

KURZANLEITUNG PINCODE-TERMINAL 3068

PINCODE KEYPAD 3068 : : CLAVIER À CODE PIN 3068
: : TASTIERA A CODICE PIN 3068 : : TECLADO PARA
CÓDIGO PIN 3068 : : PINCODETOETSENBORD 3068

V-2012-09

INHALTSVERZEICHNIS

BILDER · FIG. 1 · IMAGE 1 · FIGURA 1 · AFBEELDING · FIG.	4
DEUTSCH	5
ENGLISH	18
FRANÇAIS.....	31
ITALIANO.....	44
NEDERLANDS	57
ESPAÑOL.....	70

BILD 1 · FIG. 1 · IMAGE 1 · FIGURA 1 ·
AFBEELDING 1



BILD 2 · FIG. 2 · IMAGE 2 · FIGURA 2 ·
AFBEELDING 2



BILD 3 · FIG. 3 · IMAGE 3 · FIGURA 3 ·
AFBEELDING 3



1.0 PRODUKTBEZEICHNUNG

1.1 ALLGEMEINES

Das PinCodeTerminal 3068 ist ein digitaler „Schlüssel“ (Transponder), der nach Eingabe richtiger Zahlencodes berührungslos über Funk SimonsVoss G2 Schließungen öffnet. Zur Konfiguration des Systems muss mindestens eine PIN vorkonfiguriert und der dazugehörige integrierte Transponder passend zur Schließung programmiert werden. Anschließend wird, nach Eingabe einer richtigen PIN, die zugehörige Schließung freigegeben.

2.0 WARNHINWEISE

2.1 SICHERHEITSHINWEISE

- :: Die Montage und der Einbau dürfen nur durch geschultes Fachpersonal durchgeführt werden.
- :: Das PinCodeTerminal nicht mit Öl, Farbe, Säuren o.ä. in Verbindung bringen.
- :: Es sind nur Batterien zu verwenden, welche von SimonsVoss freigegeben sind.
- :: Vorsicht! – Die in diesem Produkt verwendeten Batterien können bei Fehlbehandlung eine Feuer- oder Verbrennungsgefahr darstellen. Diese Batterien nicht aufladen, öffnen, über 100°C erhitzen oder verbrennen.
- :: Beim Batteriewechsel die neuen Batterien nur mit sauberen fettfreien Handschuhen berühren.
- :: Alte und verbrauchte Batterien fachgerecht entsorgen und nicht in Reichweite von Kindern aufbewahren.
- :: Ein Vertauschen der Polarität kann zu Beschädigungen des PinCodeTerminals führen.
- :: Beim Batteriewechsel immer alle Batterien erneuern.
- :: Das PinCodeTerminal muss mit zwei Batterien betrieben werden.
- :: Achten Sie darauf, dass das PinCodeTerminal nicht verschmutzt oder verkratzt wird, die Tastatur nicht zu Boden fällt oder sonstigen starken Stößen ausgesetzt wird.
- :: Beim Batteriewechsel darauf achten, dass die Elektronik nicht mechanisch belastet wird.

- tet oder Feuchtigkeit ausgesetzt wird bzw. anderweitig zu Schaden kommt.
- :: Weiterhin beachten Sie bitte, dass das Terminal nach Inbetriebnahme unverzüglich mit einem PIN-Code programmiert werden sollte!
 - :: Die Handhabung eines SimonsVoss PinCodeTerminals setzt Kenntnisse im Umgang mit dem Produkt und der SimonsVoss Software voraus. Deshalb sollte die Programmierung der PinCodeTerminal nur durch geschultes Fachpersonal erfolgen.
 - :: Bitte den gewählten MasterPIN gut und sicher aufbewahren, da dieser aus Sicherheitsgründen nicht reproduziert werden kann.
 - :: Für Schäden durch fehlerhafte Programmierung übernimmt die SimonsVoss Technologies AG keine Haftung.
 - :: Durch fehlerhaft programmierte oder defekte PinCodeTerminals kann der Zugang durch eine Tür versperrt werden. Für Folgen, wie versperrter Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder anderen Schäden haftet die SimonsVoss AG nicht.
 - :: Das Gehäuse ist mit zwei Torx Schrauben (TX6) gesichert. Dadurch erhöht sich die Sicherheit gegen unbefugtes Öffnen.
 - :: Die SimonsVoss Technologies AG behält sich das Recht vor, Produktänderungen bzw. technische Weiterentwicklungen ohne Vorankündigung durchzuführen.
 - :: Die Dokumentation wurde nach bestem Wissen erstellt, evtl. Fehler können aber nicht ausgeschlossen werden. Hierfür kann keine Haftung übernommen werden.
 - :: Sollten Abweichungen von Inhalten in Fremdsprachenversionen der Dokumentation bestehen, gilt im Zweifelsfalle das deutsche Original.

3.0 FUNKTIONSWEISE

3.1 ALLGEMEINE BESCHREIBUNG

Das PinCodeTerminal besteht aus den Komponenten:

- :: PIN-Code Eingabe und Auswertung
- :: Integrierter digitaler Schlüssel (Transponder), der die zugehörige Schließung öffnet, wenn er nach erfolgreicher PIN-Code Auswertung ausgelöst wird.

Mit dem PinCodeTerminal sind Sie somit jederzeit in der Lage, alle SimonsVoss G2 Schließungen (z.B. Zylinder G2, Smart Relais G2 sowie Scharfschalteinheiten etc.) mittels PIN-Code anzusprechen.

