# Montage- und Installationsanleitung

# Zutrittskontroll-Steuergerät
# C-S P 100
# C-S A 100

## Inhaltsverzeichnis

## 1 Verwendete Abkürzungen

| | | | |
|---|---|---|---|
| DC | Direct current (Gleichstrom) | LED | Light emitting diode (Leuchtdiode) |
| OM | Ausgabemodus | PIN | Persönliche Identifikationsnummer |
| RFID | Radio Frequency Identification | TTL | Transistor-Transistor-Logik (hier: Transistor-Schaltausgang) |

**Achtung!**
Allgemeiner Hinweis auf Gefahren und notwendiger Einhaltung von Vorgaben.

**Hinweis!**
Allgemeiner Hinweis und Information, die zur fachlich richtigen Arbeitsausführung gehört.

**Handlungsaufforderung**
Fordert Sie zur Handlung (Arbeitsschritt) auf.

**Entsorgung**
Die Zutrittskontrolle ist als Elektronikschrott an öffentlichen Rücknahmestellen und Wertstoffhöfen zu entsorgen. Dieses Produkt ist für eine Entsorgung im Hausmüll nicht geeignet!
Das Gehäuse und die Verpackung sind separat zu entsorgen.

## 2 Sicherheitshinweise

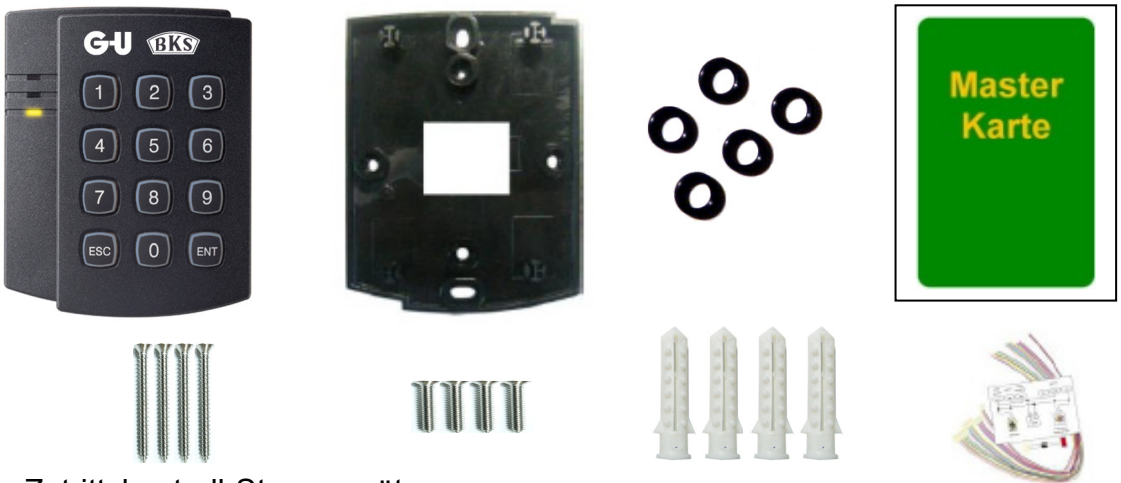
- Vor jeder Montage, Reparatur, Wartungs- oder Einstellarbeit sind alle zugehörigen Netzteile spannungslos zu schalten und gegen unbeabsichtigtes Wiedereinschalten abzusichern.
- Der elektrische Anschluss darf nur von ausgebildetem Fachpersonal vorgenommen werden.
- Die jeweils lokal geltenden Montage- und Installationsbestimmungen, Richtlinien und Vorschriften sind einzuhalten. Das gilt insbesondere für VDE-Richtlinien, DIN VDE 0100, DIN VDE 0160, DIN VDE 0632 EN 50133-1 / DIN VDE 0830 Teil 8-1:2003-09, EN 50133-2-1 / DIN VDE 0830 Teil 8-2-1:2001-08, EN 50133-7 / DIN VDE 0830 Teil 8-7:2000-04
- Die primärseitigen Schutzmaßnahmen erfolgen bauseits. Als netzseitige Trennvorrichtung ist ein bauseitiger Sicherungsautomat zu verwenden.
- Die DIN VDE 0100 und sowie ggf. die Muster-Leitungsanlagen-Richtlinie (MLAR) sind zu Berücksichtigen und Einzuhalten.
- Bei unsachgemäßem Einsatz, Montage und Installation oder bei Verwendung von nicht originalen Zubehörteilen wird keine Haftung übernommen!
- Bei Schäden, die durch Nichtbeachten dieser Installationsanleitung verursacht werden, erlischt der Garantieanspruch! Für Folgeschäden wird keine Haftung übernommen!
- Aus Sicherheits- und Zulassungsgründen (CE) ist das eigenmächtige Umbauen und/oder Verändern des Produkts nicht gestattet.
- Die Beachtung der nachstehenden Montageanleitung gewährleistet eine optimale Funktion und eine lange Lebensdauer.
- Bitte Lieferumfang auf Vollständigkeit und Beschädigungen prüfen. Für Beschädigungen durch unsachgemäße Behandlung kann keine Haftung übernommen werden.
- ACHTUNG: Die einschlägigen Sicherheitsbestimmungen des Arbeitsschutzes und der Berufsgenossenschaften sind bei der Montage und den späteren Wartungsarbeiten unbedingt zu beachten!

## 3 Technische Daten

| | |
|---|---|
| **Modell** | C-S P 100, C-S A 100 |
| **CPU** | 8 Bit Mikroprozessor |
| **Speicher** | Programm-Speicher 20 KByte ROM<br>Datenspeicher 2 KByte ROM |
| **Anzahl Nutzer** | 512 Nutzer |
| **Spannung/Strom** | DC 12 V, 0,2 A |
| **Schutzart** | IP20 |
| **Leser Anschluss** | 26 Bit Wiegand (4/8 Bit Burst für PIN) |
| **Eingänge** | 5 (Tür-Freigabe-Taster, Türkontakt,<br>Hilfseingänge Aux1, Aux2, Aux3) |
| **Ausgänge** | 2x Relaisausgang: max. DC: 18V, 2 A<br>1 Alarmgeber: DC 5 V, 500 mA<br>1 TTL: DC 5 V, 20 mA |
| **LED-Anzeigen** | 3 (Rot, Grün und Gelb) |
| **Akustisches Signal** | Piezo- Summer |
| **Arbeitstemperatur** | -35°C bis +65°C |
| **Arbeitsfeuchtigkeit** | 10% bis 90% relative Luftfeuchtigkeit ohne Kondensation |
| **Abmessungen (B x H x T)** | 87 mm x 100 mm x 31 mm |
| **Zertifikate/Zulassungen** | FCC, CE, MIC |

Hiermit erklärt die BKS GmbH, dass sich diese Geräte in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befinden.

## 4 Lieferumfang




- Zutrittskontroll-Steuergerät
- Montageplatte
- 5 O-Ringe
- Masterkarte
- 4 Schrauben (3,5 x 40)
- 4 Schrauben (M3 x 12)
- 4 Dübel
- Kurzanleitung
- Anschlusskabel

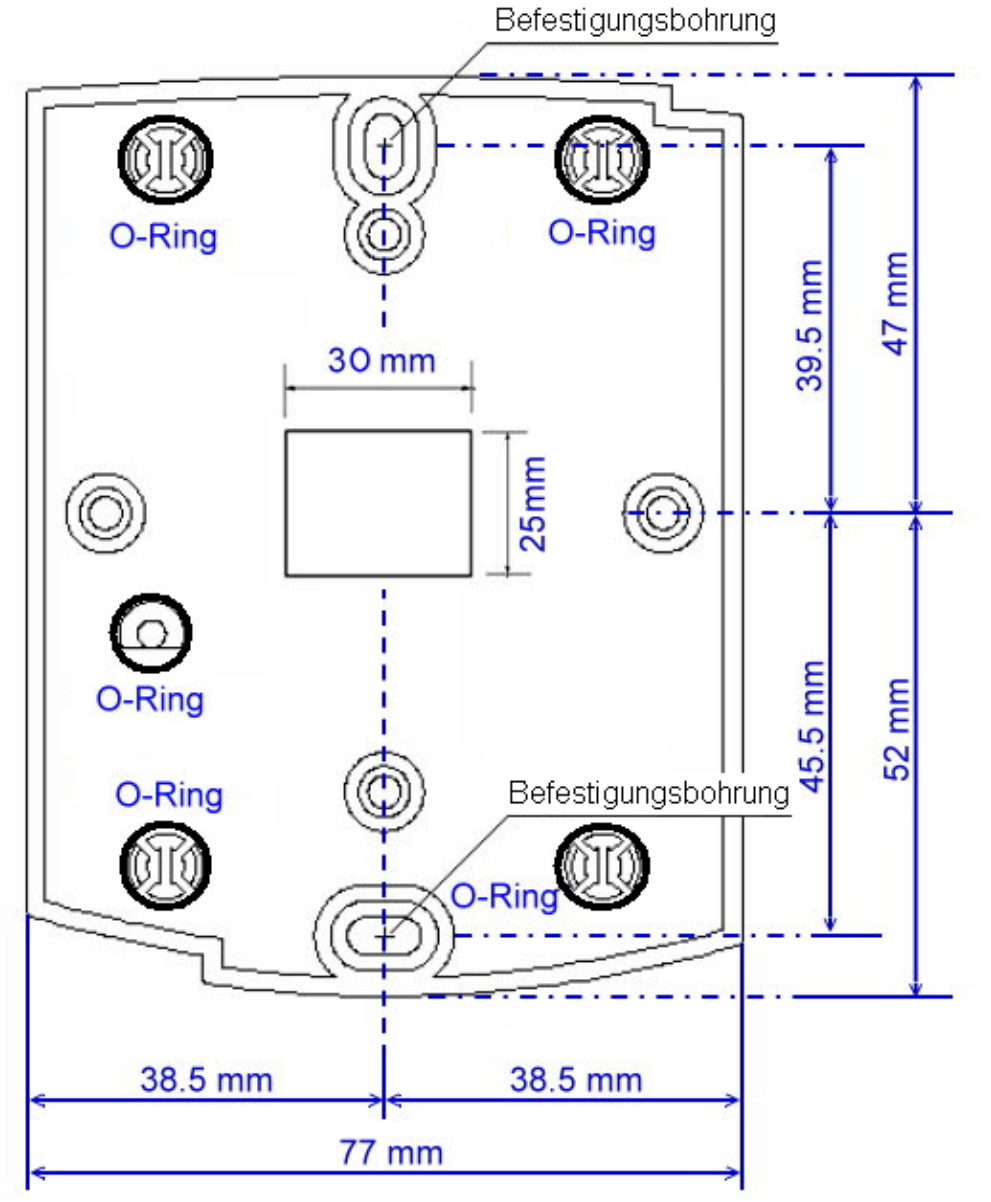
## 5 Montage

Der elektrische Anschluss ist entsprechend den im Errichtungsland geltenden Bestimmungen durchzuführen und darf nur von Fachpersonal durchgeführt werden.

Entnehmen Sie das Zutrittskontroll-Steuergerät der Verpackung.

Befestigen Sie die Montageplatte an einer ebenen Fläche. Verwenden Sie entweder die beigepackten Blechschrauben oder die M3-Schrauben zur Befestigung. Mittig ist eine Bohrung für die Anschlussleitung vorzusehen.

Idealerweise nehmen Sie nun den elektrischen Anschluss vor und testen die Funktion der Steuerung bevor Sie diese auf die Montageplatte aufklipsen. Hierzu stecken Sie die 5 O-Ringe auf die Rastungen und den Stößel für den Sabotagekontakt. Drücken Sie die Steuereinheit auf die Montageplatte. Achten Sie hierbei auf ein korrektes Einrasten.

