display zeigt **PIN-Code | Anmelden**.*
2. Wählen Sie mit < und > **Abmelden** und wieder Enter.  
*Das Display zeigt gegebenenfalls **Code-Eingabe | Schloss 1**.*
3. Wählen Sie gegebenenfalls mit < und > das Schloss und Enter.  
*Das Display zeigt bei WTU-Betrieb:*  
***Code-Eingabe | Benutzer: Master**.*  
*Mit < und > können Sie WTU-Master wählen und Enter drücken.*  
*Ohne aktivierte WTU-Funktion zeigt das Display **Code-Eingabe, Master, 0123456789 und Code:**.*
4. Geben Sie den (WTU-)Mastercode ein.  
*Das Display zeigt **(WTU-)Mastercode | Bitte warten und danach **Abmelden | Benutzer: 01****.*

- Wählen Sie mit den Menütasten < und > den Benutzer, dessen Code Sie abmelden möchten, und Enter.

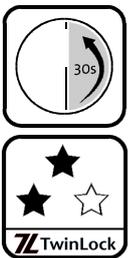
*Das Display zeigt PIN-Code | Bitte warten und Benutzer XX | Geloescht. Danach zeigt das Display Weiterer Code? | \*=JA | \*=Nein.*

- Wählen Sie \*=JA, wenn Sie weitere PIN-Codes abmelden wollen. Für jede weitere Abmeldung wiederholen Sie Schritt 5.  
Wählen Sie \*=Nein, wenn Sie das Anmelden beenden wollen.

Sie haben erfolgreich PIN-Code abgemeldet.

### 3.11.6 PIN-Code Benutzer-Anzeige

Der Schlossmaster und gegebenenfalls auch der WTU-Master können sich anzeigen lassen, welche Benutzercodes angemeldet sind. Jeder Master kann nur die Benutzer der ihm zugeordneten Gruppe anzeigen.



- Wählen Sie Menü **Einstellungen** | **PIN-Code**.  
*Eine genaue Anleitung hierfür siehe obige Beschreibung „PIN-Code ändern, Schritte 1-4. Das Display zeigt PIN-Code | Anmelden.*
- Wählen Sie mit < und > **Benutzer-Anzeige** und Taste **Enter**.  
*Das Display zeigt gegebenenfalls Code-Eingabe | Schloss 1.*
- Wählen Sie gegebenenfalls mit < und > das Schloss, dem Sie als Master zugeordnet sind, und bestätigen Sie mit **Enter**.  
*Das Display zeigt bei WTU-Betrieb:  
Code-Eingabe | Benutzer: Master.  
Mit < und > können Sie WTU-Master wählen und Enter drücken.  
Ohne aktivierte WTU-Funktion zeigt das Display Code-Eingabe, Master, 0123456789 und Code:.*
- Wählen Sie mit < und > die Ziffern des (WTU-)Mastercodes und danach jeweils **Enter**.  
*Das Display zeigt Master | Bitte warten und  
PIN-Benutzer: XXX | Ben-Code Nr.:OK/NOK.  
Oben wird die Anzahl der angemeldeten PIN-Benutzer angezeigt, unten jeweils eine Benutzernummer und OK oder NOK.*
- Blättern Sie mit < und > durch die Nummern der Benutzer.  
*In der unteren Zeile wird der Reihe nach angezeigt, für welche Benutzer PIN-Code angemeldet ist.  
OK und NOK zeigen den Zustand:  
NOK bedeutet, dass für den Benutzer kein PIN-Code angemeldet ist.  
OK bedeutet, dass für den Benutzer PIN-Code angemeldet ist.*

Sie haben erfolgreich angezeigt, für wie viele und für welche Benutzer PIN-Code angemeldet ist.

### 3.11.7 Codekarte anmelden

Der Schlossmaster und gegebenenfalls auch der WTU-Master können Codekarten TwinCard code access anmelden.

**Sie benötigen** eine Chipkarte TwinCard code access pro Benutzer.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit Taste < und > **Einstellungen** und **Enter**.  
*Das Display zeigt **Einstellungen | Mastercode**.*
3. Wählen Sie mit < und > **Codekarte** und danach **Enter**.  
*Das Display zeigt **Codekarte | Anmelden**.*
4. Bestätigen Sie mit **Enter**.  
*Das Display zeigt **Code-Eingabe | Schloss 1**.*
5. Wählen Sie mit < und > gegebenenfalls das Schloss und **Enter**.  
*Das Display zeigt bei WTU-Betrieb:  
**Code-Eingabe | Benutzer: Master**.  
Mit < und > können Sie WTU-Master wählen und **Enter** drücken.  
Ohne aktivierte WTU-Funktion zeigt das Display **Code-Eingabe, Master, 0123456789** und **Code:.***
6. Wählen Sie mit < und > die Ziffern des (WTU-)Mastercodes und danach jeweils **Enter**.  
*Das Display zeigt **Bitte warten** und **Anmelden | Benutzer: 01**.*
7. Wählen Sie mit < und > die Benutzernummer, für die Sie die Codekarte anmelden, und bestätigen Sie mit Taste **Enter**.  
*Das Display zeigt **Benutzer Nr | Karte ein**.*
8. Stecken Sie die Karte in das Kartenfach der Bedieneinheit.  
*Siehe Abschnitt „Karte einlegen“ in diesem Kapitel.  
Das Display zeigt **Bitte warten** und danach **Karte aus**.*
9. Entnehmen Sie die Karte.  
*Das Display zeigt **Benutzer Nr. | Angemeldet**. Danach zeigt das Display **Weiterer Code? | \*=JA | \*=Nein**.*
10. Wählen Sie **\*=JA**, wenn Sie weitere Codekarten anmelden wollen und wiederholen Sie jeweils die Schritte 7-10.  
Wählen Sie **\*=Nein**, wenn Sie das Anmelden beenden wollen.

Sie haben erfolgreich Codekarten angemeldet.



### 3.11.8 Codekarte abmelden



Der Schlossmaster und gegebenenfalls auch der WTU-Master können angemeldete Codekarten wieder abmelden. Selbst wenn ein Benutzer zum Schloss-Öffnen mit Codekarte autorisiert ist, kann er ein Schloss nicht öffnen, wenn seine Karte abgemeldet ist.

#### Vorsicht

#### Gefahr eines Konfigurationsfehlers: Wertbehältnis kann möglicherweise nicht mehr geöffnet werden.

Schlösser mit zu wenig angemeldeten Codes können nicht geöffnet werden. Wenn Sie Option „Codeverknüpfung“ oder „Zwangsfolge“ aktiviert haben, melden Sie an jedem Schloss mindestens so viele zur Öffnung autorisierte Codes an wie benötigt.

1. Wählen Sie Menü `Einstellungen | Codekarte`.  
*Genauere Anleitung siehe obige Beschreibung „Codekarte anmelden“, Schritte 1-3. Das Display zeigt `Codekarte | Anmelden`.*
2. Wählen Sie mit `<` und `>` `Abmelden` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Code-Eingabe | Schloss 1`.*
3. Wählen Sie mit `<` und `>` gegebenenfalls das Schloss und `Enter`.  
*Das Display zeigt bei WTU-Betrieb:  
`Code-Eingabe | Benutzer: Master`.  
Mit `<` und `>` können Sie WTU-Master wählen und `Enter` drücken.  
Ohne aktivierte WTU-Funktion zeigt das Display `Code-Eingabe, Master, 0123456789` und `Code:`. Siehe auch Abschnitt ‚PIN-Code eingeben‘.*
4. Geben Sie den (WTU-)Mastercode ein.  
*Das Display zeigt `Bitte warten und Abmelden | Benutzer: (WTU-)Master`.*
5. Wählen Sie mit `<` und `>` den Benutzer, dessen Codekarte Sie abmelden möchten, und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Benutzer Nr. | Bitte warten und Benutzer Nr. | Abgemeldet`. Danach zeigt das Display `Weiterer Code? | *=JA | *=Nein`.*
6. Wählen Sie `*=JA`, wenn Sie weitere Codekarten abmelden wollen. Für jede weitere Abmeldung wiederholen Sie Schritte 5 und 6.  
Wählen Sie `*=Nein`, wenn Sie das Abmelden beenden wollen.

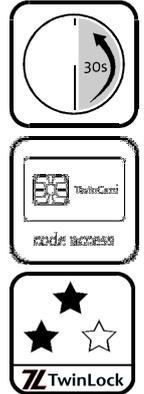
Sie haben erfolgreich Codekarten abgemeldet.

### 3.11.9 Codekarte Benutzer-Anzeige

Der Schlossmaster und gegebenenfalls auch der WTU-Master können anzeigen, für welche Benutzer Codekarten am Schloss angemeldet sind. Bei WTU-Betrieb können Master und WTU-Master jeweils nur die Benutzer ihres Benutzerbereichs anzeigen.

1. Wählen Sie Menü `Einstellungen | Codekarte`.  
*Genauere Anleitung siehe obige Beschreibung „Codekarte anmelden“, Schritte 1-3. Das Display zeigt `Codekarte | Anmelden`.*
2. Wählen Sie mit `<` und `>` `Benutzer-Anzeige` und `Enter`.  
*Das Display zeigt `Code-Eingabe | Schloss 1`.*
3. Wählen Sie mit `<` und `>` gegebenenfalls das Schloss und `Enter`.  
*Das Display zeigt bei WTU-Betrieb:  
`Code-Eingabe | Benutzer: Master`.  
Mit `<` und `>` können Sie WTU-Master wählen und `Enter` drücken.  
Ohne aktivierte WTU-Funktion zeigt das Display `Code-Eingabe, Master, 0123456789` und `Code:.`*
4. Wählen Sie mit `<` und `>` die Ziffern des (WTU-)Mastercodes und danach jeweils `Enter`.  
*Das Display zeigt `Bitte warten` und danach `Karten 000 | Karte 00 (N)OK`.  
Oben wird die Anzahl der angemeldeten Codekarten angezeigt, unten jeweils eine Benutzernummer und `OK` oder `NOK`.  
`NOK` bedeutet, dass für den Benutzer keine Karte angemeldet ist.  
`OK` bedeutet, dass für den Benutzer eine Codekarte angemeldet ist.*
5. Blättern Sie mit `<` und `>` durch die Nummern der Benutzer.  
*Sie sind im Menü `Codekarte | Benutzer-Anzeige`.*

Sie haben erfolgreich angezeigt, für welche Benutzer Codekarten angemeldet sind.



### 3.11.10 Fingerprint: Überblick

Mit Fingerprint-Code allein kann kein Schloss geöffnet werden. Benutzer müssen vor einer Öffnung zusätzlich PIN-Code oder / und Codekarte eingeben.

Damit Benutzer Fingerprint-Code eingeben können, muss sie der Systemmanager dazu in der Benutzermatrix von TwinComm USB autorisiert haben. Siehe in diesem Kapitel auch Abschnitt „Benutzer autorisieren“.

Zusätzlich muss der Schlossmaster beziehungsweise gegebenenfalls der WTU-Master gemeinsam mit den Benutzern deren Fingerprint-Code am Schloss angemeldet haben.



Abbildung 22 Bedieneinheit mit Fingerführung

Jeder Benutzer kann mit `Scan Test` (siehe auch die folgende Beschreibung „Fingerprint-Scan testen“) das Scannen üben und die für ihn charakteristischen Fingerprint-Eckdaten ermitteln.

Dies sind die Werte für

- die Anzahl an Minuten (individuelle Merkmale)
- die typische Bildqualität seines Fingerabdrucks
- den Grad der Übereinstimmung (Passung), den die bei wiederholten Durchgängen extrahierten Daten aufweisen.

Der Schlossmaster kann für die einzelnen Benutzer die Mindestanzahl an Minuten, den Schwellwert für die Bildqualität sowie die Sicherheitsstufe individuell festlegen. Generelle Untergrenzen für diese Werte sind via Software TwinComm USB gesetzt und dort einstellbar.

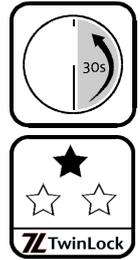
Wenn dies geschehen ist, meldet der Inhaber des Mastercodes zusammen mit dem Benutzer den Fingerprint-Code desselben an. Siehe Beschreibung „Fingerprint-Code anmelden“ in diesem Kapitel.

Siehe auch die Beschreibungen „Fingerprint: Min. Minuten festlegen“, „Fingerprint: Schwellwert für Bildqualität festlegen“ und „Fingerprint: Sicherheitsstufe festlegen“ in diesem Kapitel.

Der Systemmanager kann die Temperatur des Sensors einstellen.

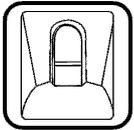
### 3.11.11 Fingerprint-Scan testen

Mit dem Menüpunkt `Scan Test` können Benutzer für sie selbst charakteristische biometrisch relevante Werte ermitteln und sie können das Scannen „üben“. Danach kann der Schlossmaster Fingerprint-Code-Einstellungen individuell festlegen. Siehe auch die anderen Fingerprint-Anleitungen in diesem Kapitel.



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit Taste `<` oder `>` `Einstellungen` und `Enter`.  
*Das Display zeigt `Einstellungen | Mastercode`.*
3. Wählen Sie mit `<` oder `>` `Fingerprint` und `Enter`.  
*Das Display zeigt `Fingerprint | Scan Test`.*
4. Bestätigen Sie mit Taste `Enter`.  
*Das Display zeigt `Scan Test | <<SCAN>>`. Sie können einen Finger auflegen, wenn die Klammern um `<<SCAN>>` animiert sind.*
5. Legen Sie einen Finger auf (Fingerkuppe oben, Innenseite in Führung) und ziehen Sie ihn direkt auf der Führung nach.  
*Das Display zeigt `Minu:XX Quali:XX | OK`, wenn die Bildqualität den eingestellten Mindestanforderungen entspricht / sie übertrifft. „Minu“ steht für „Minutien“, „Quali“ für Bildqualität.*  
*Es zeigt `Minu:XX Quali:XX | Nicht erkannt!`, wenn ein Wert den gesetzten Mindestanforderungen nicht entspricht.*
6. Wenn das Display `<SCAN>` zeigt, legen Sie den gleichen Finger nochmals auf.  
*Nach dem zweiten Durchgang zeigt das Display `Passung: XX`. Der angezeigte Wert bezeichnet den Grad der Übereinstimmung der bei den Scan Test Durchgängen ermittelten Daten. Auf der Basis dieses Wertes kann die „Sicherheitsstufe“ für Benutzer definiert werden. In einem Scan-Test Durchgang kann ein Finger 3x gescannt werden.*
7. Wenn `Fingerprint | Scan Test` angezeigt wird, bestätigen Sie mit Taste `Enter`, um einen weiteren Finger zu scannen.  
*Das Display zeigt erneut `Scan Test | <<SCAN>>`.*  
*Das Display zeigt `Scan Test | schlechtes Bild`, wenn die Qualität den eingestellten Mindestanforderungen nicht entspricht.*  
*Es zeigt `Scan Test | Kein Bild`, wenn der Sensor während des Scan-Vorgangs keinen Finger registriert hat.*

Sie haben die für den Fingerprint-Benutzer charakteristischen Eckdaten erfolgreich ermittelt und das Scannen „geübt“.



### 3.11.12 Fingerprint: Min. Minutien festlegen

Der Schlossmaster kann die Mindestanzahl von Minutien (Merkmale, Wertebereich 09 - 50, voreingestellter Wert 18) für Fingerprint-Code eines Benutzers individuell festlegen.

Wertebereich: 09 – 50, voreingestellter Wert: 18

Nach der Einstellung meldet der Schlossmaster zusammen mit dem Benutzer dessen Fingerprint-Code an. Siehe „Fingerprint-Code anmelden“ in diesem Kapitel.

**Vorbedingungen** Der Benutzer hat mit `Scan Test` (siehe „Fingerprint-Scan testen“) die für ihn charakteristische Anzahl an Minutien ermittelt.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Tasten `<` oder `>` `Service` und danach `Enter`.  
*Das Display zeigt `Service | Reset`.*
3. Wählen Sie mit `<` oder `>` `Fingerprint` und wieder `Enter`.  
*Das Display zeigt `Service | Fingerprint`.*
4. Wählen Sie wieder `Enter`.  
*Das Display zeigt `Fingerprint | Status / Info`.*
5. Wählen Sie mit `<` oder `>` `Min.Minutien` und `Enter`.  
*Das Display zeigt `Code-Eingabe | Schloss 1`.*
6. Drücken Sie `Enter` oder wählen Sie gegebenenfalls Schloss 2 / 3.  
*Das Display zeigt bei WTU-Betrieb:  
`Code-Eingabe | Benutzer: Master`.  
Mit `<` und `>` können Sie WTU-Master wählen und `Enter` drücken.  
Ohne aktivierte WTU-Funktion zeigt das Display `Code-Eingabe, Master, gegebenenfalls 0123456789` und `Code:.`*
7. Geben Sie die Ziffern des (WTU-)Mastercodes mit `<` und `>` und `Enter` ein.  
*Das Display zeigt `(WTU-)Master | Bitte warten`,  
und danach `Min.Minutien | Benutzer (WTU-)Master`.*
8. Wählen Sie den Benutzer mit den Tasten `<` oder `>` und `Enter`.  
*Das Display zeigt `Min.Minutien | 18`.  
Setzen Sie als Mindestwert den mit `Scan Test` ermittelten Wert abzüglich einer kleinen Toleranz (ca. 1-2). Mit dem optionalen Set TwinComm USB kann der allgemeine Grenzwert („9“ ab Werk) geändert werden.*
9. Vergrößern / verringern Sie den Wert mit `<` oder `>` und `Enter`.  
*Das Display zeigt `Min.Minutien | Gespeichert`.*

Sie haben die Mindestanzahl der Minutien für Fingerprint-Code eines Benutzers erfolgreich spezifiziert.

### 3.11.13 Fingerprint: Schwellwert für Bildqualität festlegen

Der Wert „Bildqualität“ wird verwendet, um nur Fingerprint-Aufnahmen guter Qualität mit eindeutigen Informationen zuzulassen. Ein Wert von 60 steht für sehr gute Qualität, viel höhere Werte sind nicht möglich.

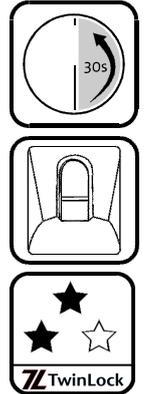
Wertebereich: 20 – 99, voreingestellter Wert: 30

Mögliche Gründe für geringe Bildqualität:

Finger zu schnell / langsam über Sensor gezogen, zu starker / zu leichter Druck auf Sensor, zu trockene / feuchte Finger, kleine Verletzungen

**Vorbedingungen** Der Benutzer ist für Fingerprint autorisiert. (siehe Abschnitt „Autorisierung von Benutzern“). Er hat mit **Scan Test** (siehe „Fingerprint-Scan testen“) den für ihn typischen Wert für „Bildqualität“ ermittelt.

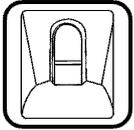
Nach jedem Scan-Test wird die Bildqualität auf dem Display angezeigt. Wir empfehlen, den Wert für Bildqualität auf etwa 90% des angezeigten Wertes zu setzen.



- Wählen Sie Menü **Service | Fingerprint**.  
*Genauere Anleitung siehe obige Beschreibung „Fingerprint: Min. Minuten festlegen“, Schritte 1-4.*  
*Das Display zeigt **Fingerprint | Status / Info**.*
- Wählen Sie mit **< oder > Bildqualität** und **Enter**.  
*Das Display zeigt **Code-Eingabe | Schloss 1**.*
- Bestätigen Sie mit Taste **Enter** oder wählen Sie gegebenenfalls Schloss 2 oder 3.  
*Das Display zeigt bei WTU-Betrieb:*  
***Code-Eingabe | Benutzer: Master**.*  
*Mit **< und >** können Sie WTU-Master wählen und **Enter** drücken.*  
*Ohne aktivierte WTU-Funktion zeigt das Display **Code-Eingabe, Master, gegebenenfalls 0123456789** und **Code :.***
- Geben Sie die Ziffern des (WTU-)Mastercodes mit **< und >** und **Enter** ein.  
*Das Display zeigt **(WTU-)Mastercode | Bitte warten** und danach **Bildqualität | Benutzer: (WTU-)Master**.*
- Wählen Sie den Benutzer mit Tasten **< oder >** und **Enter**.  
*Das Display zeigt **Bildqualität | XX**.*
- Vergrößern / verringern Sie den Wert mit **< oder >** und **Enter**.  
*Das Display zeigt **Bildqualität | Gespeichert**.*  
*Die Meldung **schlechtes Bild** wird angezeigt, wenn der Wert beim Anmelden von Fingerprint-Code unterschritten wird.*

Sie haben den Wert für die mindestens erforderliche Bildqualität für Fingerprint-Daten eines Benutzers erfolgreich spezifiziert.

### 3.11.14 Fingerprint: Sicherheitsstufe festlegen



Die Sicherheitsstufe gibt an, ab welchem Ähnlichkeitsmaß („Passung“) ein Fingerabdruck als identisch mit gegebenenfalls gespeicherten Daten interpretiert wird, ab wann eine Person also als identifiziert gilt. Dieser Wert hat direkten Einfluss auf die Sicherheit des Systems.

Wertebereich: 30 – 99, voreingestellter Wert: 60, unterer Grenzwert 30.

**Vorbedingung** Der Benutzer ist für Fingerprint autorisiert. (siehe Abschnitt „Autorisierung von Benutzern“). Er hat mit `Scan Test` (siehe „Fingerprint-Scan testen“) den für ihn typischen Wert für „Passung“ ermittelt.

Nach jedem Scan-Test wird der Wert für „Passung“ auf dem Display angezeigt. Wir empfehlen, von diesem Wert etwa 10-15 abzuziehen und das Ergebnis als „Sicherheitsstufe“ für den Benutzer zu setzen.

1. Wählen Sie Menü `Service | Fingerprint`.  
*Genauere Anleitung siehe obige Beschreibung „Fingerprint: Minuten festlegen“, Schritte 1-4.*  
*Das Display zeigt `Fingerprint | Status / Info`.*
2. Wählen Sie mit `<` oder `>` `Sicherheitsstufe` und `Enter`.  
*Das Display zeigt `Code-Eingabe | Schloss 1`.*
3. Bestätigen Sie mit Taste `Enter` oder wählen Sie gegebenenfalls Schloss 2 oder 3.  
*Das Display zeigt bei WTU-Betrieb:*  
*`Code-Eingabe | Benutzer: Master`.*  
*Mit `<` und `>` können Sie WTU-Master wählen und `Enter` drücken.*  
*Ohne aktivierte WTU-Funktion zeigt das Display `Code-Eingabe, Master, gegebenenfalls 0123456789` und `Code :`.*
4. Geben Sie mit `<` und `>` und `Enter` die Ziffern des Mastercodes ein.  
*Das Display zeigt `(WTU-)Mastercode | Bitte warten.`*  
*und `Sicherheitsstufe | Benutzer: (WTU-)Master`.*
5. Wählen Sie den Benutzer mit Tasten `<` oder `>` und `Enter`.  
*Das Display zeigt `Sicherheitsstufe | 30`.*
6. Vergrößern / verringern Sie den Wert mit `<` oder `>` und `Enter`.  
*Das Display zeigt `Sicherheitsstufe | Gespeichert`*

Sie haben den Wert für die Sicherheitsstufe der Fingerprint-Daten eines Benutzers erfolgreich spezifiziert.

### 3.11.15 Fingerprint-Code anmelden

Der Schlossmaster kann gemeinsam mit einem Benutzer dessen Fingerprint-Code anmelden. Drei erfolgreiche Scans während eines Arbeitsgangs sind Voraussetzung für das Anmelden von Fingerprint-Code.

Einer der erfassten Finger kann zum „Alarmfinger“ erklärt werden, mit dem bei einer Schlossöffnung Stiller Alarm ausgelöst wird.

**Vorbedingungen** Der Benutzer ist für Fingerprint autorisiert (siehe Abschnitt „Autorisierung von Benutzern“). Via Menü `Scan Test` hat der Benutzer seine Fingerprint-Eckdaten ermittelt und der Schlossmaster hat für ihn `Min.Minutien`, `Bildqualität` und `Sicherheitsstufe` individuell eingestellt.



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Tasten < oder > `Einstellungen` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Einstellungen | Mastercode`.*
3. Wählen Sie mit < oder > `Fingerprint` und `Enter`.  
*Das Display zeigt `Fingerprint | Scan Test`.*
4. Wählen Sie mit < oder > `Anmelden` und `Enter`.  
*Sie sind im Menü `Fingerprint | Anmelden`.*  
*Das Display zeigt gegebenenfalls `Code-Eingabe | Schloss 1`.*
5. Bestätigen Sie mit Taste `Enter` oder wählen Sie gegebenenfalls Schloss 2 oder 3.  
*Das Display zeigt bei WTU-Betrieb:*  
*`Code-Eingabe | Benutzer: Master`.*  
*Mit < und > können Sie WTU-Master wählen und `Enter` drücken.*  
*Ohne aktivierte WTU-Funktion zeigt das Display `Code-Eingabe`, `Master`, gegebenenfalls `0123456789` und `Code:`.*
6. Geben Sie die Ziffern des (WTU-)Mastercodes mit < und > und `Enter` ein.  
*Das Display zeigt `(WTU-)Mastercode | Bitte warten`.*  
*und danach `Fingerprint | Benutzer: (WTU-)Master`.*
7. Wählen Sie mit < oder > die Benutzernummer und Taste `Enter`.  
*Das Display zeigt `Benutzer: | Nr. und re. Zeigefinger`.*
8. Wählen Sie mit < oder > einen Finger und Taste `Enter`.  
*Das Display zeigt `Benutzer: | Nr. und <<SCAN >>`. So lange die Klammern animiert sind, kann der Finger aufgelegt werden.*
9. Legen Sie den Finger in die Fingerführung und ziehen Sie ihn nach unten. Wiederholen Sie dies mindestens zweimal.