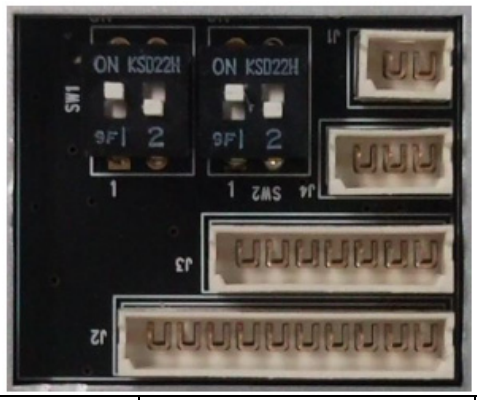


## 6 Anschluss

| Stecker | Signal | Aderfarbe |
|---|---|---|
| 2-fach (J1) | Spannung (+12V) | Rot |
| | Masse (GND) | Schwarz |
| 10-fach (J2) | Ausgang Tür-Öffner-Relais (COM) | Grau/Rot |
| | Ausgang Tür-Öffner-Relais (NC) | Blau/Weiß |
| | Ausgang Tür-Öffner-Relais (NO) | Weiß/Rot |
| | Ausgang Alarm-Relais (COM) | Weiß |
| | Ausgang Alarm-Relais (NC) | Violett/Weiß |
| | Ausgang Alarm-Relais (NO) | Violett |
| | Eingang Tür-Freigabe-Taster | Orange |
| | Eingang Türkontakt | Gelb/Rot |
| | Hilfseingang Aux 1 | Grün |
| | Hilfseingang Aux 2 | Grün/Weiß |
| 7-fach (J3) | Eingang Wiegand Data 0 | Rosa |
| | Eingang Wiegand Data 1 | Hellblau |
| | TTL-Ausgang | Orange/Weiß |
| | Summer-Ausgang | Braun/Weiß |
| | Hilfseingang Aux 3 | Grün/Rot |
| | Reserve | Blau/Rot |
| | Reserve | Gelb/Weiß |
| 3-fach (J4) | RS232-TX | Schwarz/Weiß |
| | RS232-RX | Rot/Weiß |
| | Masse (GND) | Schwarz |

### DIP-Schalter Einstellungen (optionale Wiegand-Ausgabe)

Über die beiden DIP-Schalter SW1 und SW2 kann entscheiden werden, ob die orange/weiße Ader als TTL-Ausgang und die Braun/weiße Ader als Summer-Ausgang oder beide Adern zur Wiegand-Ausgabe verwendet werden.



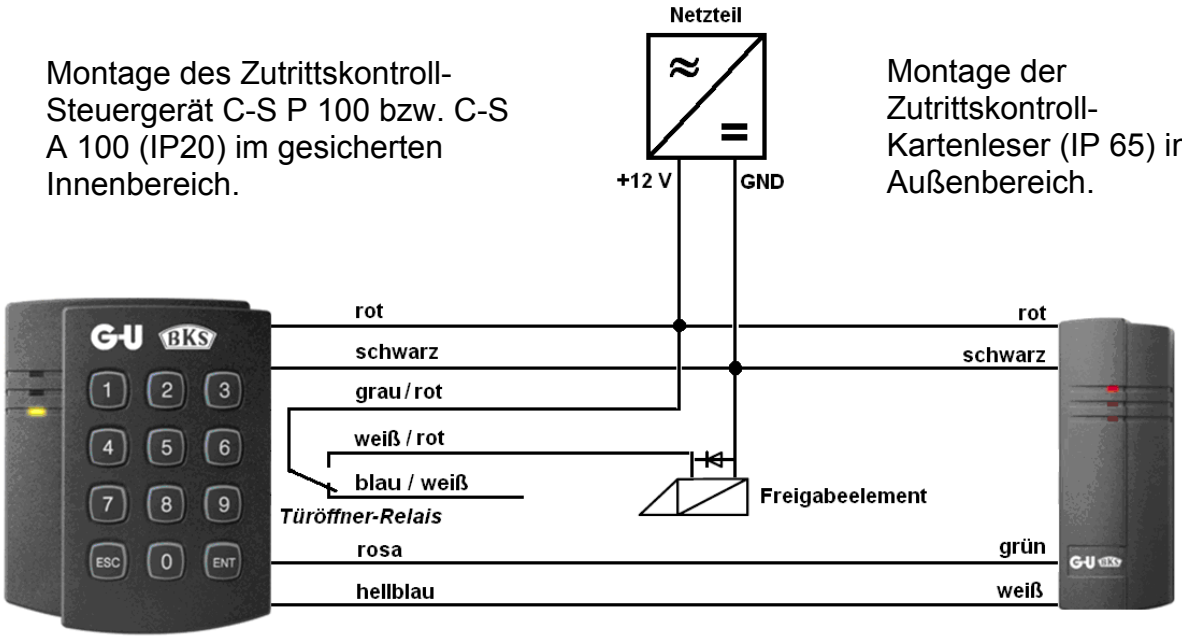

| SW1 (1) | SW1 (2) | SW2 (1) | SW2 (2) | Orange/weiß | Braun/Weiß |
|---|---|---|---|---|---|
| ON | OFF | ON | OFF | TTL-Ausgang | Summer-Ausgang |
| OFF | ON | OFF | ON | Wiegand Data 0 Ausgang | Wiegand Data 1 Ausgang |

## 7 Anschlussbeispiele

Zur Verlängerung der Leseranschlussleitungen liegen eine entsprechende Anzahl an Stoßverbindern den Produkten bei. Zur bauseitigen Verlängerung der Anschlussleitung empfehlen wir Telekommunikationsleitung vom Typ J-Y(ST)Y 2 x 2 x 0.8. Die max. Leitungslänge beträgt 50 m Die verwendeten Freigabeelemente müssen über eine Freilaufdiode verfügen!

### 7.1 Anschluss von Kartenleser außen und Freigabeelement

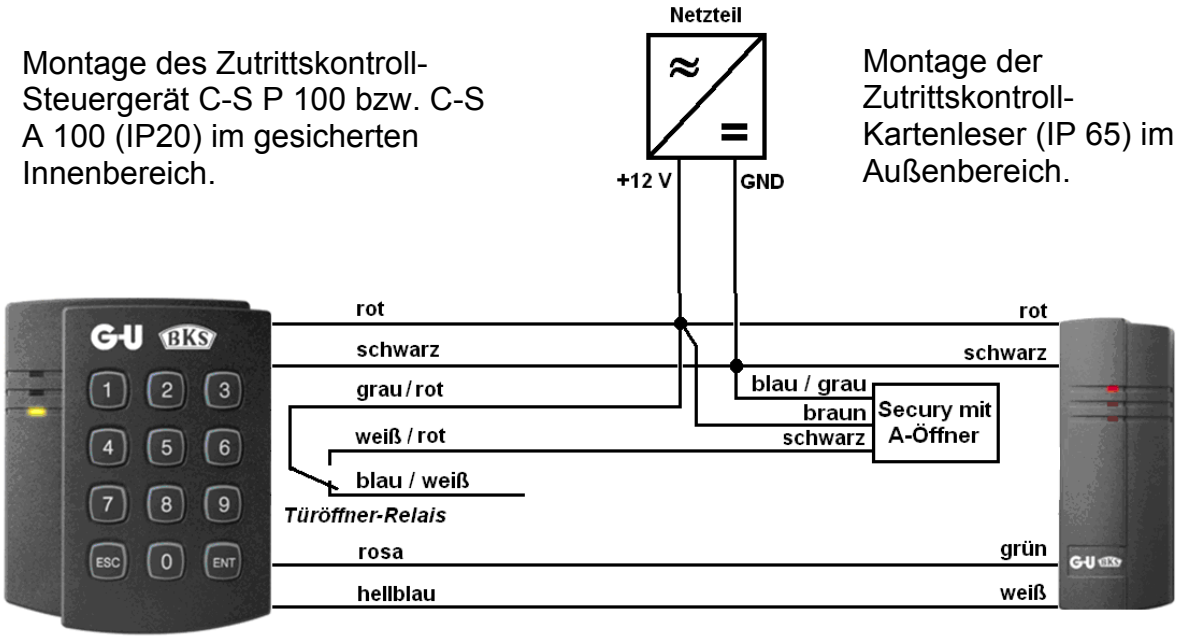
Montage des Zutrittskontroll-Steuergerät C-S P 100 bzw. C-S A 100 (IP20) im gesicherten Innenbereich.




Montage der Zutrittskontroll-Kartenleser (IP 65) im Außenbereich.

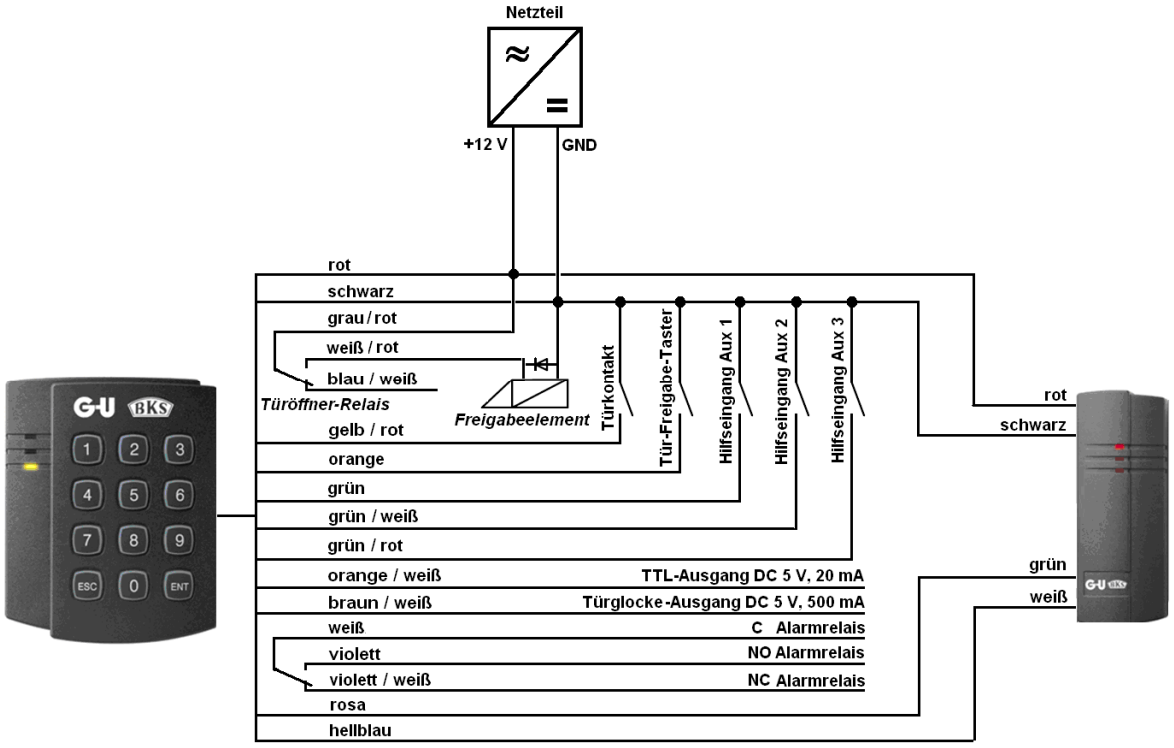
### 7.2 Anschluss von Kartenleser außen und Secury mit A-Öffner

Montage des Zutrittskontroll-Steuergerät C-S P 100 bzw. C-S A 100 (IP20) im gesicherten Innenbereich.




Montage der Zutrittskontroll-Kartenleser (IP 65) im Außenbereich.

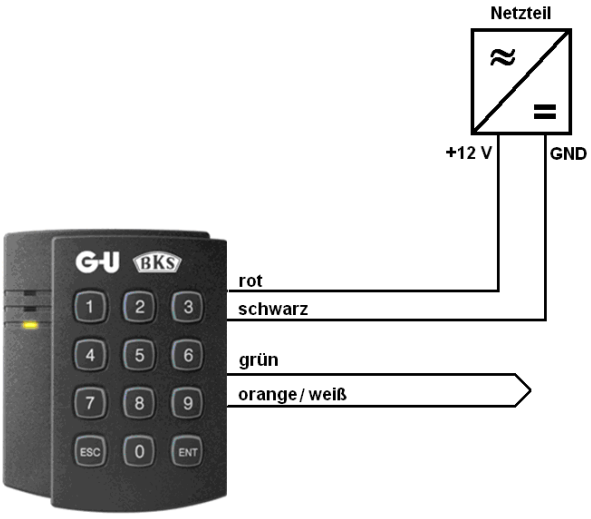
## 7.3 maximale Anschlussmöglichkeiten




## 8 Initialisierung/Reset

Jedes Zutrittskontroll-Steuergerät sollte vor der Inbetriebnahme initialisiert werden. Hierbei werden die Grundeinstellungen des Herstellers geladen. Alle gespeicherten Daten werden gelöscht. Dieses Vorgehen eignet sich auch zum Reset mit Löschung des Gesamtspeichers bei Verlust der Masterkarte:

1. Spannung ausschalten.
2. die grüne und orange/weiße Ader verbinden.
3. Spannung einschalten.
4. Alle LED's blinken und akustische Signalisierung.
5. Adern lösen und gegeneinander isolieren.