Das Display zeigt nach jedem erfolgreichen Scannen ein "x" hinter Benutzer: | Nr. als Zeichen, den Finger wieder aufzulegen.

Das Display zeigt schlechtes Bild, wenn die Qualität den eingestellten Mindestanforderungen nicht entspricht.

Es zeigt Kein Bild, wenn der Sensor keinen Finger registriert hat.  
Es zeigt Keine Passung, wenn der Sensor zu unterschiedliche Merkmale registriert hat.

Nach einem vierten fehlerhaften Scan wird die Erzeugung der Referenzdaten abgebrochen und muss neu gestartet werden.

10. Scannen Sie erneut, falls Fehlermeldungen angezeigt werden.

Das Display zeigt Minu:XX Quali:XX | Bitte warten, wenn die Bildqualität den gesetzten Mindestanforderungen entspricht.

Danach wird Benutzer: | Gespeichert angezeigt.  
sowie weiterer Finger? | \*=JA \*=NEIN.

11. Wählen Sie mit < oder > Ja oder Nein und Taste Enter.

Wie oben beschrieben werden gegebenenfalls die Meldungen zur Wahl und zum Scannen eines weiteren Fingers angezeigt.

Das Display zeigt Alarmfinger | kein Finger, wenn der Sensor keinen Finger registriert hat.

12. Melden Sie mit < oder > und Enter einen Finger als Alarmfinger an oder wählen Sie kein Finger.

Mit dem „Alarmfinger“ wird bei einer Öffnung Stiller Alarm ausgelöst.  
Das Display zeigt Fingerprint | Gespeichert. Danach zeigt das Display Weiterer Code? | \*=JA | \*=Nein.

13. Wählen Sie \*=JA, wenn Sie Fingerprint-Code für weitere Benutzer anmelden wollen und wiederholen Sie jeweils die Schritte 8 bis 13.  
Wählen Sie \*=Nein, wenn Sie das Anmelden beenden wollen.

Sie haben erfolgreich Fingerprint-Code angemeldet.

### 3.11.16 Fingerprint-Code abmelden

Schlossmaster und gegebenenfalls WTU-Master eines Schlosses können Fingerprint-Codes für die Öffnung abmelden.

Achten Sie darauf, keine für das Scharf- / Unscharf-Schalten einer optionalen Einbruchmeldeanlage nötigen Fingerprint-Codes abzumelden.

1. Wählen Sie Menü Einstellungen | Fingerprint.

Genauere Anleitung siehe obige Beschreibung „Fingerprint-Code anmelden“, Schritte 1-3.

Das Display zeigt Fingerprint | Scan Test.

2. Wählen Sie mit < und > Abmelden und bestätigen Sie mit Enter.

Das Display zeigt gegebenenfalls Code-Eingabe | Schloss 1.

3. Wählen Sie mit < und > gegebenenfalls das Schloss und Enter.

Das Display zeigt bei WTU-Betrieb:

Code-Eingabe | Benutzer: Master.



Mit < und > können Sie WTU-Master wählen und Enter drücken.

Ohne aktivierte WTU-Funktion zeigt das Display Code-Eingabe, Master, gegebenenfalls 0123456789 und Code:.

4. Geben Sie die Ziffern des (WTU-)Mastercodes mit < und > und Enter ein.

Das Display zeigt Bitte warten und Fingerprint | Benutzer: (WTU-)Master.

5. Wählen Sie mit < oder > die Benutzernummer und Taste Enter.

Das Display zeigt Benutzer Nr. und alle Finger, falls Daten vorhanden oder Benutzer Nr. | OK, falls keine Fingerprint-Daten vorhanden sind.

6. Wählen Sie Enter, wenn Sie alle Fingerprint-Daten abmelden wollen oder wählen Sie mit < oder > einen Finger und Enter. Falls Sie nicht abmelden wollen, wählen Sie Taste Clear.

Das Display zeigt Fingerprint | Geloescht, wenn Daten eines Fingers abgemeldet wurden.

Das Display zeigt Benutzer: Nr. | kein Fingerprint und Geloescht, wenn alle Fingerprint-Daten eines Benutzers abgemeldet wurden.

Das Display zeigt Abmelden | Alarmfinger, wenn ein Alarmfinger abgemeldet wird, und Alarmfinger neu | kein Finger. Mit < oder > können Sie einen anderen Finger wählen und ihn mit Enter zum Alarmfinger machen.

Das Display zeigt Weiterer Code? | \*=JA | \*=Nein.

7. Wählen Sie \*=JA, wenn Sie Fingerprint-Code weiterer Benutzer abmelden wollen und wiederholen Sie die Schritte 5 und 6. Wählen Sie \*=Nein, wenn Sie das Abmelden beenden wollen.

Sie haben erfolgreich Fingerprint-Daten abgemeldet.

### 3.11.17 Fingerprint: Benutzer-Anzeige

Der Schlossmaster und gegebenenfalls der WTU-Master eines Schlosses können an diesem Schloss angemeldete Fingerprint-Codes anzeigen.

1. Wählen Sie Menü Einstellungen | Fingerprint.

Genauere Anleitung siehe obige Beschreibung „Fingerprint-Code anmelden“, Schritte 1-3.

Das Display zeigt Fingerprint | Scan Test.

2. Wählen Sie mit < oder > Benutzer-Anzeige und Enter.

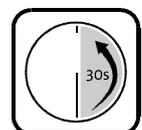
Das Display zeigt Code-Eingabe | Schloss 1.

3. Wählen Sie mit < und > gegebenenfalls das Schloss und Enter.

Das Display zeigt bei WTU-Betrieb:

Code-Eingabe | Benutzer: Master.

Mit < und > können Sie WTU-Master wählen und Enter drücken.



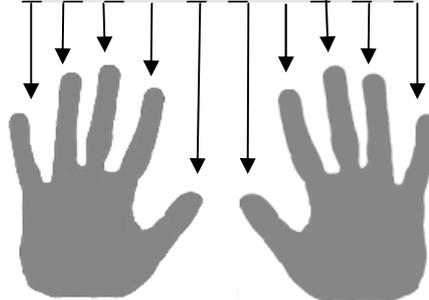
Ohne aktivierte WTU-Funktion zeigt das Display *Code-Eingabe, Master, gegebenenfalls 0123456789* und *Code:*.

4. Wählen Sie die Ziffern des (WTU-)Mastercodes mit < und > und bestätigen Sie jeweils mit Enter.

Das Display zeigt *Bitte warten, (WTU-)Master oder Benutzer Nr.*

5. Blättern Sie mit < oder > durch die Benutzer-Einträge.

Das Display zeigt *Benutzer: | Nr..*  
und beispielsweise



Jeder Unterstrich entspricht einem Finger.

\* (Sternchen / Asterisk): = angemeldeter Finger

a : = Alarmfinger

6. Beenden Sie die Anzeige mit Taste Enter oder Taste Clear.

Das Display zeigt *Fingerprint | Benutzer-Anzeige.*

Sie haben erfolgreich Benutzerdaten zu Fingerprint-Code angezeigt.

## 3.12 Service

Einige Untermenüs des Menüs **Service** sind bereits im vorigen Abschnitt „Benutzer verwalten“ beschrieben, da mit ihnen wichtige Einstellungen für Fingerprint-Code von Benutzern gemacht werden können.

### 3.12.1 System bei Netzausfall mit Spannung versorgen

Batteriehersteller bieten passende 9 Volt Blockbatterien unter den Bezeichnungen 6LR61 (Alkali-Mangan), 6F22 (Zink-Kohle), 6AM6, 522 an.

**Sie benötigen** ein Adapterkabel, eine aufgeladene 9 Volt Blockbatterie und Zugriff auf die Bedieneinheit.

1. Verbinden Sie Adapterkabel und Batterie. Achten Sie dabei auf die unterschiedliche Größe der Steckverbindungen von Plus- und Minuspol der Batterie.
2. Stecken Sie den Mini DC-Stecker des Adapterkabels in die Buchse auf der Unterseite der Bedieneinheit FlatControl.

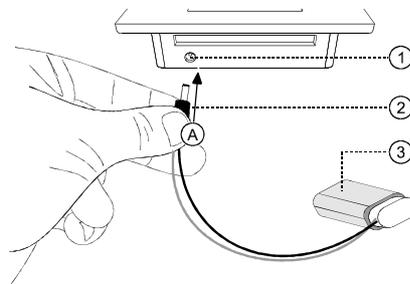


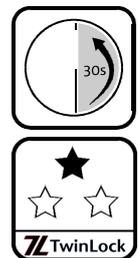
Abbildung 23 Adapterkabel mit Bedieneinheit verbinden

- 1) Buchse für Spannungsversorgung bei Netzausfall
- 2) MiniDC-Stecker des Adapterkabels
- 3) 9 Volt Blockbatterie

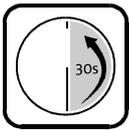
Sie versorgen das System erfolgreich mit Spannung.

### 3.12.2 Status / Info des Systems anzeigen

1. Drücken Sie kurz **Enter**.  
*Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit.*
2. Wählen Sie mit den Tasten **<** und **>** **Status / Info** und **Enter**.  
*Nacheinander werden angezeigt:*
  - „System check“ (während das System geprüft wird)
  - VdS-Klasse des Schlosssystems (optional)
  - Zustand der Schlösser (auf / Mitte / zu)
  - Zustand des Systems (entsperrt / teilgesperrt / gesichert)
  - Zustand einer optionalen Einbruchmeldeanlage (scharf / unscharf)
  - Version der Software der Bedieneinheit
  - Version der Software und der Engine des Fingerprintmoduls
  - Version der Software des Schlosses / der Schlösser
  - sowie gegebenenfalls die Softwareversion von TwinAlarm / TwinXT.



Sie haben Statusinformationen zu Komponenten erfolgreich angezeigt.



### 3.12.3 Service Reset

Der Systemmanager kann mit Menü `Reset` die aktuellen Einstellungen löschen und die Werkseinstellungen wiederherstellen.

#### Vorsicht

**Durch einen Reset werden für das System spezifische, auch Hardware- und Benutzer-Einstellungen gelöscht. Danach kann gegebenenfalls nur der Schlossmaster öffnen.**

Speichern Sie die aktuelle Konfiguration mit der optionalen Software TwinComm USB oder lassen Sie sie speichern, bevor Sie einen Reset durchführen.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit Taste `<` oder Taste `>` `Service` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Service | Reset`.*
3. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Code-Eingabe und Systemmanager, 0123456789, und Code :`.*
4. Wählen Sie mit `<` und `>` die Ziffern des Systemmanagercodes und bestätigen Sie jede Ziffer mit `Enter`.  
*Siehe auch den Abschnitt „PIN-Code eingeben“ in diesem Kapitel.  
Das Display zeigt `Systemmanager | Bitte warten, danach Reset und Finger loeschen? | *=JA *=Nein`.*  
*So können Sie alle im System gespeicherten Fingerprint-Codes löschen. Zum selektiven Löschen von Fingerprint-Daten siehe Abschnitt „Fingerprint-Code löschen“ in diesem Kapitel.*
5. Bestätigen Sie `*=Nein` mit `Enter` oder wählen Sie mit `<` oder `>` `*=Ja` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Systemmanager | Bitte warten, danach INITIALISIERUNG | EEPROM LOESCHEN, OK, TwinLock und System Setup`.*
6. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Sprache | 1 Deutsch`. Mit `<` oder `>` können Sie eine andere Sprache wählen.*
7. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Deutsch | Gespeichert und danach System - Setup | Neues System`.*
8. Wählen Sie mit `<` oder `>` `Terminal - Wechsel` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `System - Setup | Anzahl DMS : 1`.*

9. Wählen Sie mit < oder > die Anzahl der Schlösser im System und bestätigen Sie mit **Enter**.  
*Das Display zeigt Seriennummer | Schloss 1 und Code-Eingabe | Systemmanager. und Code:.*
10. Geben Sie den Systemmanagercode erneut ein.  
*Das Display zeigt Seriennummer | Bitte warten.  
Die Seriennummer der Bedieneinheit wird im Schloss gespeichert.  
Das Display zeigt Seriennummer | Gespeichert.  
Bei mehreren Schlössern im System zeigt das Display Seriennummer | Schloss 2 und Code-Eingabe | Manager und Code:.*
11. Geben Sie gegebenenfalls den Managercode des Schlosses ein.  
*Werkseingestellt entspricht dieser dem Systemmanagercode.  
Das Display zeigt Seriennummer | Bitte warten.  
Die Seriennummer der Bedieneinheit wird im Schloss gespeichert.  
Das Display zeigt Seriennummer | Gespeichert.  
Danach zeigt das Display Datum/Uhrzeit und Code-Eingabe | Systemmanager und Code:.*
12. Wählen Sie die Ziffern des Systemmanagercodes.  
*Nach der Eingabe werden System-Uhrzeit und Datum angezeigt.*
13. Drücken Sie die Taste **Enter**, um Uhrzeit und Datum einzustellen.  
*Wenn Sie 2x **Clear** drücken, behält das System die bisherige Zeiteinstellung und das Display zeigt die in Schritt 16 beschriebene Anzeige.  
Achten Sie auf eine korrekte Zeiteinstellung.  
Im Display blinkt die erste Ziffer der aktuell eingestellten Uhrzeit.*
14. Geben Sie die aktuelle Uhrzeit mit < und > und **Enter** oder mit den Zifferntasten ein.  
*Im Display blinkt der Cursor vor dem eingestellten Wochentag.*
15. Wählen Sie mit < und > die beiden ersten Buchstaben des aktuellen Wochentags und bestätigen Sie mit **Enter**.  
*Im Display blinkt der aktuell eingestellte Tag.*
16. Geben Sie Tag, Monat und Jahr ein.  
*Das Display zeigt Datum/Uhrzeit | Gespeichert,  
Schlosssystem | Angemeldet und  
TwinLock BioPIN | 11.02.10.  
Siehe auch Abschnitt „Datum und Zeit einstellen“.*

Sie haben die bisherigen Einstellungen erfolgreich gelöscht und die Werkseinstellungen wiederhergestellt.

### 3.12.4 Motor-Service



Schlossmaster können mit Menü `Motor-Service` den Schlossriegel schrittweise ein- und ausfahren.

#### Hinweis

Falls mit der optionalen Software TwinComm USB „automatisches Schließen“ eingestellt wurde, schließt das System das Schloss eine Minute nach der Ausführung der hier beschriebenen Motorschritte.

Falls nicht, bleibt der Schlossriegel in der Position, in die er mit dem letzten Motorschritt gefahren wird.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Tasten `<` oder `>` `Service` und Taste `Enter`.  
*Das Display zeigt `Service | Reset`.*
3. Wählen Sie mit `<` oder `>` `Motor-Service` und wieder `Enter`.  
*Das Display zeigt `Service | Motor-Service`.*
4. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Code-Eingabe | Schloss 01`.*
5. Wählen Sie mit `<` oder `>` gegebenenfalls das Schloss, dessen Riegel Sie schrittweise bewegen wollen, und Taste `Enter`.  
*Das Display zeigt `Code-Eingabe, Master, 0123456789, Master und Code :.`*
6. Geben Sie mit `<` und `>` und `Enter` die Ziffern des Mastercodes ein.  
*Das Display zeigt `Motor-Service | <== Auf | Zu ==>`.*
7. Wählen Sie mit `<` oder `>` `Auf` oder `Zu`.  
*Das Display zeigt `Bitte warten. Der Schlossriegel fährt einen Schritt auf oder zu und das Display zeigt Schritt OK`.*
8. Wiederholen Sie Schritt 7 beliebig oft, wenn gewünscht, auch in Gegenrichtung.

Sie haben den Schlossriegel erfolgreich schrittweise ein- / ausgefahren.

### 3.12.5 Schloss anmelden

#### Vorsicht



**Verletzungsgefahr für Personen, die nicht fachgerecht montieren sowie Gefahr der Beschädigung und des Funktionsausfalls von System TwinLock.**

Stellen Sie sicher, dass das System von geschulten Fachkräften montiert und in Betrieb genommen wird.



Mit dem Menü `Service | Schloss anmelden` können nur neue, noch nicht adressierte Schlösser im System angemeldet werden - beim Auswechseln eines Schlosses (`Schloss wechseln`) oder beim Erweitern des Systems um ein Schloss (`Schloss neu`).

Zum Anmelden von Schlössern, die bereits zuvor adressiert worden sind, gehen Sie bitte vor wie beim Wechseln der Bedieneinheit. Siehe Beschreibung „Service Reset“ in diesem Kapitel und die Montageanleitung.

**Take** ein neues, noch nicht adressiertes Schloss

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Tasten < oder > `Service` und bestätigen Sie mit `Enter`.  
*Das Display zeigt `Service | Reset`.*
3. Wählen Sie mit < oder > `Schloss anmelden` und Taste `Enter`.  
*Das Display zeigt `Service | Schloss anmelden`.*
4. Bestätigen Sie mit `Enter`.  
*Das Display zeigt `Schloss anmelden | Schloss neu`.*

#### 3.12.5.1 Schloss neu

ist die Fortsetzung von „Schloss anmelden“, falls Sie ein zusätzliches neues Schloss anmelden. Siehe auch „Schloss wechseln“.

5. Bestätigen Sie `Schloss neu` mit `Enter`.  
*Das Display zeigt `Code-Eingabe und Systemmanager, 0123456789, und Code:.`*
6. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt `Bitte warten | Schloss neu und Schloss 2/3`. Das Display zeigt `! Buskabel ein !`. Die angezeigte Schlossnummer ist die, die das neue Schloss im System bekommt (Anzahl der vorhandenen Schlösser + 1).*
7. Wenn Sie das Kabel verbunden haben, bestätigen Sie mit `Enter`.  
*Das Display zeigt `Seriennummer | Bitte warten`. Die Seriennummer der Bedieneinheit wird im Schloss gespeichert. Das Display zeigt `Seriennummer | Gespeichert`.  
*Das Display zeigt `Com-Fehler | Setup-Fehler`, wenn das „neue“ Schloss schon einmal adressiert wurde.**

*Das Display zeigt Datum/Uhrzeit | Gespeichert,  
Schloss | Angemeldet und  
TwinLock BioPIN | 11.02.10.*

Sie haben das neue Schloss erfolgreich angemeldet.

### 3.12.5.2 Schloss wechseln

ist die Fortsetzung von „Schloss anmelden“, falls Sie ein Schloss auswechseln.

1. Führen Sie Schritte 1-4 der Anleitung „Schloss anmelden“ aus.  
*Das Display zeigt Schloss anmelden | Schloss neu.*
2. Wählen Sie mit < oder > Schloss wechseln und Enter.  
*Das Display zeigt Schloss wechseln und Schloss 1<.*
3. Wählen Sie mit < oder > gegebenenfalls das zu ersetzende Schloss und bestätigen Sie mit Enter.  
*Das Display zeigt ! Buskabel ein !.*
4. Wenn Sie das Kabel verbunden haben, bestätigen Sie mit Enter.  
*Das Display zeigt Com-Fehler | Setup-Fehler, wenn das „neue“ Schloss schon einmal adressiert wurde.  
Das Display zeigt Seriennummer | Schloss 2/3 und  
Code-Eingabe | Systemmanager, 0123456789 und  
Code:.*
5. Geben Sie den Systemmanagercode ein.  
*Das Display zeigt Seriennummer | Bitte warten.  
Die Seriennummer der Bedieneinheit wird im Schloss gespeichert.  
Das Display zeigt Seriennummer | Gespeichert.*

*Das Display zeigt Datum/Uhrzeit | Gespeichert,  
Schlosssystem | Angemeldet und  
TwinLock BioPIN | 11.02.10.*

Sie haben das neue Schloss erfolgreich angemeldet.

### 3.12.6 System bei defektem Riegelwerkskontakt schließen

Wenn Sie eine Schaltung für einen Riegelwerkskontakt (TwinXT oder TwinAlarm) angeschlossen haben, können Sie das System auch bei defektem Kontakt einmalig verschließen, indem Sie die im Folgenden beschriebenen Schritte ausführen.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Tasten < oder > **Service** und bestätigen Sie mit **Enter**.  
*Das Display zeigt **Service | Reset**.*
3. Wählen Sie mit < und > **1x Riegelwerk** und danach **Enter**.  
*Sie befinden sich im Menü **1x Riegelwerk**.  
Das Display zeigt **1x Riegelwerk | \*=Ja \*=Nein**.*
4. Wählen Sie mit < und > **Ja** und danach **Enter**.  
*Das Display zeigt **1x Riegelwerk | Gespeichert**. Sie können das System nun bei defektem Schalter einmalig schließen.*
5. Schließen Sie alle Schlösser im System.  
*Siehe auch die Beschreibungen „Schloss...schließen“.  
Das System ist gesichert.*

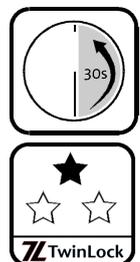
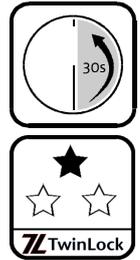
Sie haben das System trotz defektem Kontakt erfolgreich verschlossen.

### 3.12.7 Fingerprint Status / Info

Benutzer können mit dem Menü **Fingerprint | Status / Info** die Version von Software und Engine des Fingerprint-Moduls anzeigen.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).  
*Siehe auch „Der Systemstatus“ am Anfang dieses Kapitels.*
2. Wählen Sie mit den Tasten < und > **Service** und Taste **Enter**.  
*Das Display zeigt **Service | Reset**.*
3. Wählen Sie mit < oder > **Fingerprint** und **Enter**.  
*Das Display zeigt **Fingerprint | Status / Info**.*
4. Bestätigen Sie mit Taste **Enter**.  
*Die Version der Software und der Engine des Fingerprintmoduls werden nacheinander angezeigt.*

Sie haben Informationen zum Fingerprint-Modul erfolgreich angezeigt.



### 3.12.8 Fingerprint: Temperatur anzeigen / ändern



Der Systemmanager kann die Temperatur anzeigen, auf die der Sensor geheizt wird, und sie gegebenenfalls ändern.

Wertebereich: 18 – 50, voreingestellter Wert: 40° Celsius.

#### Hinweis

**Gefahr von Fingerabdruck-Scans minderer Qualität.**  
Die richtige Temperatur ist wichtig für die gute Qualität der Fingerprint-Aufnahmen. Testen Sie die Qualität nach jeder Temperaturänderung.

1. Wählen Sie Menü `Service | Fingerprint`.  
*Genauere Anleitung siehe obige Beschreibung „Fingerprint Status / Info“, Schritte 1-3.*  
*Das Display zeigt `Fingerprint | Status / Info`.*
  2. Wählen Sie mit `<` oder `>` `Temperatur` und Taste `Enter`.  
*Das Display zeigt `Code-Eingabe, Systemmanager, 0123456789` und `Code :.`*
  3. Geben Sie mit `<` und `>` und `Enter` die Ziffern des Codes ein.  
*Das Display zeigt `Temperatur | 40° <`.*
  4. Vergrößern / verringern Sie den Wert mit `<` oder `>` und `Enter`  
*Das Display zeigt `Temperatur | Gespeichert`.*
- Sie haben die Temperatur erfolgreich angezeigt / geändert.

## 4 Reinigung

#### Vorsicht

**Gefahr von Kurzschluss der elektronischen Komponenten durch Kontakt mit Wasser.**  
**Gefahr der Beschädigung des Systems**  
Beachten Sie die Ausführungen zur Reinigung.

Reinigen Sie die Eingabeeinheit mit **sehr wenig Wasser** oder einer milden Seifenlösung. Verwenden Sie dazu ein feuchtes, weiches, sauberes und fusselfreies Tuch. Verwenden Sie keine anderen Mittel.

Reinigen Sie alle anderen Komponenten des Systems TwinLock nur, wenn Ihnen dies unumgänglich erscheint. Benutzen Sie ausschließlich ein trockenes, weiches, sauberes und fusselfreies Tuch.

Wischen Sie über die Oberfläche, ohne großen Druck auszuüben.

## 5 Störungsabhilfe

### 5.1 Fehlermeldungen

Siehe auch Kapitel Bedienung, Abschnitt „Meldungen beim Einlesen der Konfiguration“.