Im Normalbetrieb müssen die nicht verwendeten Anschlussadern gut gegeneinander isoliert sein, damit nicht versehentlich ein Reset ausgelöst wird.

## 8.1 Festlegen des Betriebsmodus

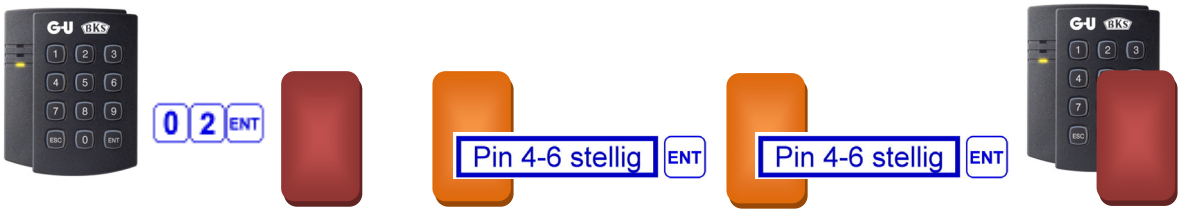
Durch Drücken der Tastenfolge 0, 1 und ENT legen Sie fest, dass das Zutrittskontroll-Steuergerät nur RFID-Karten zur Prüfung der Zutrittsberechtigung akzeptiert. Mit der Tastenfolge 0, 2 und ENT werden RFID-Karten immer zusammen mit einer vom Nutzer einzugebenden PIN geprüft. Sie können aber auch ausschließlich mit einer PIN oder wahlweise mit PIN oder Karte arbeiten.


## 8.2 Betriebsmodus 1: Registrierung von RFID-Karten

1. Initialisierung durchführen. Nach der Initialisierung müssen alle 3 LEDs im Gleichtakt blinken.
2. Durch Drücken der Tastenfolge 0, 1 und ENT legen Sie fest, dass das Zutrittskontrollsteuergerät RFID-Karten zur Prüfung der Zutrittsberechtigung akzeptiert.
   *Sie können aber auch ausschließlich einem PIN-Code oder einen der voran genannten Betriebsmodi verwenden (siehe Betriebsmodus 2, 3, 5)*
3. Eine RFID-Karte einlesen. Diese erste RFID-Karte ist jetzt die Masterkarte.
4. Jetzt nacheinander die Nutzerkarten einlesen (max. 512 Nutzerkarten möglich).
5. Zum Abschluss der Programmierung noch mal die Masterkarte einlesen.

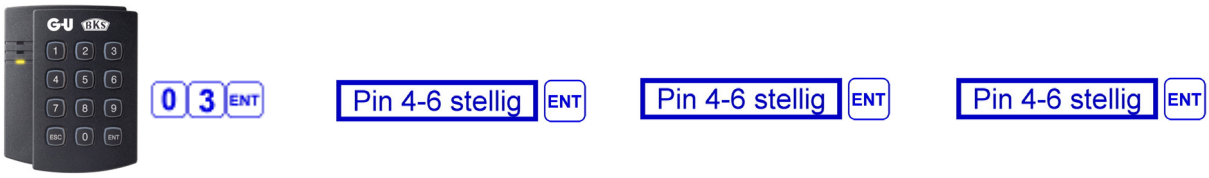

## 8.3 Betriebsmodus 2: Registrierung von RFID-Karten + PIN

1. Initialisierung durchführen. Nach der Initialisierung müssen alle 3 LEDs im Gleichtakt blinken.
2. Durch Drücken der Tastenfolge 0, 2 und ENT legen Sie fest, dass das Zutrittskontrollsteuergerät RFID-Karten und eine 4-6 stellige Nutzer-PIN zur Prüfung der Zutrittsberechtigung akzeptiert.
3. Eine RFID-Karte einlesen. Diese erste RFID-Karte ist jetzt die Masterkarte.
4. Jetzt eine Nutzerkarte einlesen, direkt nachfolgend den Nutzer-PIN (4-6 strellig) eingeben und mit ENT bestätigen (max. 512 Nutzerkarten möglich).
5. Zum Abschluss der Programmierung noch mal die Masterkarte einlesen.



## 8.4 Betriebsmodus 3: Registrierung über PIN

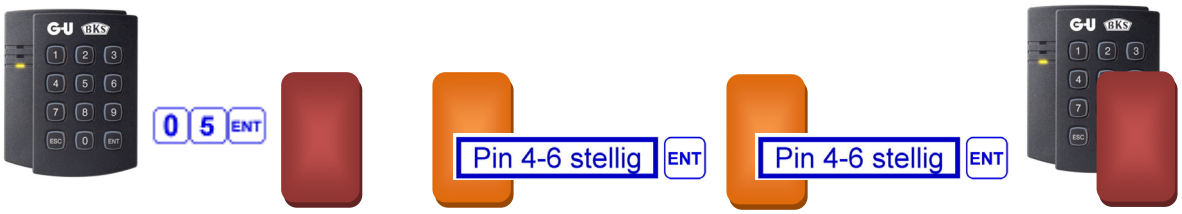
1. Initialisierung durchführen. Nach der Initialisierung müssen alle 3 LEDs im Gleichtakt blinken.
2. Durch Drücken der Tastenfolge 0, 3 und ENT legen Sie fest, daß das Zutrittskontrollsteuergerät einen 4-6 stelligen PIN-Code zur Prüfung der Zutrittsberechtigung akzeptiert.
3. Einen PIN-Code 4-6 stelllig eingeben und mit ENT abschließen. Dieser PIN-Code ist jetzt der Master-PIN-Code.
4. Jetzt nacheinander die Nutzer-PIN (4-6 stellig) eingeben (max. 512 Nutzer-PIN möglich) und jeweils mit ENT abschließen.
5. Zum Abschluss der Programmierung noch mal den Master-PIN eingeben und mit ENT bestätigen.




Betriebsmodus 3 | Master-PIN | Nutzer-PIN | Master-PIN

## 8.5 Betriebsmodus 5: Registrierung von RFID-Karten oder PIN

1. Initialisierung durchführen. Nach der Initialisierung müssen alle 3 LEDs im Gleichtakt blinken.
2. Durch Drücken der Tastenfolge 0, 5 und ENT legen Sie fest, daß das Zutrittskontrollsteuergerät einen 4-6 stelligen PIN-Code oder eine RFID-Karte zur Prüfung der Zutrittsberechtigung akzeptiert.
3. Eine RFID-Karte einlesen. Diese erste RFID-Karte ist jetzt die Masterkarte.
4. Jetzt eine Nutzerkarten einlesen, direkt nachfolgend den 4-6 stelligen Nutzer-PIN eingeben und mit ENT bestätigen (max. 512 Nutzerkarten möglich).
5. Zum Abschluss der Programmierung noch mal den Master-PIN eingeben und mit ENT bestätigen.




Erste Karte = Masterkarte | Nutzerkarte oder PIN | Masterkarte

## 9 Betrieb

- Im Normalbetrieb blinkt die gelbe LED.
- Das Türöffner-Relais schaltet bei einer Freigabe für 3 s, die grüne LED der Zutrittskontrollsteuerung leuchtet für 3 s.
- Bei der Abweisung einer nicht zutrittsberechtigten Karte schaltet das Alarm-Relais für 2 s, die rote LED leuchtet für 2 s.
- Wird der Tür-Freigabe-Taster betätigt, so reagiert die Steuerung wie bei einer Freigabe über eine Nutzerkarte (Tür-Öffner-Relais schaltet für 3 s)

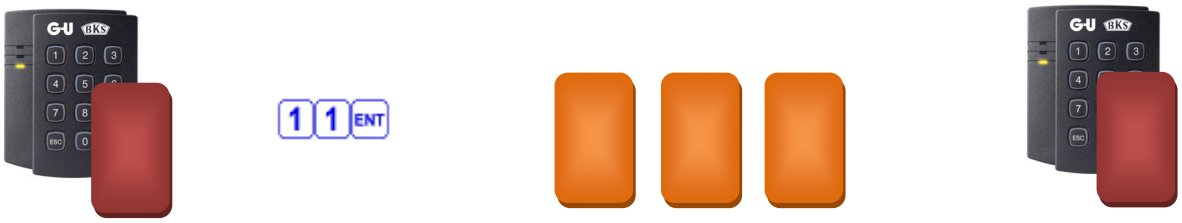
- Im Falle einer Bedrohung geben Sie das 2-stellige Bedrohungs- Passwort (Werkseinstellung 00) vor der Lesung der Karte ein und die Tür öffnet sich wie üblich. Jedoch wird der Bedrohungs- Alarm (TTL-Ausgang) aktiviert und bei entsprechender Installation das Sicherheitspersonal benachrichtigt.
- Mit der ESC Taste kann der Türglocke-Ausgang für 5 s aktiviert werden.

## 9.1 Werkseinstellungen

| | | Kommando | | | |
|---|---|---|---|---|---|
| **Funktion** | **Default** | **Aktivieren** | **Deaktivieren** | **Ändern** | ***Seite*** |
| Nutzerkarten hinzufügen | | | | 11 | *13* |
| Nutzerkarten plus PIN hinzufügen | | | | 12 | *13* |
| Nutzer PIN's hinzufügen | | | | 13 | *13* |
| Nutzerkarten oder PIN's hinzufügen | | | | 15 | *13* |
| Nutzer löschen | | | | 14 | *14* |
| Schaltdauer Tür-Öffner-Relais | 3 s | | | 21 | *15* |
| Schaltdauer Alarm-Relais bei Abweisung | 2 s | | | 22 | *15* |
| Schaltdauer bei Alarmen / aktiven Eingängen | | | | 23-28 | *15* |
| PIN für Bedrohungsalarm | 00 | | | 29 | *16* |
| TTL-Ausgang Schaltdauer bei Bedrohungsalarm | 3 s | | | 30 | *17* |
| Test der Schaltdauern | | | | 31-37 | *17* |
| Schaltdauer Türglocke-Ausgang | 5 s | 77 | 78 | 39 | *17* |
| Dauerfreigabe | Deaktiviert | 41 | 42 | | *18* |
| Schnellzugriffmodus | Deaktiviert | 43 | 44 | | *18* |
| Toggle-Modus | Deaktiviert | 45 | 46 | | *18* |
| Türkontaktauswertung | Deaktiviert | 47 | 48 | | *19* |
| Tastentöne/Öffnungsbestätigung | Aktiviert | 52 | 51 | | *19* |
| Tastatursperre nach mehrfachen Falscheingaben | 60 s | | | 60 | *20* |
| Auswertung der Eingänge | Öffner | | | 61-70 | *20* |
| Konfiguration des TTL-Ausgang | Schließer | | | 71 / 72 | *21* |
| Verzögerungszeit der Türkontaktauswertung | 00 s | | | 81 | *21* |
| Anzahl der max. Falscheingaben | 5 | | | 82 | *22* |
| Zeitfenster für Codeeingabe | 20 s | | | 83 | *22* |
| Sabotagekontaktauswertung | Deaktiviert | 88 | 89 | 84 | *22* |
| Zurücksetzen auf Werkseinstellungen | | | | 99 | *23* |

# 10 Nutzer hinzufügen

## 10.1 Hinzufügen von RFID-Karten




Masterkarte | Kommando | neue Nutzerkarten | Masterkarte

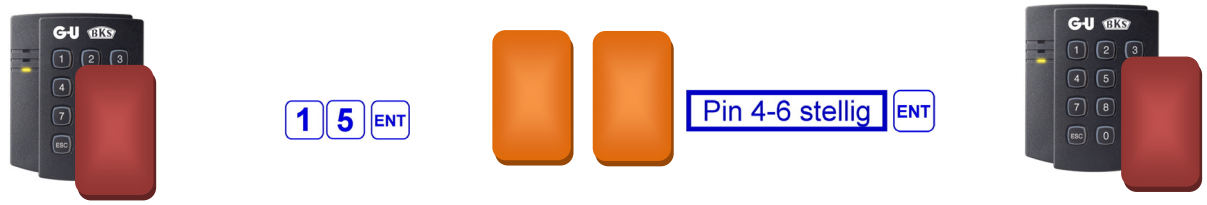
## 10.2 Hinzufügen von RFID-Karten + PIN


Masterkarte | Kommando | neue Nutzerkarten + PIN | Masterkarte

## 10.3 Hinzufügen von Nutzer-PINs


Master-PIN | Kommando | Nutzer-PIN | Master-PIN

## 10.4 Hinzufügen von Nutzerkarten oder PINs




Masterkarte | Kommando | neue Nutzerkarten oder PIN | Masterkarte

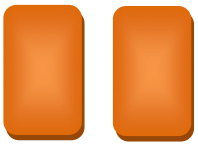
## 11 Nutzer Löschen

### 11.1 Löschen von RFID-Karten

Masterkarte

1 4 ENT

Kommando



zu löschende Nutzerkarten

Masterkarte

### 11.2 Löschen von Nutzer-PINs

Master PIN ENT

Master-PIN

1 4 ENT

Kommando

Pin 4-6 stellig ENT

zu löschende PIN-Nr.

Master PIN ENT

Abschließen

### 11.3 Gezieltes Löschen von einzelnen Karten

Sie können z.B. bei Verlust einer Nutzerkarte diese Löschen, ohne dass die Karte verfügbar ist. Voraussetzung ist jedoch, dass Sie die auf der Karte aufgedruckte Kartennummer bei der Ausgabe notiert haben. Zunächst wird das Tastenfeld zur Eingabe der Kartennummern aktiviert (Kommando 73), dann löschen Sie die verlorene Karte (Kommando 14) und deaktivierern schließlich die Eingabe der Kartennummern über das Tastenfeld (Kommando 74).

Masterkarte

7 3 ENT

Kommando

Der Tastenfeld-Eingang ist aktiviert um Kartennummern über das Tastenfeld eingeben zu können.

Masterkarte

1 4 ENT

Kommando

Jetzt die letzten 8 Stellen (Bsp. *802* **078 64231**, *hier 802 weglassen*) der Kartennummer der zu löschenden Karte plus ENT eingeben. Ggf. mit mehreren zu löschenden Kartennummern wiederholen.

Masterkarte

Masterkarte

7 4 ENT

Kommando

Tastenfeld-Eingang ist deaktiviert. Es können keine Kartennummern über das Tastenfeld eingegeben und auch keine Kartennummern mit der Tastatur gelöscht werden.

## 12 Erweiterte Einstellungen

Sie haben in den erweiterten Einstellungen die Möglichkeit, verschiedene Zustände der Zutrittskontrollsteuerung zu konfigurieren. Sie können über den Ausgangs-Modus festlegen, welcher Ausgang bei welchem Ereignis oder aktiven Eingang geschaltet wird.

| Bei einem Ereignis werden folgende Ausgänge geschaltet: | Ausgangs-Modus OM |
|---|---|
| Nur Türöffner-Relais | 51 |
| Nur Alarm-Relais | 52 |
| Nur TTL-Ausgang | 54 |
| Türöffner-Relais- + TTL-Ausgang | 55 |
| Alarm-Relais + TTL-Ausgang | 56 |

### 12.1 Türoffenzeit ändern

(tt= 00 – 99 s voreingestellt sind 3 s für das Türöffner-Relais und 0 s für den TTL-Ausgang)

2 1 ENT — t t ENT — t t ENT

Masterkarte | Kommando | Schaltdauer Tür-Öffner-Relais | Schaltdauer TTL-Ausgang

### 12.2 Alarmzeit bei falscher Karte oder PIN-Eingabe ändern

Siehe Tabelle für OM, tt = 00-99 s, Werkseinstellung Alarm-Relais = 2 s. Damit Beispielsweise bei einer nicht zutrittsberechtigten Karte oder PIN das Alarm-Relais und der TTL-Ausgang schalten, wählen Sie OM = 56. Da das Türöffner-Relais nicht schalten soll, geben sie hier 00 ein, dann die gewünschte Schaltdauer des Alarm-Relais, z.B. 05 für 5 s und die Schaltdauer des TTL-Ausgangs, z.B. 30 für 30 s.

2 2 ENT — O M ENT — t t ENT — t t ENT — t t ENT

| Masterkarte | Kommando | Ausgangs-Modus | Schaltdauer Tür-Öffner-Relais | Schaltdauer Alarm-Relais | Schaltdauer TTL-Ausgang |
|---|---|---|---|---|---|

### 12.3 Änderung der Alarmzeit bei Mehrfach-Falscheingaben des PIN

(Siehe Tabelle für OM, tt = 00-99 s, Werkseinstellung Alarm-Relais = 10 s)

2 3 ENT — O M ENT — t t ENT — t t ENT — t t ENT

| Masterkarte | Kommando | Ausgangs-Modus | Schaltdauer Tür-Öffner-Relais | Schaltdauer Alarm-Relais | Schaltdauer TTL-Ausgang |
|---|---|---|---|---|---|

## 12.4 Änderung der Alarmzeit bei Unterbrechung des Türkontakts

(Siehe Tabelle für OM, tt = 00 - 99 s)
Der Türkontakt ist standardmäßig als Öffner konfiguriert. Die Verzögerungszeit der Türkontaktauswertung muss eingestellt sein, siehe dazu 12.26. Diese Funktion ist nicht gleichzeitig mit 12.17 (Türkontaktauswertung) möglich!

2 4 ENT | OM ENT | tt ENT | tt ENT | tt ENT

| Masterkarte | Kommando | Ausgangs-Modus | Schaltdauer Tür-Öffner-Relais | Schaltdauer Alarm-Relais | Schaltdauer TTL-Ausgang |
|---|---|---|---|---|---|

## 12.5 Änderung der Alarmzeit: Hilfseingang Aux 1 - 3

(Siehe Tabelle für OM, tt = 00-99 s)

2 5 ENT Aux 1
2 6 ENT Aux 2
2 7 ENT Aux 3 | OM ENT | tt ENT | tt ENT | tt ENT

| Masterkarte | Kommando | Ausgangs-Modus | Schaltdauer Tür-Öffner-Relais | Schaltdauer Alarm-Relais | Schaltdauer TTL-Ausgang |
|---|---|---|---|---|---|

## 12.6 Änderung der Alarmzeit bei Sabotageversuch mittels Magneten

(Siehe Tabelle für OM, tt = 00 - 99 s)

2 8 ENT | OM ENT | tt ENT | tt ENT | tt ENT

| Masterkarte | Kommando | Ausgangs-Modus | Schaltdauer Tür-Öffner-Relais | Schaltdauer Alarm-Relais | Schaltdauer TTL-Ausgang |
|---|---|---|---|---|---|

## 12.7 Registrierung des 2-stelligen Bedrohungscodes für den Bedrohungsalarm

Sie können einen Bedrohungscode für den sog. Bedrohungsalarm festlegen. Wird dieser Code plus ENT vor der Lesung der Nutzerkarte oder des Nutzer-PIN eingegeben, so schaltet der TTL-Ausgang. Beachten Sie, dass „00“ der voreingestellte Code ist.

(PW = 00-99, Werkseinstellung PW= 00, bitte 7 7 ENT nicht als Code benutzen)

2 9 ENT | PW ENT

| Masterkarte | Kommando | Code |
|---|---|---|

## 12.8 Änderung der Alarmzeit nach Auslösung des Bedrohungsalarms

Hier legen Sie die Schaltdauer des TTL-Ausgangs bei einem Bedrohungsalarm fest.
(tt = 00 - 99 s, Werkseinstellung TTL-Zeit = 03 s, Deaktiv bei tt = 00)

3 0 ENT  t t ENT

Masterkarte  Kommando  Schaltdauer TTL-Ausgang

## 12.9 Testen von Alarmzeiten

3 1 ENT bis 3 7 ENT

Masterkarte  Kommandos

Durch das Blinken der gelben LED im 1 Hz Rhythmus (rote oder grüne LED leuchten jeweils für die Dauer der eingestellten Aktion) wird die Dauer der Kontaktgabe angezeigt.
Wenn keine Zeit eingestellt wurde, blinkt die gelbe LED im Normalbetriebsmodus (1 Hz) und die rote und die grüne LED werden vom System nicht angesteuert.

| | |
|---|---|
| Test der unter Kommando 21 eingestellten Türoffenzeit | 3 1 ENT |
| Test der unter Kommando 22 eingestellten Alarmzeit bei falscher Karte oder PIN-Eingabe | 3 2 ENT |
| Test der unter Kommando 23 eingestellten Alarmzeit bei Mehrfach-Falscheingabe | 3 3 ENT |
| Test der unter Kommando 24 eingestellten Alarmzeit bei Unterbrechung des Türkontakts | 3 4 ENT |
| Test der unter Kommando 25 eingestellten Alarmzeit Hilfseingang Aux 1 | 3 5 ENT |
| Test der unter Kommando 26 eingestellten Alarmzeit Hilfseingang Aux 2 | 3 6 ENT |
| Test der unter Kommando 27 eingestellten Alarmzeit Hilfseingang Aux 3 | 3 7 ENT |

## 12.10 Änderung der Schaltdauer des Türglocke-Ausgangs

(tt = 00 - 99 s, Werkseinstellung = 05 s)

3 9 ENT  t t ENT

Masterkarte  Kommando  Schaltdauer Türglocke-Ausgang

## 12.11 Aktivierung Dauerfreigabe

4 1 ENT

Masterkarte Kommando

Die Tür ist dauerhaft freigegeben. Karten/PIN's werden nicht gelesen. Diese Funktion ist mit einer Masterkarte immer schaltbar!

## 12.12 Deaktivierung der Dauerfreigabe

4 2 ENT

Masterkarte Kommando

## 12.13 Aktivierung des Schnell-Zugangsmodus (Zutritt ohne Prüfung der Zutrittsberechtigung)

4 3 ENT

Masterkarte Kommando

Wenn der Schnell-Zugangsmodus aktiviert ist, genügt zum Öffnen der Tür die ENT Taste zu betätigen.
Diese Funktion ist nur mit einer Masterkarte zu aktivieren!

## 12.14 Deaktivierung des Schnell-Zugangsmodus

(Werkseinstellung = Deaktiviert)

4 4 ENT

Masterkarte Kommando

## 12.15 Aktivierung des Schritt-Schalt-Modus (Toggle-Modus)

4 5 ENT

Masterkarte Kommando

Ist der Schritt-Schalt-Modus aktiviert, wird das Türöffner-Relais dauerhaft ein- oder ausgeschaltet, sobald eine registrierte Karte oder PIN eingegeben wird. Man kann diese Funktion z.B. zum Scharf- / Unscharf-Schalten einer Einbruchmeldeanlage oder zur Ansteuerung einer Garagentoransteuerung nutzen.