#### Alarm-Codefehler

- ! Fehler beim Speichern eines Codes in TwinAlarm.
- ✓ *Wiederholen Sie den Speicherungsversuch. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Meldung wiederholt angezeigt wird.*

#### Autorisierung

- ! Codekarte Fingerprint Keine Freigabe Öffnen PIN-Code Schließen&Code Service Unscharfschalten
- ! Benutzer ist für den gewählten Vorgang nicht autorisiert. Nach einer Sekunde zeigt das Display, welche Art der Autorisierung dem Benutzer in der Benutzermatrix von TwinComm nicht verliehen wurde (siehe unten, „Codekarte“, „Fingerprint“...).
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, damit er die Autorisierung in der Benutzerverwaltung von TwinComm USB ergänzt.*

#### Codekarte

- ! Benutzer darf keine Codekarte benutzen.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

#### Fingerprint

- ! Benutzer darf keinen Fingerprint-Code eingeben.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

#### Keine Freigabe

- ! Benutzer hat keine Freigabe für die Eingabe von Codes.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

#### Öffnen

- ! Benutzer darf kein Schloss öffnen.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

#### PIN-Code

- ! Benutzer darf keinen PIN-Code eingeben.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

#### Schließen&Code

- ! Benutzer darf Schlösser mit der Eingabe von PIN-Code nicht schließen.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

#### Service

- ! Benutzer darf Protokoll nicht exportieren.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

**Unscharfschalten**

- ! Benutzer darf Einbruchmeldeanlage nicht „unscharf“ schalten. Behebung siehe oben.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

**Bio Fehler**

- ! Fehler beim Ausführen eines Fingerprint-Befehls.
- ✓ *Wiederholen Sie den Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung abermals angezeigt wird.*

**Bus A/B empfangen****Bus A/B senden**

- ! Ein Schloss TwinLock lässt sich auf Bus A / Bus B nicht mehr ansprechen. Eventuell ist ein Kabel nicht korrekt eingesteckt oder defekt.
- ✓ *Setzen Sie sich bitte mit dem Support in Verbindung.*

**Codes identisch!**

- ! Ein neuer Code entspricht dem bisherigen, zu ändernden.
- ✓ *Melden Sie einen anderen Code an.*

**COM-Fehler****Fehler Antwort**

- ! In der Kommunikation zwischen der Bedieneinheit und einer anderen Komponente (z.B. einem Schloss) ist ein Fehler aufgetreten. Die Bedieneinheit hat einen nicht vorgesehenen Befehl empfangen.
- ✓ *Softwarefehler. Setzen Sie sich bitte mit dem Support in Verbindung.*

**COM-Fehler****Bus A/B senden Bus A/B empfangen**

- ! Ein Schloss TwinLock lässt sich auf Bus A / Bus B nicht mehr ansprechen. Eventuell ist ein Kabel nicht korrekt eingesteckt oder defekt.
- ✓ *Setzen Sie sich bitte mit dem Support in Verbindung.*

**COM-Fehler Bio**

- ! In der Kommunikation mit dem Fingerprint-Modul ist ein Fehler aufgetreten.
- ✓ *Wiederholen Sie den Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

**EEPROMfehler AB / DMS / TM**

- ! Fehler beim Lesen vom / Schreiben ins EEPROM der Bussysteme (AB)/ von Schloss TwinLock (DMS) / der Bedieneinheit (TM für Terminal).
- ✓ *Wiederholen Sie den Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

**Eingabefehler**

- ! Falsche / ungültige Eingabe. Möglicherweise wurde ein PIN-Code nicht korrekt eingegeben oder bei gewählter Option „Parallelcode“ oder „Codeverknüpfung“ haben nicht zwei verschiedene Benutzer ihren Code eingegeben, sondern nur einer.
- ✓ *Wiederholen Sie den Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

**Falscher Code | Sperrzeit**

- ! Beim Versuch, ein Schloss zu öffnen, wurde viermal ein falscher Code eingegeben / mehr als fünfmal ein falscher Finger gescannt, wodurch eine Sperrzeit aktiviert wurde. Die Sperrzeit verlängert sich bei jeder weiteren Falscheingabe um eine Minute.
- ✓ *Warten Sie ab, bis die Sperrzeit abgelaufen ist, und geben Sie den Code korrekt ein.*
- ✓ *Setzen Sie sich bitte mit Ihrem Systemadministrator / dem Support in Verbindung, wenn Sie nicht im Besitz des korrekten Codes sind.*

**Falsche Karte**

- ! Ein Benutzer hat eine Karte des falschen Typs in die Bedieneinheit gesteckt, beispielsweise eine Sprach- statt einer Konfigurationskarte.
- ✓ *Wählen Sie die passende Karte. Setzen Sie sich bitte mit dem Support in Verbindung, wenn Sie nicht im Besitz der geeigneten Karte sind.*

**Fehler DMS Nr.**

- ! Das Schloss TwinLock mit der angegebenen Nummer meldet einen allgemeinen Fehler.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung.*

**Fehler Karte**

- ! In der Kommunikation zwischen der Bedieneinheit und einer Chipkarte ist ein Fehler aufgetreten.
- ✓ *Wiederholen Sie den Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

**Fehler Motor A****Fehler Motor B**

- ! Der Riegel des Schlosses TwinLock kann nicht über Bus A / Bus B bewegt werden.  
Eventuell ist die Platine oder der Motor des Schlosses defekt oder der Riegel erreicht die Endposition nicht.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung.*

**Fehler Scharf!**

- ! TwinAlarm meldet Fehler beim Scharfschalten der Einbruchmeldeanlage (EMA): EMA kann nicht scharf geschaltet werden, weil das System nicht gesichert ist.
- ✓ *Schließen Sie die Schlösser und wiederholen Sie den Vorgang.*

**Fehler: Seriennr.**

- ! Die Seriennummern in der Bedieneinheit und im Schloss sind nicht identisch.
- ✓ *Diese Meldung wird angezeigt, wenn Bedieneinheit oder Schloss nicht vorschriftsmäßig gewechselt wurden. Sabotage ist möglich. Bitte setzen Sie sich mit den für die Sicherheit zuständigen Personen in Verbindung.*

**Fehler TwinAlarm**

- ! In der Kommunikation mit der Schalteinrichtung TwinAlarm ist ein Fehler aufgetreten.
- ✓ *Wiederholen Sie den Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

**Fehler Unscharf!**

- ! TwinAlarm meldet Fehler beim Unscharf-Schalten der Einbruchmeldeanlage (EMA): EMA kann nicht unscharf geschaltet werden, weil von ihr keine Quittierung der Unscharf-Schaltung erfolgt.
- ✓ *Setzen Sie sich bitte mit dem Alarmtechniker / Support in Verbindung, um die Verbindung zur EMA überprüfen zu lassen.*

**Finger Timeout**

- ! Zeitspanne für das Scannen eines Fingers ist abgelaufen, ohne dass ein Finger über den Sensor gezogen wurde.
- ✓ *Wiederholen Sie den Vorgang und ziehen Sie einen Finger über den Sensor vorne an der Bedieneinheit.*

**Kein Bild**

- ! Zeit für das Scannen eines Fingers ist abgelaufen, ohne dass der Sensor einen Fingerabdruck erkannt hat.
- ✓ *Wiederholen Sie den Scan-Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

**Keine Freigabe**

- ! Keine Öffnung möglich. Schloss ist über den Eingang FREIGABE von TwinXT / TwinAlarm nicht freigegeben.
- ✓ *Prüfen Sie, ob TwinXT / TwinAlarm richtig angeschlossen ist und ob das Schloss berechtigterweise gesperrt ist. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Meldung weiterhin angezeigt wird.*

**Keine Karte**

- ! Es wurde keine Chipkarte in die Bedieneinheit eingelegt.
- ✓ *Legen Sie eine Chipkarte in das Kartenfach unten in der Bedieneinheit.*

**Keine Passung!**

- ! Beim Anmelden von Fingerprint-Code / bei Scan Test ist nicht wie vorgesehen mehrmals der gleiche Finger über den Sensor gezogen worden.
- ✓ *Ziehen Sie mehrmals ein- und denselben Finger über den Sensor, bis der Fingerabdruck registriert ist.*

**Keine TwinAlarm!**

- ! Die Schalteinrichtung TwinAlarm ist deaktiviert.
- ✓ *Stellen Sie sicher, dass die Schalteinrichtung richtig angeschlossen und initialisiert ist.*

**Kein Fingerprint**

- ! Im Schloss ist für den Benutzer, bei dem die Meldung angezeigt wird, kein Fingerabdruck gespeichert.
- ✓ *Informieren Sie Ihren Systemadministrator, wenn ein Fingerabdruck im Schloss gespeichert werden soll.*

**! Manipulation !**

- ! Ein Code wurde mehr als dreimal falsch eingegeben oder mehr als fünfmal wurde ein falscher Finger gescannt.
- ✓ *Kontrollieren Sie Sie im Protokoll, welcher Benutzer dies verursacht hat.*

**Motorfehler**

- ! Der Riegel des Schlosses kann nicht bewegt werden. Eventuell ist die Platine oder der Motor des Schlosses defekt oder der Riegel erreicht die Endposition wegen eines mechanischen Problems nicht.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung.*

**Nicht erkannt!**

- ! Gescannter Fingerabdruck wurde nicht erkannt.
- ✓ *Wiederholen Sie den Scan-Vorgang mit anderer Geschwindigkeit und anderem Druck. Wählen Sie einen anderen Finger, wenn möglich. Prüfen Sie die eingestellte Sicherheitsstufe und ändern Sie sie gegebenenfalls.*
- ✓ *Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

**RTC-Fehler**

- ! Die Uhr (Real Time Clock) der Bedieneinheit funktioniert nicht korrekt.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

**schlechtes Bild**

- ! Gescannter Fingerabdruck erfüllt die eingestellten Mindestanforderungen bezüglich der Anzahl der Minutien und / oder der Qualität nicht.
- ✓ *Wiederholen Sie den Scan-Vorgang mit anderer Geschwindigkeit und anderem Druck. Wählen Sie einen anderen Finger, wenn möglich. Prüfen Sie die eingestellten Anforderungen (Anzahl Minutien und Bildqualität).*
- ✓ *Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

**Schloss Mitte**

- ! Schlossriegel ist weder geschlossen noch geöffnet, sondern in Mittelposition.
- ✓ *Prüfen Sie, ob sich ein Hindernis vor dem Schlossriegel befindet, welches das Ausfahren des Riegels behindert.*
- ✓ *Prüfen Sie, ob sich das Schloss öffnen / schließen lässt. Wenn nicht, setzen Sie sich bitte mit dem Support in Verbindung.*

**Schlosssystem**

- ! Es wurde versucht, einen Code abzumelden, ohne den das System nicht mehr zu öffnen wäre.
- ✓ *Deaktivieren Sie gegebenenfalls „Codeverknüpfung“ oder „Parallelcode“ oder ordnen Sie die Öffnungsberechtigung für das Schloss weiteren Benutzern zu, bevor Sie den Code abmelden.*

**Sondertage**

- ! Das aktuelle Datum fällt auf einen „Sondertag“, an dem das Öffnen des Schlosses nicht gestattet ist.
- ✓ *Warten Sie ab, bis der „Sondertag“ vorbei ist.*
- ✓ *Öffnen Sie Ihr Schloss (mit Autorisierung zur Schnellöffnung).*
- ✓ *Prüfen Sie das an der Eingabeeinheit FlatControl eingestellte Datum und korrigieren Sie es gegebenenfalls.*

**Sperrzeit**

- ! Beim Versuch, das Schloss zu öffnen,
  - wurde mehr als dreimal ein falscher Code eingegeben
  - wurde eine Sperrzeit von 90 Minuten aktiviert, weil mindestens ein Schloss während eines Terminalwechsels geschlossen war
  - wurde versucht, das Schloss während eines Sperrzeitraums zu öffnen.
- ✓ *Warten Sie ab, bis die Sperrzeit abgelaufen ist und geben Sie den korrekten Code ein.*

**stromlos**

- ! Das System war getrennt von der Stromversorgung. Nach der Öffnung des Schlosses wird die Meldung nicht mehr angezeigt.
- ✓ *Überprüfen sie das Protokoll und prüfen Sie, ob Datum und Uhrzeit richtig eingestellt sind. Lassen Sie vom für die Sicherheit zuständigen Personal prüfen, ob am System manipuliert wurde.*

**Terminal-Wechsel**

- ! Bedieneinheit wurde gewechselt oder zurückgesetzt. Nach der Öffnung des Schlosses wird die Meldung nicht mehr angezeigt.
- ✓ *Diese Meldung erfolgt beim ersten Öffnungs-/Schliessvorgang nach dem Zurücksetzen (Reset) oder nach dem Wechsel der Bedieneinheit. Sie erfordert keine Maßnahmen.*
- ✓ *Wenn die Meldung unerwartet erfolgt, könnte es sich um einen Manipulationsversuch handeln. Setzen Sie sich in diesem Fall bitte mit dem für die Sicherheit zuständigen Personal in Verbindung.*

**trivialer Code**

- ! Ein Benutzer hat Code angemeldet, der aus einer Folge auf -, absteigender – oder gleicher Ziffern besteht.
- ✓ *Aus Sicherheitsgründen kann eingestellt werden, dass solche Codes nicht erlaubt sind. Geben Sie einen anderen Code ein.*

**ungültige Karte**

- ! Die Codekarte ist ungültig.
- ✓ *Prüfen Sie, ob Sie eine gültige Karte haben. Setzen Sie sich bitte mit dem Systemadministrator / dem Support in Verbindung, wenn Sie keine gültige Karte besitzen.*

**Unscharf-Code??**

- ! TwinAlarm kann die angeschlossene Einbruchmeldeanlage (EMA) nicht scharf schalten, weil noch kein Code zum Unscharf-Schalten angemeldet wurde.
- ✓ *Aktivieren Sie gegebenenfalls TwinAlarm und melden Sie einen Code zum Unscharf-Schalten an.*

**War Neustart oder | stromlos**

- ! Das System war getrennt von der Stromversorgung.
- ✓ *Prüfen Sie, ob am System manipuliert wurde und ob Datum und Uhrzeit richtig eingestellt sind.*

**Wochenprogramm**

- ! Die aktuelle Uhrzeit liegt nicht innerhalb eines mit der Funktion „Wochenprogramm“ definierten Zeitfensters für die Öffnung des Schlosses.
- ✓ *Warten Sie, bis das Zeitfenster für die Öffnung kommt.*
- ✓ *Lassen Sie das Schloss von einem via Benutzermatrix in TwinComm zur „Schnellöffnung“ autorisierten Benutzer öffnen.*
- ✓ *Prüfen Sie das an der Bedieneinheit eingestellte Datum und korrigieren Sie es gegebenenfalls.*

**Zeitprog. Abbruch**

- ! Statusmeldung. Die Schaltung Zeitprogramm Sperre im gesicherten Bereich Ihres Systems ist geschlossen und unterbricht alle aktiven Zeitprogramme oder ein zur „Schnellöffnung“ autorisierter Benutzer hat ein Schloss trotz aktiven Zeitprogramms geöffnet.
- ✓ *Wenn Sie nicht wünschen, dass aktive Zeitprogramme unterbrochen werden, öffnen Sie die Schaltung Zeitprogramm Sperre.*

## 6 Technische Unterstützung

INSYS MICROELECTRONICS GmbH  
Geschäftsbereich Sicherheitstechnik  
Waffnergasse 8  
93047 Regensburg, Deutschland  
Telefon: +49(0) 941 / 586 92-22  
Telefax: +49(0) 941 / 563 471  
E-Mail: [service@insys-security.de](mailto:service@insys-security.de)  
Internet: <http://www.insys-security.de>

## 7 Entsorgung

Entsorgen Sie **Plastik-, Elektronikteile und Kabel**, indem Sie sie zu einem zertifizierten Entsorgungsfachbetrieb in Ihrer Nähe bringen oder sie an diese Adresse senden:



Frankenberg Metallhandel  
Niederlassung Coburg  
Gärtnersteite 8  
D 96450 Coburg, Deutschland  
Telefon: +49(0) 9561 / 235 344  
Fax: +49(0) 9561 / 235 319  
E-Mail: [info@recycling-coburg.de](mailto:info@recycling-coburg.de)  
Internet: <http://www.recycling-coburg.de>

Senden Sie **Schlösser**, gekennzeichnet als „zur Entsorgung“, für eine ordnungsgemäße Rücknahme und Verwertung an diese Adresse:



INSYS MICROELECTRONICS GmbH  
Waffnergasse 8  
D 93047 Regensburg, Germany  
Telefon: +49(0) 941 / 586 92-22  
Fax: +49(0) 941 / 563 471  
E-Mail: [service@insys-security.de](mailto:service@insys-security.de)  
Internet: <http://www.insys-security.de>

## 8 Glossar

Bei Begriffen, die wie **Alarmcode** im Fließtext fettgedruckt sind, handelt sich um Begriffe, zu denen es eigene Einträge im Glossar gibt.

Um die Lesbarkeit nicht zu sehr zu beeinträchtigen, sind nur ausgewählte Begriffe fett gedruckt, die im jeweiligen Kontext eine wichtige Rolle spielen. Lesen Sie auch die Einträge zu diesen Begriffen.

Alle Einträge sind in alphabetischer Reihenfolge aufgeführt.

### Abmelden

PIN-Codes und Codekarten müssen vom Schlossmaster an einem Schloss angemeldet werden, damit Benutzer das Schloss mit diesen Codes öffnen können. Auch Fingerprint-Codes müssen am Schloss angemeldet werden.

Wenn der Schlossmaster einen PIN-Code / eine Codekarte an einem Schloss abmeldet, kann der zugehörige Benutzer das Schloss damit nicht öffnen.

Wenn der Schlossmaster Fingerprint-Code abmeldet, wird der entsprechende Finger am Schloss nicht mehr erkannt.

### Alarmcode (für Stillen Alarm)

Aktiviert **Stillen Alarm** und berechtigt zu den gleichen Aktionen wie der zugehörige PIN- / Fingerprint-Code (Benutzer- oder Mastercode).

**Fingerprint-Code:** „Alarmfinger“, siehe **Fingerprint**.

**PIN-Code:** Benutzer-PIN- oder Mastercode, dessen letzte Ziffer um den in der Software TwinComm gesetzten Wert für Alarmcode erhöht ist.

Ist beispielsweise die letzte Ziffer Ihres PIN-Codes 9, geben Sie als letzte Ziffer des Alarmcodes die Ziffer „9+eingetragener Wert“ ein. Wenn das Ergebnis dieser Addition zweistellig ist, übertragen Sie nur die zweite Stelle als letzte Codeziffer, beispielsweise nach  $9 + 1 = 10$  wird die letzte Codeziffer „0“.

### Anmelden

PIN-Codes und Codekarten müssen vom Schlossmaster an einem Schloss angemeldet werden, damit Benutzer das Schloss mit diesen Codes öffnen können. Fingerprint-Code muss vom Schlossmaster gemeinsam mit dem jeweiligen Benutzer angemeldet werden.

### Autorisierung

bedeutet hier das, was der **Systemmanager** für Benutzer von System TwinLock in der **Benutzermatrix** von TwinComm festlegt. Siehe auch Kapitel „Bedienung“, Abschnitt „Autorisierung von Benutzern“.

### Autorisierung zum Öffnen eines Schlosses

Ein Benutzer kann ein Schloss nur öffnen,

- wenn ihn der Systemmanager dazu autorisiert hat (siehe Kapitel „Bedienung“, Abschnitt „Benutzer autorisieren“) und
- wenn der Schlossmaster für ihn an diesem Schloss PIN-Code / Fingerprint-Code / Codekarte (passend zur Autorisierung) angemeldet hat und
- wenn aktuell kein Zeitprogramm das Öffnen unterbindet.

Optional kann System TwinLock so konfiguriert werden, dass nur zwei Personen gemeinsam oder zeitlich versetzt ein Wertbehältnis öffnen können (siehe auch **Codeverknüpfung, Parallelcode**).

**Benutzermatrix**

Registerkarte in Software TwinComm USB, auf der die Benutzerrechte festgelegt werden; siehe Kapitel „Bedienung“, Abschnitt „Benutzer autorisieren“.

**Bildqualität**

Der Wert kann benutzerspezifisch eingestellt werden im Menü Service / Fingerprint / Bildqualität.

Wertebereich: 20 - 99 (nur der untere Grenzwert kann via TwinComm USB erhöht werden)

Voreingestellter Wert: 30, sollte möglichst nicht unterschritten werden.

Der Wert für minimale Bildqualität soll **Fingerprint-Code**-Aufnahmen ausschließen, die nicht genug Informationen enthalten, um den Abdruck analysieren und die Merkmale extrahieren zu können. Ein Wert von 60 steht für hervorragende Bildqualität, viel höhere Werte sind nicht möglich.

Mögliche Gründe für geringe Qualität:

- Finger zu schnell / zu langsam über Sensor gezogen
- zu starker / zu leichter / wechselnder Druck auf den Sensor
- falsche Position des Fingers
- zu trockene, zu feuchte oder verschmutzte Finger
- kleine Verletzungen am Finger

Um ein Bild hoher Qualität zu erhalten, sollte der Finger mit konstant niedrigem Druck und durchgängiger Bewegung über den Sensor gezogen werden. Beginnen Sie mit der Fingerkuppe ganz oben in der Führung und ziehen Sie den Finger nach unten.

Nach jedem Scan-Test wird die Bildqualität auf dem Display angezeigt. Wir empfehlen, jeden Benutzer die für ihn charakteristische Bildqualität durch Scan-Tests ermitteln zu lassen und danach die bei den Benutzern mindestens erforderliche Bildqualität auf etwa 90% des zuvor ermittelten Wertes zu setzen (im Menü Service/Fingerprint/Bildqualität).

**Code**

steht hier für geheime Daten, die ein Benutzer dem System übermitteln muss, bevor er Schlösser öffnen / gegebenenfalls schließen und anderes ausführen darf. Kann in Form von PIN- / Fingerprint-Code oder via Codekarte übermittelt werden.

**Codealterung**

Gültig für PIN-Code. Einstellbar von 00-12 Monate, 00 Monate = deaktiviert

Wenn die Option aktiviert ist, wird jeder PIN-Code bei jedem Öffnungsversuch eines Schlosses auf den Zeitpunkt seiner Anmeldung geprüft. Wenn der Code vor längerer Zeit als dem eingestellten Intervall angemeldet wurde, muss der Benutzer den Code ändern.

**Code-Eingabe**

Möglich sind drei kombinierbare Arten der Code-Eingabe von Benutzern:

- Eingeben von PIN-Code
- Einlegen eines Fingers (berechtigt alleine nicht zur Schloss-Öffnung)
- Einstecken einer Codekarte.

Der Systemmanager kann jedem Benutzer alle Arten oder zwei davon oder auch nur PIN-Code oder Codekarte zuordnen. Der Benutzer darf gegebenenfalls auch

wählen (Kontrollkästchen „1 aus 3“ in Benutzermatrix). Siehe „Autorisierung zum Öffnen eines Schlosses“.

### **Codekarte**

Chipkarte TwinLock code access, wird in Kartenfach in Bedieneinheit FlatControl gelegt. Trägermedium von Code, Alternative / Ergänzung zur Eingabe von PIN-/Fingerprint-Code.

### **Codeverknüpfung (4-Augen Prinzip)**

Mit dieser Option kann das System so eingestellt werden, dass nur zwei Benutzer gemeinsam ein Schloss öffnen können (4-Augen-Prinzip). Ausgewählte Benutzer können über die Benutzermatrix in TwinComm USB dazu berechtigt werden, trotz dieser Einstellung Schlösser auch alleine öffnen zu können.

### **Echtzeituhr**

Datum und Uhrzeit werden von einer speziell gepufferten Echtzeituhr generiert und bleiben im Notfall auch trotz mehrtägiger Stromlosigkeit des Systems aktuell.

Wird die Bedieneinheit für längere Zeit von der Stromversorgung getrennt, müssen Systemzeit und Datum neu eingegeben werden. Die automatische Sommer- / Winterzeitumstellung ist werksseitig voreingestellt.

### **Fingerprint, Fingerprint-Code**

Für das Öffnen von Schlössern reicht die Eingabe von Fingerprint-Code alleine nicht aus. Sie kann aber ein Teil der Benutzer-Authentifizierung sein.

Für jedes Schloss kann der „Schlossmaster“ (Inhaber des Mastercodes) gemeinsam mit jedem Benutzer bis zu 10 biometrische Fingerprint-Codes anmelden, ändern und auch wieder abmelden.

Vor dem Anmelden eines Fingerprint-Codes eines Benutzers können Mindestanforderungen für Fingerabdrücke dieses Benutzers bezüglich der Anzahl der eindeutigen Merkmale (**Minutien**), der **Bildqualität** und der **Sicherheitsstufe** festgelegt werden. Es wird empfohlen, die Mindestanforderungen für Benutzer vor dem ersten Anmelden nicht niedriger als ab Werk einzustellen.

Einer der angemeldeten Fingerprint-Codes kann als „Alarmfinger“ definiert werden, der beim Öffnen eines Schlosses **Stillen Alarm** auslöst.

Der Inhaber des Mastercodes kann sich auf dem Display anzeigen lassen, welche Finger von welchen Benutzern als Fingerprint-Codes angemeldet sind.

### **Freigabezeit**

Die Freigabezeit können Sie mit der optionalen PC-Software TwinComm USB für jedes Schloss auf eine Dauer von 1-15 Minuten festlegen.

Für jedes Schloss können Sie mit TwinComm USB eine **Öffnungsverzögerung** programmieren, während der das Schloss nach der Code-Eingabe eines Benutzers noch geschlossen bleibt.

Bei aktivierter Option „Freigabezeit“ (TwinComm USB) muss der Benutzer nach Ablauf der Öffnungsverzögerung seinen Code während der sogenannten Freigabezeit erneut übermitteln, damit sich das Schloss öffnet.

Wenn Sie die Option „Freigabezeit“ nicht aktiviert haben, öffnet sich das Schloss sofort nach Ablauf der Öffnungsverzögerung.

## Managercode

### Vorsicht

**Mit werksseitigem Systemmanagercode ist die Konfiguration Ihres Systems nicht gesichert.**

Ändern Sie werksseitige Codes so bald wie möglich. Verwenden Sie keine persönlichen Daten beim Ändern von Codes. Testen Sie neue Codes mehrmals bei geöffneten Wertbehältnissen.

Für jedes Schloss gibt es genau einen dem Benutzer Nr.225 (Manager) zugeordneten Managercode, der im Schloss gespeichert ist und nicht abgemeldet werden kann. Der Managercode des Schlosses 1, des Systemschlusses, berechtigt dazu, Systemeinstellungen zu machen und wird daher auch als **Systemmanagercode** und kurz als Systemcode bezeichnet. Werksseitig ist der Managercode von jedem Schloss als Code „111111“ (bei Systemen der VdS Klasse 2) oder „11111111“ (bei Systemen der VdS Klasse 3) programmiert.