## 12.16 Deaktivierung des Schritt-Schalt-Modus (Toggle-Modus)

4 6 ENT

Masterkarte Kommando

## 12.17 Türkontaktauswertung aktivieren

4 7 ENT

Masterkarte Kommando

Wird die Türkontaktauswertung aktiviert, schaltet das Türöffner-Relais bei geöffneter Tür permanent. Wird die Tür wieder geschlossen, fällt das Türöffner-Relais wieder ab. Wird die Tür bei einer Freigabe nicht geöffnet, so schaltet das Türöffner-Relais für die vorgegebene Schaltdauer. Standardmäßig wird hier ein Schließer erwartet, d.h. geschlossener Kontakt bei geschlossener Tür.
**Diese Funktion ist nicht gleichzeitig mit 12.4 (Alarm bei Unterbrechung des Türkontaktes) möglich!**

## 12.18 Türkontaktauswertung deaktivieren

4 8 ENT

Masterkarte Kommando

## 12.19 Deaktivierung der Tastentöne/Öffnungsbestätigung

5 1 ENT

Masterkarte Kommando

## 12.20 Aktivierung der Tastentöne/Öffnungsbestätigung (Werkseinstellung)

5 2 ENT

Masterkarte Kommando

## 12.21 Änderung der Abschaltdauer der Tastatur nach einer Mehrfach-Falscheingabe

(mm = 00 - 99 min, Werkseinstellung = 01 min)

6 0 ENT  m m ENT

Masterkarte  Kommando  Abschaltdauer in Minuten

## 12.22 Eingangs-Einstellungen

6 1 ENT bis 7 0 ENT

Masterkarte  Kommandos

| | |
|---|---|
| Auswertung der steigenden Flanke (Schließerkontakt) am Hilfseingang Aux 1 | 6 1 ENT |
| Auswertung der fallenden Flanke (Öffnerkontakt) am Hilfseingang Aux 1 (Werkseinstellung) | 6 2 ENT |
| Auswertung der steigenden Flanke (Schließerkontakt) am Hilfseingang Aux 2 | 6 3 ENT |
| Auswertung der fallenden Flanke (Öffnerkontakt) am Hilfseingang Aux 2 (Werkseinstellung) | 6 4 ENT |
| Auswertung der steigenden Flanke (Schließerkontakt) am Hilfseingang Aux 3 | 6 5 ENT |
| Auswertung der fallenden Flanke (Öffnerkontakt) am Hilfseingang Aux 3 (Werkseinstellung) | 6 6 ENT |
| Auswertung steigende Flanke (Schließerkontakt) am Eingang Tür-Freigabe-Taster | 6 7 ENT |
| Auswertung fallende Flanke (Öffnerkontakt) am Eingang Tür-Freigabe-Taster | 6 8 ENT |
| Auswertung steigende Flanke (Schließerkontakt) am Eingang Türkontakt | 6 9 ENT |
| Auswertung fallende Flanke (Öffnerkontakt) am Eingang Türkontakt | 7 0 ENT |

## 12.23 Ausgangs-Einstellungen

7 1 ENT bis 7 8 ENT

Masterkarte Kommandos

| | |
|---|---|
| TTL-Ausgang ändert seinen Status von logisch 0 zu logisch 1 (Schließerkontakt) bei Aktivierung. | 7 1 ENT |
| TTL-Ausgang ändert seinen Status von logisch 1 zu logisch 0 (Öffnerkontakt) bei Aktivierung (Werkseinstellung). | 7 2 ENT |
| Aktivierung des Türglocke-Ausgangs (Werkseinstellung). | 7 7 ENT |
| Deaktivierung des Türglocke-Ausgangs. | 7 8 ENT |

## 12.24 Aktivierung des Tastenfeldes zur Eingabe der Kartennummern

7 3 ENT

Masterkarte Kommando

Der Tastenfeld-Eingang ist aktiviert um Kartennummern über das Tastenfeld eingeben zu können.
In dieser Betriebsart erfolgt die Öffnung der Tür durch Eingabe der letzten 8 Stellen (Bsp. *802* **078 64231**, *hier 802 weglassen*) der Kartennummer und ENT

## 12.25 Deaktivierung des Tastenfeldes zur Eingabe der Kartennummern

7 4 ENT

Masterkarte Kommando

Tastenfeld Eingang ist deaktiviert. Es können keine Kartennummern über das Tastenfeld eingegeben und auch keine Kartennummern mit der Tastatur gelöscht werden.

## 12.26 Einstellung der Verzögerungszeit der Türkontaktauswertung

8 1 ENT t t ENT

Masterkarte Kommando Dauer der Verzögerungszeit

(tt = 00 - 99 s, Werkseinstellung = 00 s hat keine Detektierung der Tür zur Folge, siehe „Einstellung von Alarmzeiten“.12.4

### 12.27 Begrenzung der Anzahl der möglichen Falscheingaben

(NN = 00 - 99, Werkseinstellung Anzahl = 05)

8 2 ENT  N N ENT

Masterkarte  Kommando  Anzahl der möglichen Falscheingaben

### 12.28 Zeitfenster für Codeeingabe

(tt = 10 - 99 s, Werkseinstellung Zeitfenster = 20 s Minimum tt = 10 s)

8 3 ENT  t t ENT

Masterkarte  Kommando  Zeitfenster für Codeeingabe

### 12.29 Einstellung des Sabotage-Alarmausgang

Hier legen Sie fest, welcher Ausgang bei einem Sabotagealarm schalten soll (siehe Tabelle für OM)

8 4 ENT  O M ENT

Masterkarte  Kommando  Ausgangs-Modus

### 12.30 Aktivierung des Sabotage-Alarms

Um die Anforderungen der UL 294 zu erfüllen, muss der Sabotagealarm aktiviert sein.

8 8 ENT

Masterkarte  Kommando

### 12.31 Deaktivierung des Sabotage-Alarms (Werkseinstellung)

8 9 ENT

Masterkarte  Kommando

## 12.32 Zurücksetzen auf Werkseinstellung und Löschen aller Zutrittsberechtigungen

Masterkarte


Kommando

Bitte benutzen Sie dieses Kommando, wenn Sie alle eingegebenen Daten löschen und neu beginnen wollen. Anschließend beginnen Sie mit der Eingabe der Masterkarte oder des Master-PIN's wie unter Kapitel 8 beschrieben.

## Kontakt

Internet http://www.g-u.de oder http://www.bks.de.

Telefonnummern bei Fragen zu den Produkten:
+49 7156 301 0 oder +49 2051 201 0

BKS GmbH, D-42502 Velbert
Telefon (02051) 201-0
Telefax (02051) 201-431
www.g-u.com

**Hinweis**

# Installation Instructions

# Access Control Unit C-S P 100
# C-S A 100

## Contents

## 1 Abbreviations

| | | | |
|---|---|---|---|
| DC | Direct Current | LED | Light Emitting Diode |
| OM | Output mode | PIN | Personal Identification Number |
| RFID | Radio Frequency Identification | TTL | Transistor-transistor logic (here : transistor switching output) |

**Warning !**
Sign indicating danger and the importance of observing guidelines.

**Attention !**
Sign referring to information with regard to correct and professional job execution.

**Call to action !**
Sign demanding your action (work step).

**Disposal**
The disused Access Control Unit must be disposed of as electronic waste at a special waste collection site. This product must not be disposed of as domestic waste !
Casing and packing must be disposed of separately.

## 2 Safety Advice

- Before you start doing any installation, repair, service or adjustment work, ensure that no voltage is applied to any of the mains adapters to avoid unintended switch-on.
- The electrical connection may only be performed by trained personnel.
- It is important that the particular regional and/or local installation directives and regulations should be observed. This applies especially to VDE directives, DIN VDE 0100, DIN VDE 0160, DIN VDE 0632 EN 50133-1 / DIN VDE 0830 Part 8-1:2003-09, EN 50133-2-1 / DIN VDE 0830 Part 8-2-1:2001-08, EN 50133-7 / DIN VDE 0830 Part 8-7:2000-04.
- All primary safety measures on site are the responsibility of the customer. The power supply must be provided with a cut-out.
- (Within Germany,) it is important that the DIN VDE 0100 directive and MLAR directive (Muster-Leitungsanlagen Richtlinie) should be observed.
- No liability is assumed for damage arising from improper use, assembly and installation, and from use of non-original parts and accessories !
- In case of damage caused by non-observance of these instructions all claims for guarantee will become extinct. No liability is assumed for consequential damage !
- With regard to safety and to product approval (CE), it is not permitted to change or alter the product in any manner without our authorisation.
- The observance of the installation instructions given ensures optimal functioning and a long service life of the unit.
- Please verify that the product delivered is complete and undamaged. We assume no liability for damage arising from improper use.
- ATTENTION : It is absolutely necessary that the appropriate industrial safety regulations and safety regulations of the trade associations should be followed during installation and maintenance.

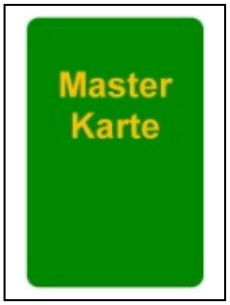
## 3 Technical Data

| | |
|---|---|
| **Type** | C-S P 100, C-S A 100 |
| **CPU** | 8 Bit microprocessor |
| **Memory** | Program memory 20 KByte ROM<br>Data memory 2 KByte ROM |
| **Number of users** | 512 |
| **Voltage/Current** | DC 12 V, 0.2 A |
| **IP Protection class** | 20 |
| **Reader connection** | 26 Bit Wiegand (4/8 Bit Burst for PIN) |
| **Input terminals** | 5 (e.g., door release button, door contact, auxiliary inputs Aux 1, Aux2, Aux3) |
| **Output terminals** | 2 relay outputs: max. DC 18 V, 2 A<br>1 alarm transmitter : DC 5 V, 500 mA<br>1 TTL : DC 5 V, 20 mA |
| **LED indication** | 3 LEDs (Red, Green, Yellow) |
| **Acoustic signal** | Piezo buzzer |
| **Operating temperature** | -35° C to +65° C |
| **Air humidity** | 10% to 90% relative air humidity without condensation |
| **Dimensions (W x H x D)** | 87 mm x 100 mm x 31 mm |
| **Certificates/Approvals** | FCC, CE, MIC |

BKS GmbH hereby declare that this appliance fully complies with the basic requirements and further relevant regulations specified in the directive 1999/5/EC

## 4 Scope of delivery








- Access control unit
- Mounting plate
- 5 O-rings
- Master card
- 4 screws (3.5 x 40)
- 4 screws (M3 x 12)
- 4 dowels
- Brief instruction
- Cable

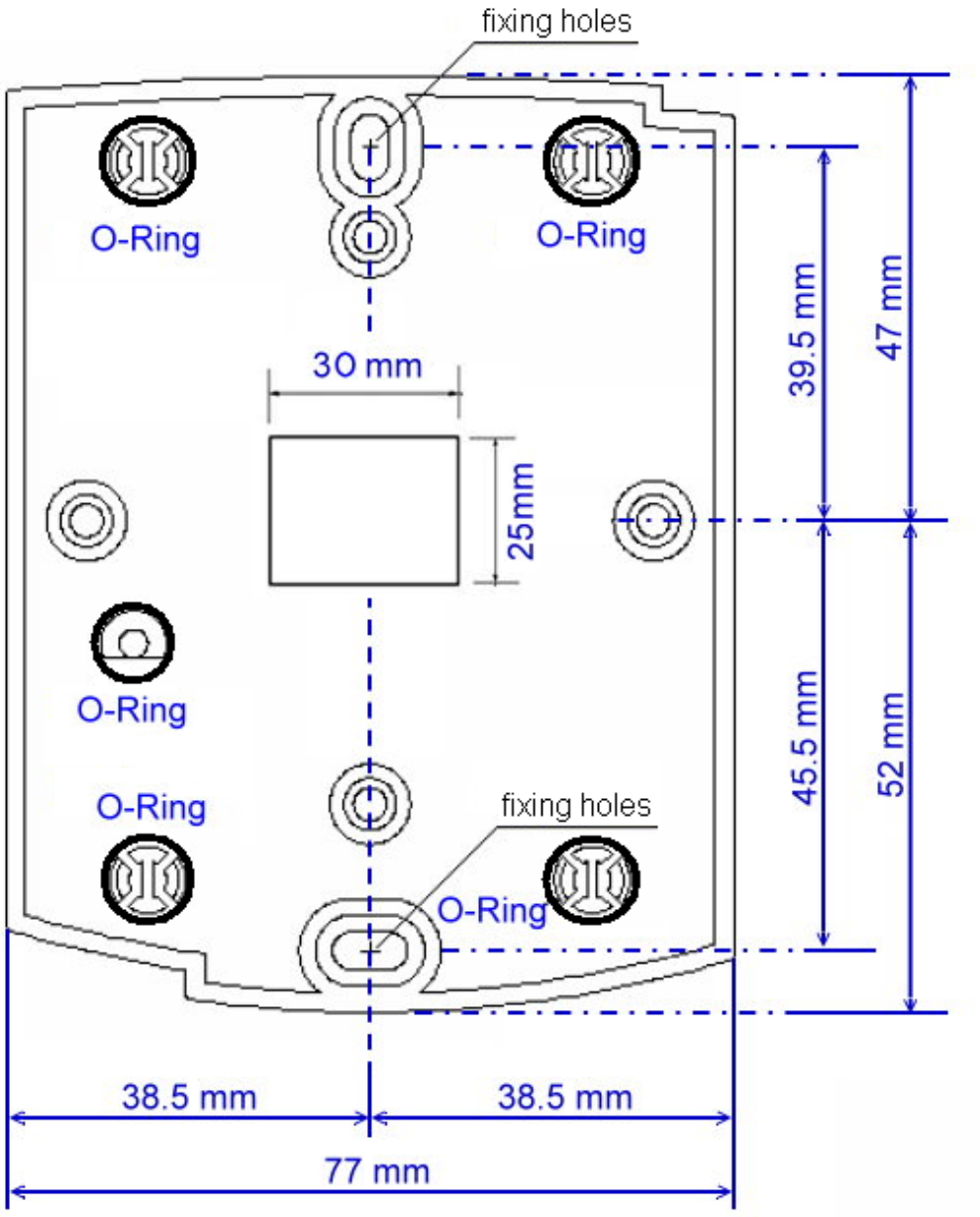
## 5 Installation

The electrical connection may only be carried out by trained personnel and must be performed in compliance with the particular national regulations.

Take the control unit from the packing.

Attach the mounting plate on a smooth surface using the sheet metal screws or the M3 screws enclosed. Drill a hole at centre for the connecting cable.

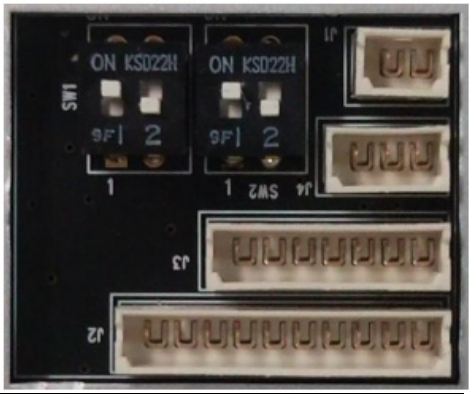
Before finally mounting the control unit, you should connect the wires and verify its proper functioning. Put 4 O-rings on the snap-on fixtures and 1 O-ring on the plug for the sabotage contact. Press the control unit on the mounting plate ensuring that it snaps into place correctly.



## 6 Electrical Connection

| Connector | Signal | Wire Colour |
|---|---|---|
| J1 | Voltage (+12 V) | red |
| | Ground (GND) | black |
| J2 | Output door opener relay (COM) | grey/red |
| | Output door opener relay (NC) | blue/white |
| | Output door opener relay (NO) | white/red |
| | Output alarm relay (COM) | white |
| | Output alarm relay (NC) | purple/white |
| | Output alarm relay (NO) | purple |
| | Input door release button | orange |
| | Input door contact | yellow/red |
| | AUX input 1 | green |
| | AUX input 2 | green/white |
| J3 | Input Wiegand Data 0 | pink |
| | Input Wiegand Data 1 | light blue |
| | TTL output | orange/white |
| | Buzzer output | brown/white |
| | AUX input 3 | green/red |
| | Reserve | blue/red |
| | Reserve | yellow/white |
| J4 | RS232-TX | black/white |
| | RS232-RX | red/white |
| | Ground (GND) | black |

**DIP-Switch (optional Wiegand-Output)**
The default output format is TTL and Buzzer output. But, you can configure the output to generate output in Wiegand format and use it like a reader. (The device can output data from card reading, but cannot output data from keypad input.)
If you want to generate Wiegand instead of TTL output format, follow the table below.

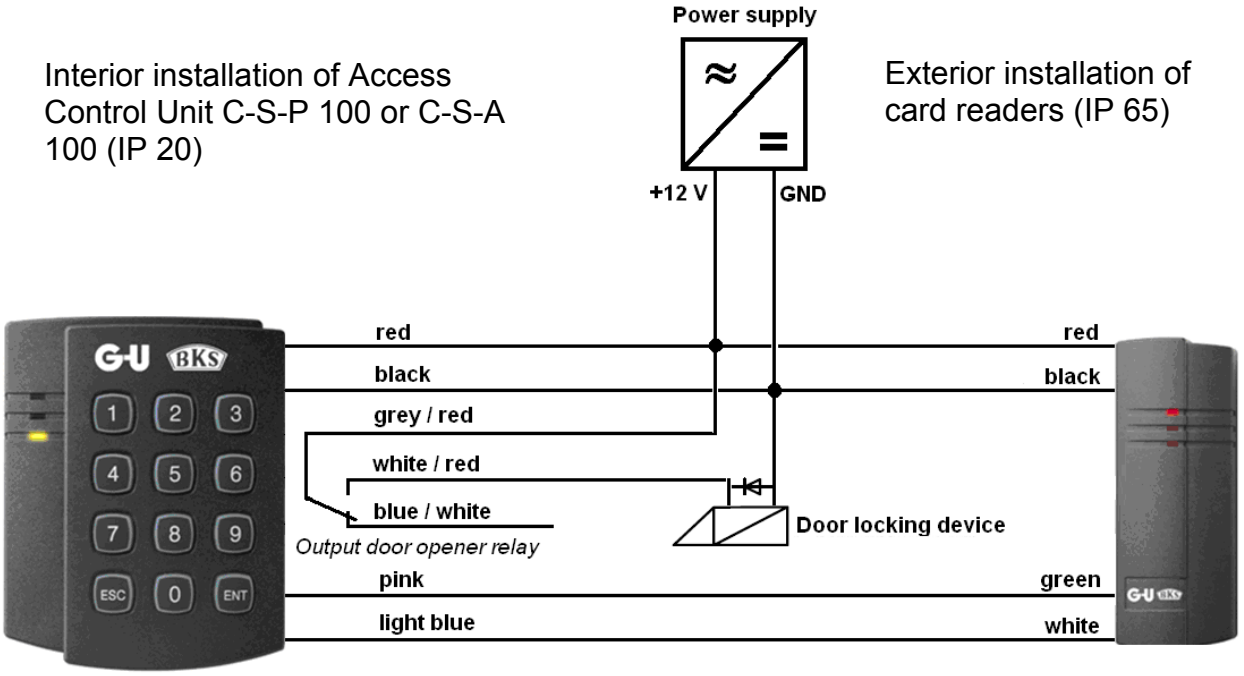



| SW1 (1) | SW1 (2) | SW2 (1) | SW2 (2) | orange/white | brown/white |
|---|---|---|---|---|---|
| ON | OFF | ON | OFF | TTL output | Buzzer output |
| OFF | ON | OFF | ON | Wiegand Data 0 output | Wiegand Data 1 output |

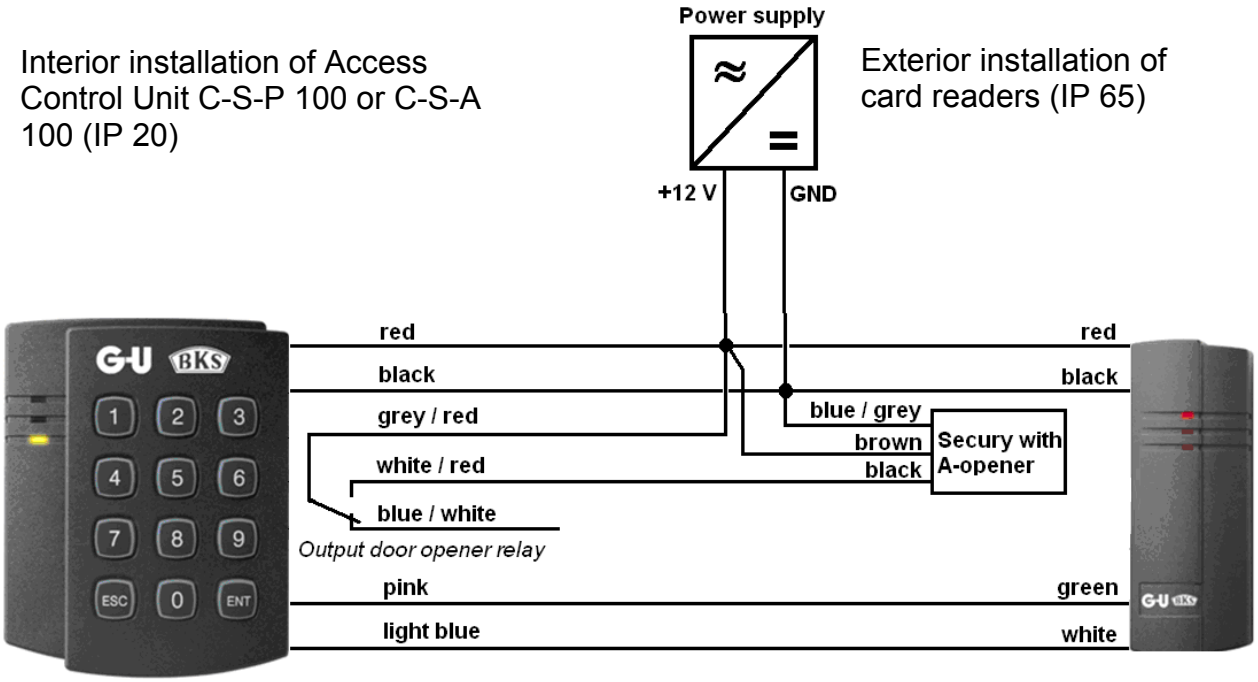
## 7 Connection Examples

The connecting cables for the readers can be extended by means of the butt connectors enclosed. For the extension of the local access line we recommend to use telecommunication cable type J-Y(ST)Y 2 x 2 x 0.8. Maximum cable length 50 m. The door locking devices used must feature a flyback diode.

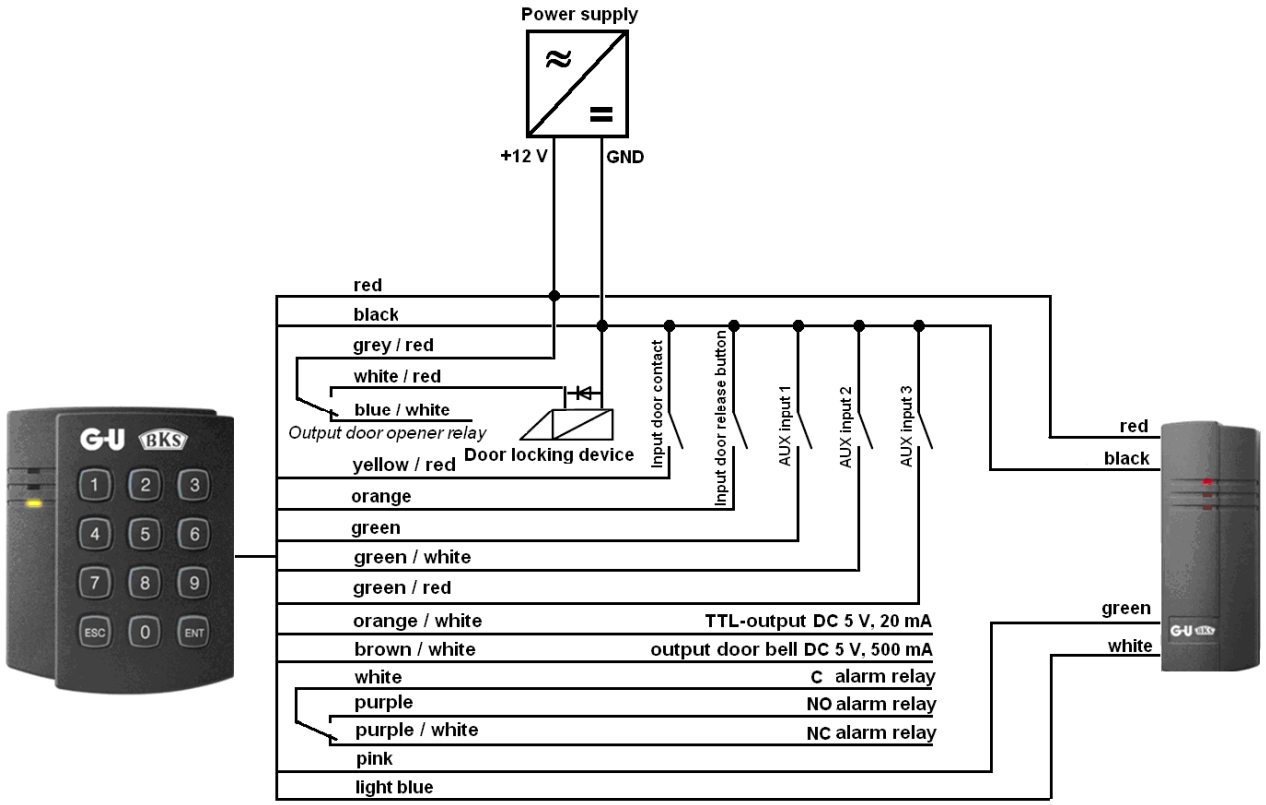
### 7.1 Connecting Outside Card Reader and Door Locking Device