## Mastercode

### Vorsicht

**Mit werksseitigen Mastercodes ist Ihr System nicht gesichert.**

Ändern Sie werksseitige Codes so bald wie möglich. Verwenden Sie keine persönlichen Daten beim Ändern von Codes. Testen Sie neue Codes mehrmals bei geöffneten Wertbehältnissen.

Für jedes Schloss gibt es genau einen dem Benutzer Nr.00 (Schlossmaster) zugeordneten Mastercode, der im Schloss gespeichert ist und nicht abgemeldet werden kann. Nur der Mastercode berechtigt dazu, Schlossbenutzer zu verwalten. Werksseitig ist der Mastercode für Schlösser der VdS Klasse 2 als Ziffernfolge „123456“ und für Schlösser der Klasse 3 als „12345678“ programmiert. In der Benutzermatrix der optionalen PC-Software TwinComm kann der **Systemmanager** festlegen, ob der Mastercode zur Schlossöffnung berechtigt.

## Minutien

Eindeutig unterscheidbare Merkmale eines Fingerabdrucks. Eine Mindestanzahl dieser Merkmale für den Referenzabdruck kann eingestellt werden im Service-Menü Fingerprint\Min. Minutien.

Wertebereich: 09 - 50 (nur unterer Grenzwert kann erhöht werden)

Voreingestellter Wert: 18

Bei Einstellung „18“ wird das Ergebnis jeden Scan-Durchgangs, bei dem vom Sensor weniger als 18 Minutien registriert werden, als qualitativ nicht gut genug zum Anmelden von Fingerprint-Code zurückgewiesen.

Die Beschaffenheit von Fingerkuppen ist individuell unterschiedlich. Wir empfehlen, jeden Benutzer durch Test-Scans ermitteln zu lassen, wie viele Minutien jeder seiner anzulernenden Finger aufweist. Danach kann der Schlossmaster für jeden Benutzer die geringste zulässige Anzahl von Minutien festlegen als Wert des Fingers mit den wenigsten Minutien minus 3 oder 4 (in Menü Service / Fingerprint / Min. Minutien).

## Netzausfall

Um Schlösser auch bei Netzausfall öffnen und schließen zu können, wenn das System über ein Netzteil (Netzteilbetrieb über TwinConnect) versorgt wird, schließen Sie eine 9 Volt Blockbatterie Typ Alkaline an die Bedieneinheit an. Stecken Sie das Adapterkabel in die Buchse an der Unterseite der Bedieneinheit. Siehe auch Abschnitt „System während Netzausfall mit Spannung versorgen“.

### **Öffnungsverzögerung**

Für jedes Schloss können Sie mit der optionalen PC-Software TwinComm USB eine Öffnungsverzögerung von 1-99 Minuten programmieren. Für diesen Zeitraum bleibt das Schloss auch nach der Code-Eingabe des Benutzers geschlossen. Siehe auch Option „**Freigabezeit**“.

Wenn Sie die Option „Freigabezeit“ nicht aktiviert haben, öffnet sich das Schloss sofort nach Ablauf der Öffnungsverzögerung.

### **Öffnungszeit**

Siehe **Sperrzeit / Öffnungszeit (Zeitprogramm)**.

### **Parallelcode**

Nur möglich bei Systemen mit mindestens zwei Schlössern. Der erste Benutzer kann Schloss 1, 2 oder 3 öffnen, der zweite gegebenenfalls eines der beiden noch geschlossenen und der dritte das letzte. Für jeden beteiligten Benutzer muss bei den Schlössern der gleiche Code angemeldet sein.

Kombinierbar mit „**Zwangsfolge**“. Wenn 2 Schlösser im System sind, kann ein Benutzer während einer „**Teilsperrezeit**“ ein Wertbehältnis auch alleine öffnen.

Bei Aktivierung dieser Funktion mit dem optionalen Parametrierset TwinComm USB wird die Funktion „Codeverknüpfung“ automatisch deaktiviert.

### **PIN-Code**

Eine nur einem oder einem Benutzer und dem Schlossmaster bekannte Ziffernfolge, mit der Benutzer sich authentifizieren können. Alternative / Ergänzung zu **Codekarte** und **Fingerprint-Code**.

### **Protokoll (Ereignisprotokoll)**

Alle wichtigen Ereignisse werden mit Datum und Uhrzeit chronologisch protokolliert und können übertragen werden. Beteiligte Geräte und Benutzer werden aufgeführt. Die jüngsten 3000 Ereignisse werden im Protokoll gespeichert. Ereignisse sind Programmiervorgänge, Systemfehler, kritische Statusmeldungen sowie Manipulations- und Sabotageversuche. Der gesamte Ereignisspeicher kann auch auf Chipkarte TwinCard configuration II gespielt und mit der PC-Software TwinComm USB angezeigt und gedruckt werden.

### **Schlossmaster**

Inhaber des Mastercodes eines Schlosses, der die Codes (PIN-Codes, Fingerprint-Codes und Codekarten) der Benutzer dieses Schlosses verwaltet. Ob der Schlossmaster das Schloss selbst öffnen kann, ist abhängig davon, was der Systemmaster in der Benutzermatrix einstellt. Siehe auch **WTU-Funktion**.

### **Schnellöffnung**

Kontrollkästchen in der Benutzermatrix der optionalen Software TwinComm USB. Wenn es aktiviert ist, kann ein Benutzer ein Schloss trotz programmierter Zeitprogramme öffnen, ohne warten zu müssen.

Er kann dies nur, wenn für ihn auch alle anderen zur Schlossöffnung nötigen Kontrollkästchen für die Autorisierung aktiviert worden sind und wenn sein PIN-Code am Schloss angemeldet wurde.

### **Service**

- 1) Menü im Display der Bedieneinheit FlatControl für Servicefunktionen
- 2) Kontrollkästchen in der Benutzermatrix der PC-Software TwinComm USB. Wenn der Systemmanager das Kontrollkästchen „Service“, für einen Benutzer aktiviert, kann dieser das Ereignisprotokoll mittels Chipkarte aus dem System exportieren und es mit der Software TwinComm USB anzeigen und drucken.

### Sicherheitsstufe

Die Sicherheitsstufe gibt an, ab welchem Ähnlichkeitsmaß ein Fingerabdruck als identisch mit gespeicherten Daten interpretiert wird, ab wann eine Person also als erkannt gilt. Dieser Wert hat direkten Einfluss auf die Sicherheit des Systems. Das Ähnlichkeitsmaß wird beim Test-Scannen nach dem zweiten Scannen eines Fingers als „Passung“ angezeigt. Ziehen Sie vom angezeigten Wert eine Toleranz von etwa 10-15 ab und tragen Sie das Ergebnis als „Sicherheitsstufe“ für den jeweiligen Benutzer ein. Der Wert kann eingestellt werden im Menü Service/Fingerprint/Sicherheitsstufe.

Wertebereich: 30 - 99

Voreingestellter Wert: 60, Mindestanforderung ab Werk (TwinComm USB): 40

Sicherheitsstufe	Falsche Abweisung	Falsche Autorisierung
45	<2%	0.0001
50	<3%	0.00001
60	<4%	0.000001

Die obige Tabelle zeigt, dass, je höher der Wert der Sicherheitsstufe ist, desto niedriger die Wahrscheinlichkeit einer falschen Autorisierung und desto höher die Wahrscheinlichkeit, dass Benutzer fälschlich zurückgewiesen werden.

So werden etwa bei einer Sicherheitsstufe von 45 weniger als 2% aller Abdrücke fälschlich als „nicht übereinstimmend“ eingestuft und mit einer Wahrscheinlichkeit von 0,01 % wird der Abdruck einer unberechtigten Person fälschlich für den einer berechtigten Person gehalten.

### Sondertage

#### Vorsicht

**Gefahr von nicht erwünschten Sondertagen.  
Schlossöffnung unbeabsichtigt nicht möglich.**

Achten Sie darauf, Feiertage wie Ostern, die jedes Jahr auf ein anderes Datum fallen, nicht als „jährlich wiederkehrend“ zu markieren.

Sondertage sind Tage, an denen das System ganztägig nicht geöffnet werden kann. Bis zu 30 Sondertage im Jahr können Sie über die optionale Software TwinComm USB definieren. Jeder Öffnungsversuch, der an einem Sondertag erfolgt, wird abgebrochen. Sondertage können als „alljährlich wiederkehrend“ definiert werden.

Werkseinstellung ist „Sondertage“ / „wiederkehrende Sondertage“ deaktiviert. Stellen Sie vor der Aktivierung des **Zeitprogramms** „Sondertage“ sicher, dass Uhrzeit, Wochentag und Datum korrekt eingestellt sind.

### Sperrzeit bei Terminalwechsel, bei dem ein Schloss geschlossen ist

Zeitraum von 90 Minuten, während dem ein Schloss gesperrt ist, nachdem ein Terminalwechsel durchgeführt wurde, bei dem mindestens ein Schloss geschlossen war. Siehe auch die folgenden Einträge.

### Sperrzeit nach Eingabe von falschem Code

Zeitraum von einigen Sekunden bis zu einigen Minuten, in dem ein Schloss trotz Code-Eingabe nicht öffnet, weil ein Benutzer zuvor (wiederholt) Code falsch eingegeben hat. Je öfter falscher Code eingegeben worden ist, desto länger wird die Dauer der Sperrzeit. Siehe auch **Sperrzeit / Öffnungszeit (Zeitprogramm)**.

### Sperrzeit / Öffnungszeit (Zeitprogramm 1)

Eine Sperrzeit ist ein Zeitraum von einem Tag bis zu zwei Monaten, während dem das System ganztägig nicht geöffnet werden kann. Sie können über die PC-Software TwinComm USB (optionales Zubehör) bis zu 3 Sperrzeiten definieren. Mit programmierter Sperrzeit wird jeder Öffnungsvorgang abgebrochen, der im definierten Zeitraum erfolgt. Sperrzeiten können auch zu einzuhaltenden Öffnungszeiten definiert werden, außerhalb derer nicht geöffnet werden kann. Werkseinstellung ist „Sperr- / Öffnungszeiten deaktiviert“. Stellen Sie vor der Aktivierung sicher, dass Uhrzeit, Wochentag und Datum korrekt eingestellt sind. Siehe auch **Sperrzeit nach Eingabe von falschem Code / ...bei Terminalwechsel...**  
Voreinstellung: keine Sperr- / Öffnungszeiten.

### Stiller Alarm

Nur bei Eingabe von PIN-Code, nicht bei Codekarte. In einer Bedrohungssituation kann durch Eingabe eines speziellen „**Alarmcodes**“ beim Öffnen und Programmieren des Systems ein stiller Alarm ausgelöst werden. Das System verhält sich für Benutzer und Bedroher genau so wie beim normalen Öffnen, nur dass zugleich ein stilles Alarmsignal an die Einbruchmeldeanlage geleitet wird.

### Systemmanager

Inhaber des Systemmanagercodes, mit dem das System konfiguriert wird. Der Systemmanager kann selbst Schlösser nicht öffnen und schließen.

### Systemmanagercode (=Managercode von Schloss 1)

#### Vorsicht

**Mit werksseitigem Systemmanagercode ist Ihr System nicht gesichert.**

Ändern Sie werksseitige Codes so bald wie möglich.

Verwenden Sie in Codes keine persönlichen Daten.

Testen Sie neu programmierte Codes mehrmals bei geöffneten Wertbehältnissen.

Der **Systemmanagercode**, auch Systemcode genannt, berechtigt dazu, das System über die Bedieneinheit zu konfigurieren. Er wird in Schloss Nr.01 Ihres Systems gespeichert und ist Benutzer Nr.225 zugeordnet.

Werksseitig ist als Code „111111“ (bei allen Systemen der VdS Klasse 2) oder „11111111“ (bei allen Systemen der VdS Klasse 3) programmiert.

### Teilsperrezeit (3 Zeiträume pro Tag)

Stellen Sie vor der Aktivierung einer Teilsperrezeit sicher, dass Uhrzeit, Wochentag und Datum korrekt eingestellt sind. Für Systeme mit zwei Schlössern können Sie über Software TwinComm USB (optionales Zubehör) eine Teilsperrezeit mit drei Zeiträumen pro Tag definieren. Während der Teilsperrezeiten schließt nur Schloss 2, Schloss 1 bleibt offen. Mit aktivierter Teilsperrezeit wird jeder Schließvorgang von Schloss 1 abgebrochen, der in einem definierten Teilsperrezeitraum liegt. Werkseinstellung ist „Teilsperrezeit deaktiviert“.

Soll trotz aktivierter Teilsperrezeit Schloss 01 geschlossen werden:

Drücken Sie die ENTER Taste, während **Schliessen | Schloss 1 Teilversperrt!** angezeigt wird. Schloss 1 wird geschlossen, die Teilsperrezeit einmalig außer Kraft gesetzt.

Funktion „Teilsperrezeit“ können Sie kombinieren mit Funktion „Automatisches Schließen mit Türschalter“. Die Folge ist, dass Schloss 1 innerhalb der Teilsperrezeit offen bleibt und nach ihrem Ende geschlossen wird.

**TwinComm USB**

Optionales Zubehör. Parametrierset, Software für System TwinLock. Jedes System wird nach der Installation mit TwinComm parametriert. Die Benutzermatrix von System TwinLock, in der die grundsätzlichen Berechtigungen für alle Benutzer festgelegt sind, ist ein Teil der Software TwinComm USB.

**Wochenprogramm**

Über die optionale Software TwinComm USB können Sie bis zu 5 Wochenprogramme mit flexibel definierbaren Öffnungszeiträumen für jeden Wochentag einstellen. Über die Benutzermatrix können Sie die Programme individuell Benutzern zuordnen. Mit programmiertem Wochenprogramm wird jeder Öffnungsvorgang abgebrochen, der nicht in einem definierten Öffnungszeitraum liegt. Stellen Sie vor der Aktivierung eines Wochenprogramms sicher, dass Uhrzeit und Datum korrekt eingestellt sind. Ab Werk sind die Wochenprogramme deaktiviert.

**WTU-Funktion****Vorsicht**

**Ohne autorisierten WTU-Master kann der WTU-Benutzerbereich nicht verwaltet werden.**

Autorisieren Sie Benutzer 99 vor Aktivierung der WTU-Funktion mit allen gewünschten Rechten.

Bei aktivierter Option „WTU-Funktion“ werden die Benutzer jeden Schlosses im System in zwei Gruppen aufgeteilt. Der neue Benutzerbereich bekommt Benutzer Nr.99, der zum „WTU-Master“ wird, als Verwalter. Der ursprüngliche Benutzerbereich verkleinert sich um den neuen Bereich. Die Größe der Gruppen kann fest eingestellt / über das optionale Parametrierset TwinComm definiert werden.

Für Benutzer ändert sich die Bedienung durch die WTU-Funktion nicht.

Die erste Benutzergruppe (Benutzer Nr.01 bis zu Benutzer Nr.XX-1,) wird nach wie vor vom **Schlossmaster** verwaltet. Die neue Gruppe der WTU-Benutzer von Benutzer Nr.XX (= frei definierbare Nr. zwischen 1 und 98) bis Nr.98 wird von Benutzer Nr.99, dem WTU-Master verwaltet.

**Zeitprogramm**

Das Öffnen der Schlösser kann auf diverse Zeiträume beschränkt werden. Siehe auch die Einträge **Sondertage**, **Sperrzeit**, **Teilsperrezeit** und **Wochenprogramm**. Zeitprogramme / Sperrzeiten können von privilegierten Benutzern unterbrochen werden. Siehe auch „**Zeitprogrammunterbrechung**“ und „**Schnellöffnung**“.

**Zeitprogrammunterbrechung**

Eine innerhalb des gesicherten Bereichs eingeschlossene Person kann einen im Inneren des Wertbehältnisses angebrachten Druckschalter betätigen, wodurch ein Schloss trotz aktiver **Zeitprogramme** (Wochenprogramm, Sondertage, Sperrzeit oder Teilsperrezeit) von außen durch Benutzerautorisierung (üblicherweise Codeeingabe) geöffnet werden kann. Nach einer Öffnung werden die Zeitprogramme automatisch wieder aktiviert. Der Anschluss eines solchen Druckschalters ist nur an der optionalen Schalteinrichtung TwinAlarm möglich, nicht an der Erweiterungseinheit TwinXT.

Auch ohne TwinAlarm kann ein Benutzer, der vom Systemmanager zur Schnellöffnung autorisiert wurde (Benutzermatrix TwinComm), aktive Zeitprogramme unterbrechen. Siehe auch „**Schnellöffnung**“.

**Zwangsfolge (ZF)**

Möglichkeit, eine Reihenfolge festzulegen, die beim Öffnen und Schließen der Schlösser des Systems TwinLock eingehalten werden muss.

Wenn Sie die Option „Zwangsfolge“ mit der PC-Software TwinComm USB programmieren, müssen Benutzer zuerst Schloss 1, dann Schloss 2 und danach gegebenenfalls Schloss 3 öffnen. Nach der Öffnung von Schloss 1 ist das System teilgesichert (entspricht bei Option ZF dem Zustand „gesichert“), nach der Öffnung aller Schlösser ist das System entsperrt und damit ungesichert.

Beim Schließen muss zuerst gegebenenfalls Schloss 3, Schloss 2 und zuletzt Schloss 1 geschlossen werden. Erst nach dem Schließen von Schloss 01 ist das System gesichert.

Werkseinstellung: keine Zwangsfolge.

**Kundendienst**

CLAVIS Deutschland GmbH  
Grüner Weg 38  
34117 Kassel

Telefon: +49 (0)561 988 499-0

E-Mail: [info@tresore.eu](mailto:info@tresore.eu)

Internet: [www.tresore.eu](http://www.tresore.eu)  
[www.tresorschloss.de](http://www.tresorschloss.de)

## 9 Anhang

### 9.1 Stichwortverzeichnis

1 aus 3 .....	87	Codesicherung .....	20
4-Augen-Prinzip .....	38	Codeverknüpfung .....	87
Abmelden .....	85	Datum einstellen.....	43
Adapterkabel .....	69	Echtzeituhr .....	87
Alarmcode .....	85	Einbruchmeldeanlage.....	41, 42
Alarmgeräte ein- / ausschalten .....	44	scharf schalten .....	42
Anmelden .....	85	unscharf schalten .....	41
Autorisierung.....	77, 85	Einsatzgebiet.....	9
Kontrollkästchen .....	27	Entsorgung .....	84
1 aus 3 .....	29	Fehlermeldungen.....	77
2-Augen .....	29	Fingerprint.....	8, 87
Benutzermatrix.....	27	Benutzer anzeigen.....	67
Freigabe .....	29	Bildqualität.....	63, 86
Schnellöffnung.....	29	Min. Minuten.....	62
Service .....	29	Scan testen .....	61, 75
Unscharfschalten .....	29	Sicherheitsstufe .....	64, 90
Wochenprogramm .....	29	Temperatur einstellen.....	76
Basissystem.....	9	Überblick.....	60
Basissystem 1.1.....	10	Fingerprint-Code	
Basissystem 2.1.....	11	abmelden.....	66
Basissystem 3.2.....	12	Alarmfinger .....	65
Batterie.....	69	anmelden.....	65
Batteriewarngrenze.....	23	eingeben .....	36
Bedieneinheit Menüführung.....	30	FlatControl .....	7
Benutzer Autorisierung.....	27	Reinigung.....	76
Benutzercode.....	7	Softwareversion .....	69
Benutzermatrix .....	85	Freigabezeit.....	39, 87
ab Werk.....	28	Funktionsübersicht.....	21
Autorisierung .....	28	Handbuch.....	6
Kontrollkästchen .....	29	Handlungsaneisung	
Benutzerqualifikation.....	6	Handlungsziel.....	8
Bestimmungsgemäßer Gebrauch ..	24	Materialien .....	8
Bildqualität.....	86	Menüpunkt.....	8
Busverteiler .....	17	Tasten .....	8
Chipkarte .....	8, 19	Vorbedingung.....	8
in Bedieneinheit stecken .....	32	Werkzeug.....	8
Code .....	86	Hinweis .....	7
Codealterung.....	86	Kabel.....	78
Code-Eingabe .....	86	Komfortsystem .....	9, 13
Managercode .....	88	Komfortsystem 1 .....	13
Mastercode .....	88	Komfortsystem 2 .....	15
Codekarte		Konfiguration.....	49
Benutzer anzeigen .....	59	Fehler config. ....	47
abmelden .....	58	Schlosssystem.....	47
anmelden .....	57, 85		

Kurzbedienungsanleitung.....	6	Sondertageprogramm .....	24
Managercode.....	8	Sperreinrichtung.....	18
Mastercode .....	7, 88	Sperrzeit .....	90, 91
ab Werk.....	32	falscher Code .....	90
ändern.....	52	Zeitprogramm .....	89, 91
Minutien .....	88	Sprache	
Montageanleitung .....	6	einlesen .....	51
Motor-Service .....	72	wählen.....	50
Netzausfall .....	88	Stiller Alarm.....	37, 91
Spannungsversorgung.....	69	Störung	
Not-Öffnung .....	73, 74	Abhilfe .....	77
Öffnungsverzögerung .....	39, 87, 89	Symbolbedeutungen.....	7
Parallelcode.....	40, 89	System	
Parametrierset .....	23, 27	Einstellungen .....	26
PIN-Code .....	89	Systemmanager .....	91
Benutzer anzeigen.....	56	Systemaufbau .....	10
ändern.....	54	Systembeschreibung.....	9
anmelden .....	53, 85	Systemcode .....	8, 91
persönliche Daten .....	31	ab Werk .....	32
Protokoll.....	45, 46, 89	ändern .....	51, 52
Ereignisse .....	89	Systemkomponenten.....	17
Manipulation.....	89	Teilsperzeit.....	89, 91
prüfen.....	82	Textauszeichnungen .....	7
Reinigung.....	76	Türschalter.....	23
Riegelwerkskontakt .....	18	TwinAlarm .....	18
ignorieren.....	75	PIN-Codes anmelden.....	53
Rücknahme .....	84	TwinCard	
Sachschaden .....	7	code access.....	19
Schalteinrichtung.....	18	configuration II.....	19, 45, 47
Schloss		language .....	19, 51
automatisch schließen .....	42	TwinComm .....	92
Managercode .....	88	Benutzermatrix.....	86
mit Codekarte öffnen .....	35	TwinComm USB.....	23, 27, 47
mit PIN-Code öffnen.....	35	TwinConnect .....	17
Motorschritt .....	72	TwinXT .....	18
öffnen.....	37, 38, 39	Uhrzeit	
öffnen mit Parallelcode .....	40	einstellen .....	43
schließen .....	41, 42	VdS-Klasse.....	31
TwinLock.....	17	Verwertung .....	84
Schlossmaster.....	89	Werkzeug.....	7
Schnellöffnung.....	89	Wochenprogramm .....	24, 92
Service .....	89	WTU	
Autorisierung .....	89	WTU-Benutzer .....	92
Menü .....	89	WTU-Funktion .....	45, 92
Reset .....	70	WTU-Master.....	34, 92
Sicherheitshinweise.....	7	Zeitprogramm.....	92
Sicherheitsstufe .....	90	Unterbrechung.....	92
Softwareversion anzeigen.....	69	Zeitprogramme .....	24
Sondertage .....	90	Zwangsfolge.....	93
wiederkehrend.....	90		

## 9.2 Abbildungsverzeichnis

Abbildung 1	Systemaufbau von Basissystem 1.1 .....	10
Abbildung 2	Systemaufbau von Basissystem 2.1 .....	11
Abbildung 3	Systemaufbau von Basissystem 3.2 .....	12
Abbildung 4	Systemaufbau von Komfortsystem 1 ohne EMA.....	13
Abbildung 5	Systemaufbau von Komfortsystem 1 mit EMA.....	14
Abbildung 7	Systemaufbau von Komfortsystem 2 mit EMA.....	16
Abbildung 8	Bedieneinheit FlatControl BioPIN .....	17
Abbildung 9	Schloss TwinLock .....	17
Abbildung 10	Busverteiler TwinConnect .....	17
Abbildung 11	Sperreinrichtung TwinXT.....	18
Abbildung 12	Schalteinrichtung TwinAlarm .....	18
Abbildung 13	Symbol TwinCard code access.....	19
Abbildung 14	Symbol TwinCard language .....	19
Abbildung 15	Symbol TwinCard configuration II.....	19
Abbildung 16	Übersicht Codes im System.....	20
Abbildung 17	PC-Software TwinComm USB (Zubehör) .....	23
Abbildung 18	Bedieneinheit FlatControl BioPIN .....	23
Abbildung 19	Startseite der PC-Software TwinComm USB (Zubehör).....	23
Abbildung 20	Ausschnitt Benutzermatrix in TwinComm USB.....	23
Abbildung 21	Karte und Kartenfach FlatControl BioPIN.....	23
Abbildung 22	Bedieneinheit mit Fingerführung.....	23
Abbildung 23	Adapterkabel mit Bedieneinheit verbinden.....	23

## 9.3 Änderungshistorie des Dokuments

Version	Stand	Änderung	Name
1.00	09.02.09	Erstausgabe	MR
1.01	16.03.09	Update	MR
1.02	28.08.09	Update	MR
1.03	22.10.09	Update	MR
1.03A	11.02.10	Update Bilder	MR
1.03B	24.03.10	Update TwinConnect	MR

!!! Irrtum vorbehalten!!!

**Kundendienst**



CLAVIS Deutschland GmbH  
Grüner Weg 38  
34117 Kassel

Telefon: +49 (0)561 988 499-0  
E-Mail: [info@tresore.eu](mailto:info@tresore.eu)  
Internet: [www.tresore.eu](http://www.tresore.eu)  
[www.tresorschloss.de](http://www.tresorschloss.de)