### 7.2 Connecting Outside Card Reader and Door Lock SECURY with A-Opener



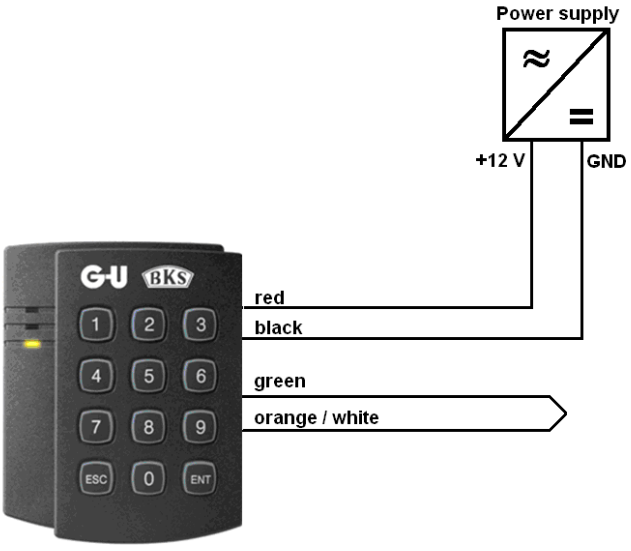
## 7.3 Maximal Connections




## 8 Initialisation/Reset

Before start-up, every Access Control Unit should be initialised. During the initialisation process, the factory settings of the manufacturer are loaded and all memorised data deleted. This procedure is also suited for reset and total memory deletion in case of loss of the master card.

1. Disconnect the control unit from the mains.
2. Connect the green with the orange/white wire.
3. Apply voltage again.
4. All LEDs are flashing, the acoustic signal is heard.
5. Disconnect wires and isolate them from each other.



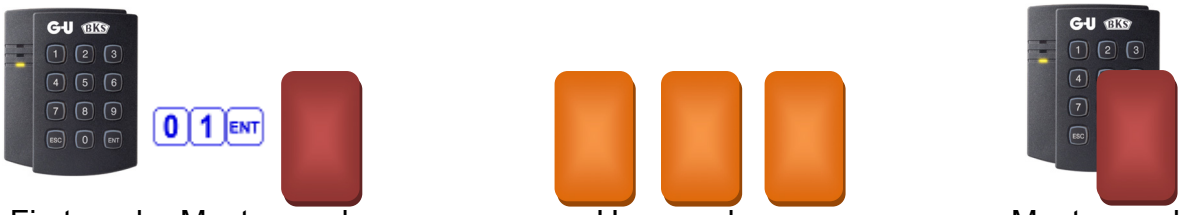

In normal operation, the wires not used must be isolated from each other appropriately to prevent accidental reset !

## 8.1 Determining the Operating Mode

Press the keys 0, 1 and ENT in sequence to make the access control unit accept RFID cards for authorisation verification. By pressing the keys 0, 2 and ENT in sequence, the RFID cards are verified together with a PIN entered by the user. Please note that you have the possibility to work with PIN codes only, or alternatively with PIN and card.

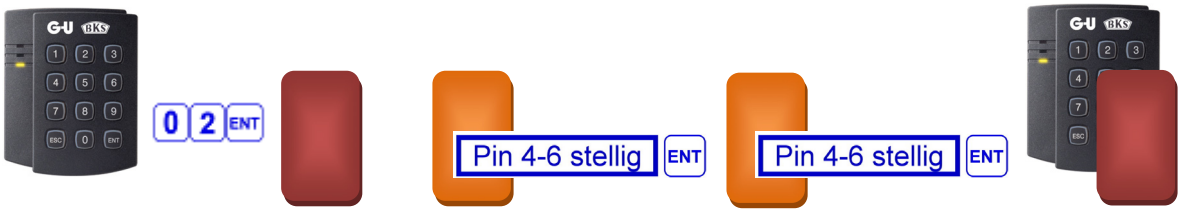

## 8.2 Operating Mode 1 : RFID Card Identification

6. Initialise the control unit as described above. After correct initialisation, all 3 LEDs flash at the same rhythm.
7. Press the keys 0, 1 and ENT in sequence to make the access control unit accept RFID cards for authorisation verification.
   *Please note that you have the possibility to work with PIN codes only, or to use operating modes 2, 3, 5 (see descriptions below).*
8. Insert any RFID card. This very first RFID card is the master card now.
9. Read in the user cards one by one (512 cards at the maximum)
10. To finish the programming, read in the master card once more.




## 8.3 Operating Mode 2 : RFID Cards + PIN Identification

6. Initialise the control unit as described above. After correct initialisation, all 3 LEDs flash at the same rhythm.
7. Press the keys 0, 2 and ENT in sequence to make the access control unit accept RFID cards plus a 4 to 6 digit user PIN code for authorisation verification.
8. Insert any RFID card. This very first RFID card is the master card now.
9. Now read in a user card, enter the 4 to 6 digit user PIN and confirm with ENT (max. 512 user cards possible)
10. To finish the programming, read in the master card once more.



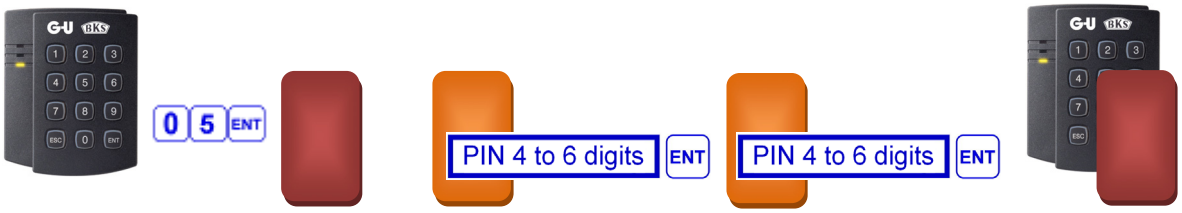
### 8.4 Operating Mode 3: PIN Identification

6. Initialise the control unit as described above. After correct initialisation, all 3 LEDs flash at the same rhythm.
7. By pressing the keys 0, 3 and ENT in sequence, the access control unit is caused to accept a 4 to 6-digit PIN code for authorisation verification.
8. Enter a 4 to 6-digit PIN code and finish by pressing ENT. This PIN code is the master PIN code now.
9. Enter the user PINs (4 to 6 digits) one by one (512 users at the maximum) and confirm with ENT.
10. To finish the programming, re-enter the master PIN and confirm with ENT.


Operating mode 3 | Master PIN | User PIN | Master PIN

### 8.5 Operating Mode 5 : RFID Card or PIN Identification

6. Initialise the control unit as described above. After correct initialisation, all 3 LEDs flash at the same rhythm.
7. By pressing the keys 0, 5 and ENT in sequence, the access control unit is caused to accept a 4 to 6-digit PIN code or an RFID card for authorisation verification.
8. Insert any RFID card. This very first RFID card is the master card now.
9. Next, read in a user card, enter the 4 to 6-digit user PIN, and confirm with ENT (max. 512 user cards possible).
10. To finish the programming, re-enter the master PIN and confirm with ENT.




First card = Master card | User card or PIN | Master card

## 9 Operation

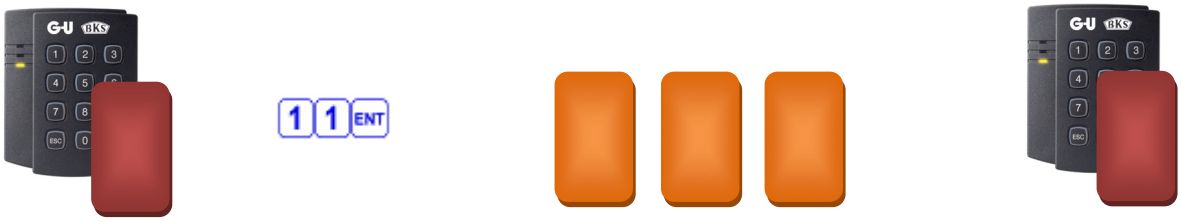
- Yellow LED flashing indicates normal operation.
- If an identification is accepted, the door opener relay switches for 3 seconds, the green LED of the control unit lights up for 3 s.
- If an identification is rejected, the alarm relay switches for 2 seconds and the red LED lights up for 2 s.
- When the door release button is pressed, the control unit responds as if released via a user card (door opener relay switches for 3 s)
- In the event of a personal threat enter the 2-digit threat password (factory setting 00) before inserting the card. The door will open as usual, except that the threat alarm will be activated (TTL output) and security personnel alarmed (provided an appropriate system is installed).
- By pressing the ESC button, the door bell output can be activated for 5 s.

## 9.1 Factory Settings

| | | Command (keypad entry) | | | |
|---|---|---|---|---|---|
| **Function** | **Default** | **Activate** | **Deactivate** | **Change** | ***Page*** |
| Adding user cards | | | | 11 | *37* |
| Adding user cards plus PINs | | | | 12 | *37* |
| Adding user PINs | | | | 13 | *37* |
| Adding user cards or PINs | | | | 15 | *37* |
| Deleting users | | | | 14 | *38* |
| Switching time of door opener relay | 3 s | | | 21 | *39* |
| Switching time of alarm relay at refusal | 2 s | | | 22 | *39* |
| Switching time at alarms / active inputs | | | | 23-28 | *39* |
| PIN for threat alarm | 00 | | | 29 | *40* |
| Switching time of TTL outputs at threat alarm | 3 s | | | 30 | *41* |
| Testing the switching times | | | | 31-37 | *41* |
| Switching time of door bell output | 5 s | 77 | 78 | 39 | *41* |
| Permanent release | deactivated | 41 | 42 | | *42* |
| Rapid access mode | deactivated | 43 | 44 | | *42* |
| Toggle mode | deactivated | 45 | 46 | | *42* |
| Door contact evaluation | deactivated | 47 | 48 | | *43* |
| Key sounds | activated | 52 | 51 | | *43* |
| Keypad interlock after false entries | 60 s | | | 60 | *44* |
| Input evaluation | Door opener | | | 61-70 | *44* |
| TTL output configuration | Door closer | | | 71 / 72 | *45* |
| Time lag of door contact evaluation | 00 s | | | 81 | *45* |
| Max. number of incorrect keypad entries | 5 | | | 82 | *46* |
| Time window for code entries | 20 s | | | 83 | *46* |
| Sabotage contact evaluation | deactivated | 88 | 89 | 84 | *46* |
| Reset to factory settings | | | | 99 | *47* |

# 10 Adding Users

## 10.1 Adding RFID Cards




Master card | Keypad entry | New user cards | Master card

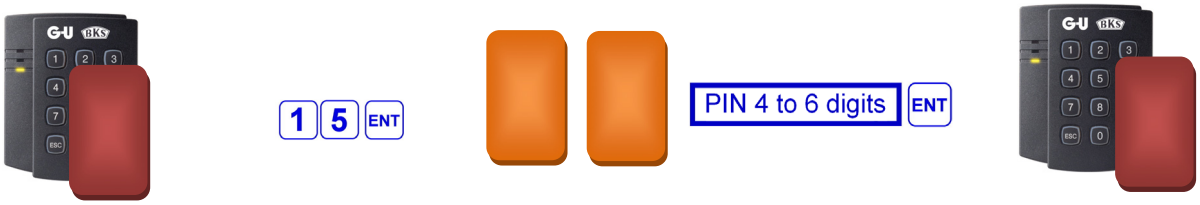
## 10.2 Adding RFID Cards + PIN


Master card | Keypad entry | New user cards + PIN | Master card

## 10.3 Adding User PINs


Master PIN | Keypad entry | User PIN | Master PIN

## 10.4 Adding User Cards or PINs




Master card | Keypad entry | New user cards or PIN | Master card

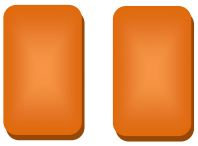
## 11 Deleting User PINs

### 11.1 Deleting RFID Cards

Master card

1 4 ENT

Keypad entry



User cards for deletion

Master card

### 11.2 Deleting User PINs

Master PIN ENT

Master PIN

1 4 ENT

Keypad entry

PIN 4 to 6 digits ENT

User PIN for deletion

Master PIN ENT

Finish

### 11.3 Selected Deletion of Individual Cards

A lost or stolen user card can be deleted without being physically available, provided the owner has written down the number printed on it. First, the keypad is activated to accept the entry of card numbers (entry 73); next, it is prepared to delete the number(s) of the lost card(s) (entry 14); finally, the keypad is deactivated again to refuse the entry of card numbers (entry 74).

Master card

7 3 ENT

Keypad entry

The keypad is activated to accept the entry of the card number.

Master card

1 4 ENT

Keypad entry

Now enter the last 8 digits (example *802* **078 64241,** *omit "802")* of the card to be deleted plus ENT. Repeat the procedure for deleting several cards.

Master card

Master card

7 4 ENT

Keypad entry

Keypad is deactivated. It is not possible to enter or delete card numbers with the numeric keys.

## 12 Extended Setting Functions

A range of extended setting functions allows to configure different statuses of the access control unit. In Output Mode it is possible to determine which output is to be switched at which event or active input.

| Outputs to be switched at a particular event : | Output Mode OM |
|---|---|
| Door opener relay only | 51 |
| Alarm relay only | 52 |
| TTL output only | 54 |
| Door opener relay + TTL output | 55 |
| Alarm relay + TTL output | 56 |

### 12.1 Changing the Door Open Time

tt= 00 – 99 s (factory settings : 3 s for door opener relay and 0 s for TTL output)

Master card — 2 1 ENT — Keypad entry — t t ENT — Switching time door opener relay — t t ENT — Switching time TTL output

### 12.2 Changing the Alarm Switching Time in Case of False Card or PIN

See table for OM, tt = 00 - 99 s, factory setting for alarm relay = 2 s. For alarm relay and TTL output to be switched in case of an unauthorised card or PIN, select OM = 56. Since the door opener relay is not supposed to switch, you have to enter 00 and then determine the switching time of the alarm relay, e.g., 05 for 5 s, as well as the switching time of the TTL output, e.g., 30 for 30 s.

Master card — 2 2 ENT — Keypad entry — O M ENT — Output mode — t t ENT — Switching time Door op. relay — t t ENT — Switching time Alarm relay — t t ENT — Switching time TTL output

### 12.3 Changing the Alarm Switching Time at Repeated Entry of False PIN

See table for OM, tt = 00 - 99 s (factory setting for alarm relay = 10 s)

Master card — 2 3 ENT — Keypad entry — O M ENT — Output mode — t t ENT — Switching time Door op. relay — t t ENT — Switching time Alarm relay — t t ENT — Switching time TTL output

## 12.4 Changing the Alarm Switching Time at Interruption of Door Contact

(See table for OM, tt = 00 - 99 s)
The door contact is configured as opener as a standard. The time lag of the door contact evaluation must be set, see chapter 12.26. This function is not possible with function 12.17 (Door Contact Evaluation) activated !

2 4 ENT | O M ENT | t t ENT | t t ENT | t t ENT

| Master card | Keypad entry | Output mode | Switching time Door op. relay | Switching time Alarm relay | Switching time TTL output |
|---|---|---|---|---|---|

## 12.5 Changing the Alarm Switching Time : Auxiliary Inputs Aux 1 - 3

(See table for OM, tt = 00 - 99 s)

2 5 ENT Aux 1
2 6 ENT Aux 2
2 7 ENT Aux 3

O M ENT | t t ENT | t t ENT | t t ENT

| Master card | Keypad entry | Output mode | Switching time Door op. relay | Switching time Alarm relay | Switching time TTL output |
|---|---|---|---|---|---|

## 12.6 Changing the Alarm Switching Time at Attempted Sabotage with Magnet

(See table for OM, tt = 00 - 99 s)

2 8 ENT | O M ENT | t t ENT | t t ENT | t t ENT

| Master card | Keypad entry | Output mode | Switching time Door op. relay | Switching time Alarm relay | Switching time TTL output |
|---|---|---|---|---|---|

## 12.7 Registering a 2-Digit Threat Code for Threat Alarm

You can determine a threat code for the so-called threat alarm. If this code is entered plus ENT before the user card is read or the user PIN entered, the TTL output will switch. Please note that the preset code is "00".

(Access key = 00 - 99, factory setting is PW = 00, do not use 7 7 ENT as code)

2 9 ENT | P W ENT

| Master card | Keypad entry | Access key ("password") |
|---|---|---|

## 12.8 Changing the Alarm Switching Time after Released Threat Alarm

Here you determine the switching time of the TTL output in the event of a threat alarm.
(tt = 00 - 99 s, factory-set TTL time = 03 s, deactivated at tt = 00)

3 0 ENT  t t ENT

Master card  Keypad entry  Switching time TTL output

## 12.9 Testing Alarm Switching Times

3 1 ENT up to 3 7 ENT

Master card  Keypad entries

Yellow LED flashing at a 1-Hz rhythm indicates the duration of contact making (red or green LED lights up over duration of the function set).
If no time has been set, the yellow LED flashes in standard operating mode (1 Hz); neither red nor green LED are triggered.

| | |
|---|---|
| Testing the door open time set with entry 21 | 3 1 ENT |
| Testing the alarm time set with entry 22 for false card or PIN | 3 2 ENT |
| Testing the alarm time set with entry 23 for repeated entry of false PIN | 3 3 ENT |
| Testing the alarm time set with entry 24 for door contact interruption | 3 4 ENT |
| Testing the alarm time set with entry 25 for auxiliary input Aux 1 | 3 5 ENT |
| Testing the alarm time set with entry 26 for auxiliary input Aux 2 | 3 6 ENT |
| Testing the alarm time set with entry 27 for auxiliary input Aux 3 | 3 7 ENT |

## 12.10 Changing the Switching Time of the Door Bell Output

(tt = 00 - 99 s, factory setting = 05 s)

3 9 ENT  t t ENT

Master card  Keypad  Switching time of door bell output

## 12.11 Activating the Permanent Door Release

4 1 ENT

Master card Keypad entry

Door is released permanently. Cards/PINs are not read. With a master card, this function is available at any time !

## 12.12 Deactivating the Permanent Door Release

4 2 ENT

Master card Keypad entry

## 12.13 Activating the Rapid Access Mode (Access without Authorisation Verification)

4 3 ENT

Master card Keypad entry

When the Rapid Access Mode is activated, the door can be opened by simply pressing ENT.
This function is available with master card onlv.

## 12.14 Deactivating the Rapid Access Mode

(Factory setting = deactivated)

4 4 ENT

Master card Keypad entry

## 12.15 Activating the Toggle Mode

4 5 ENT

Master card Keypad entry

With the Toggle Mode activated, the door opener relay is permanently switched on or off, as soon as an authorised card or PIN is used. With this function it is possible to activate or deactivate a burglar alarm system or to control a garage door.

## 12.16 Deactivating the Toggle Mode

4 6 ENT

Master card  Keypad entry

## 12.17 Activating the Door Contact Evaluation

4 7 ENT

Master card  Keypad entry

If you enable the Door Contact Evaluation, the Door only is locked followed by Door Contact so the door will remain open until the door is completely closed.
**This function is not possible with function 12.4 (Alarm at door contact interruption) activated !**

## 12.18 Deactivating the Door Contact Evaluation

4 8 ENT

Master card  Keypad entry

## 12.19 Deactivating the Key Sounds / Acoustic Opening response

5 1 ENT

Master card  Keypad entry

## 12.20 Activating the Key Sounds / Acoustic Opening response (Factory Setting)

5 2 ENT

Master card  Keypad entry

## 12.21 Changing the Keypad Switch-Off Time After Repeated False Entry

(mm = 00 - 99 min, factory setting = 01 min)

6 0 ENT  m m ENT

Master card  Keypad entry  Switch-off time in minutes

## 12.22 Input Settings

6 1 ENT bis 7 0 ENT

Master card  Keypad entries

| | |
|---|---|
| Evaluation of rising edge of pulse (closer contact) at input Aux 1 | 6 1 ENT |
| Evaluation of falling edge of pulse (opener contact) at input Aux 1 (factory setting) | 6 2 ENT |
| Evaluation of rising edge of pulse (closer contact) at input Aux 2 | 6 3 ENT |
| Evaluation of falling edge of pulse (opener contact) at input Aux 2 (factory setting) | 6 4 ENT |
| Evaluation of rising edge of pulse (closer contact) at input Aux 3 | 6 5 ENT |
| Evaluation of falling edge of pulse (opener contact) at input Aux 3 (factory setting) | 6 6 ENT |
| Evaluation of rising edge of pulse (closer contact) at input for door release button | 6 7 ENT |
| Evaluation of falling edge of pulse (opener contact) at input for door release button | 6 8 ENT |
| Evaluation of rising edge of pulse (closer contact) at input for door contact | 6 9 ENT |
| Evaluation of falling edge of pulse (opener contact) at input for door contact | 7 0 ENT |

## 12.23 Output Settings

7 1 ENT up to 7 8 ENT

Master card Keypad entries

| | |
|---|---|
| TTL output changes status from logic 0 to logic 1 (closer contact) at activation. | 7 1 ENT |
| TTL output changes status from logic 1 to logic 0 (opener contact) at activation (= factory setting). | 7 2 ENT |
| Activation of door bell output (= factory setting). | 7 7 ENT |
| Deactivation of door bell output. | 7 8 ENT |

## 12.24 Activating the Keypad for Entry of Card Numbers

7 3 ENT

Master card Keypad entry

The keypad is activated to accept the entry of the card number.
In this operating mode, the door is opened by entering the last 8 digits of the card number (e.g., *802* **078-64231**, *omit "802"*) and ENT

## 12.25 Deactivating the Keypad against Entry of Card Numbers

7 4 ENT

Master card Keypad entry

The keypad is deactivated. It is not possible to enter or delete card numbers with the numeric keys.

## 12.26 Setting the Time Lag of Door Contact Evaluation

8 1 ENT t t ENT

Master card Keypad entry Duration of time lag

tt = 00 - 99 s; with factory setting = 00 s, the door contact will not be recognised, see chapter 12.4 "Alarm switching time at interruption of door contact".

### 12.27 Limiting the Number of False Entries Allowed

(NN = 00 - 99, factory-set number = 05)

8 2 ENT  N N ENT

Master card  Keypad entryNumber of false entries allowed

### 12.28 Time Window for Code Entry

(tt = 10 - 99 s, factory-set time window = 20 s. Minimum tt = 10 s.

8 3 ENT  t t ENT

Master card  Keypad entryTime window for code entry

### 12.29 Setting the Sabotage Alarm Output

Here you determine the output to be switched at sabotage alarm (see table for OM)

8 4 ENT  O M ENT

Master card  Keypad entryOutput mode

### 12.30 Activating the Sabotage Alarm

In order to comply with the requirements of the UL 294 standard, it is necessary that the sabotage alarm should be activated.

8 8 ENT

Master card  Keypad entry

### 12.31 Deactivating the Sabotage Alarm (Factory Setting)

8 9 ENT

Master card  Keypad entry

## 12.32 Reset to Factory Settings and Deleting All Access Authorisations

Master card


Keypad entry

Use this command if you wish to delete all data entered and to restart from the beginning. Afterwards, you start anew by reading in the master card or entering the master PIN as described in chapter 8.

## Contact

Internet http://www.g-u.de or http://www.bks.de.

If you have any questions concerning the products call the telephone numbers:
+49 7156 301 0 or +49 2051 201 0

BKS GmbH, D-42502 Velbert
Telefon (02051) 201-0
Telefax (02051) 201-431
www.g-u.com

**Advice**

We reserve the right to change the contents of this document without prior notice.
The company Gretsch-Unitas Baubeschläge is not liable for technical or editorial error or omission in the present document; moreover, Gretsch-Unitas GmbH Baubeschläge does not assume liability for damage arising directly or indirectly from the delivery, performance or usage of the device.