Es stehen bis zu 500 unterschiedliche PIN zur Verfügung. Änderungen der PIN können jederzeit, je nach konfigurierten Modi, vom Nutzer selber durchgeführt werden. Hierzu muss nicht der Anlagenadministrator eingebunden werden. Darüber hinaus ist es möglich, in SimonsVoss G2 Schließungen (mit ZK-Funktion, d.h. Zutrittskontroll- und Zeit-zonensteuerung) einer Person bzw. Personengruppe auch zeitlich befristeten Zugang zum Gebäude zu gewähren, sowie zu protokollieren, welche PIN wann Zutritt hatte.

3.2 PROGRAMMIERUNG / SOFTWARE

Zur Programmierung und Nutzung des PinCodeTerminal werden folgende Komponenten/Software benötigt:

- :: LSM 3.1 SP1 oder höher
- :: SmartCD.G2
- :: G2 Schließungen

4.0 PROGRAMMIERUNG ALLGEMEIN

4.1 TRIVIAL-PIN

Um die Sicherheit des PinCodeTerminals zu erhöhen, werden sehr einfache PIN vom System nicht zugelassen. Folgende Trivial PIN sind nicht zulässig:

- :: PIN mit aufsteigender Ziffernfolge
- :: PIN mit absteigender Ziffernfolge
- :: PIN mit mehr als zwei gleichen Ziffern hintereinander

Falls PIN nach diesem Aufbau gewählt werden, werden diese automatisch vom System abgewiesen.

4.2 TIME OUT

Sollte während der Programmierung der PIN für 5 Sekunden keine Taste betätigt werden, so bricht die Programmierung mit einer Fehlermeldung ab. Die neue PIN wird dann nicht akzeptiert bzw. die bisherige bleibt bestehen, und der Vorgang muss von vorne gestartet werden.

4.3 VORGEHENSWEISE

Um den Programmiermodus am PinCodeTerminal zu starten ist die „0“ länger als 2 Sekunden gedrückt zu halten, mit einer anschließenden Präambel wird die Programmierfunktion gewählt (01 bis 99). Die entsprechenden Programmierfunktionen sind in den nächsten Kapiteln eingehend beschrieben.

Um die Programmierung mit der Software zu starten, bitte immer eine Taste <>0 länger als drei Sekunden gedrückt halten.

5.0 INBETRIEBNAHME

5.1 PROGRAMMIERMODUS ALLGEMEIN

Um in den Programmiermodus zu gelangen, ist es notwendig die „0“ länger als 2 Sekunden gedrückt zu halten. Der Wechsel in den Programmiermodus wird mit einem kurzen gelben blinken und einem kurzen Ton angezeigt.

5.2 MASTERPIN ÄNDERN

Bei der ersten Inbetriebnahme ist es zwingend erforderlich die werkssseitig eingestellte

Master-PIN: 1 2 3 4 5 6 7 8

durch eine eigene MasterPIN zu ersetzen. Wird die MasterPIN nicht geändert, können alle anderen Funktionalitäten nicht genutzt werden.

Vorgabe für die MasterPIN:

:: 8-stellig

:: Bitte beachten Sie auch Kapitel 4.1.

Der persönliche Master-PIN wird für diverse Programmiervorgänge zur Authentifizierung benötigt. Bitte verwahren Sie diese sicher und für Unbefugte unzugänglich auf.

1. Eingabe „0“ -> (länger als 2 Sekunden gedrückt halten)
2. Eingabe „09“
3. Eingabe „Default-MasterPIN“
4. Eingabe „Neue MasterPIN“
5. Wiederholung „Neue MasterPIN“

Wird bei der Eingabe der MasterPIN für 5 Sekunden keine Taste betätigt, so bricht das Terminal mit einer Fehlermeldung ab. Der MasterPIN bleibt bestehen, und der Vorgang muss von vorne gestartet werden.

Wenn ein bestehender Master-PIN geändert werden soll, bitte wie oben erläutert vorgehen. Als „Default-MasterPIN“ bitte in diesem Fall die aktuelle MasterPIN eingeben.

5.3 EINSTELLEN DER USERPIN LÄNGE

Der Systemadministrator kann im Zuge der Inbetriebnahme systemweit einmalig die UserPIN Länge in der LSM vorgegeben. Diese Länge, wählbar ist zwischen 4-8 Stellen, gilt dann für alle PIN. Der MasterPIN hat immer 8 Stellen.

Bitte gehen Sie wie folgt vor:

1. Schließenanlage öffnen
2. Konfiguration des PinCodeTerminals öffnen (Bearbeiten -> Schließenanlagen Eigenschaften -> PIN-Code Terminal)
3. Unter „PIN-Code Länge“ PIN Länge wählen
4. Mit „Übernehmen“ bestätigen

Achtung: Die UserPIN Länge darf nach Programmierung des ersten PinCodeTerminals in der Schließenanlage nicht geändert werden, ansonsten müssen alle im System vorhandenen Terminals nachprogrammiert werden, neue PIN vergeben etc..

5.4 EINSTELLEN DER BETRIEBSART

Der Systemadministrator kann im Zuge der Inbetriebnahme systemweit einmalig die Betriebsart in der LSM vorgeben. Es kann in einer Schließanlage jeweils eine Betriebsart verwendet werden.

Nähere Informationen zu den Modi 2 und Modi 3 (Verifikation) finden Sie im Handbuch.

Achtung: Die Betriebsart darf nach Programmierung des ersten PinCodeTerminals nicht geändert werden, ansonsten müssen alle im System vorhandenen Terminals nachprogrammiert werden, neue PIN vergeben, Transponder ausgegeben etc.. Dieses hat auch generelle Auswirkungen auf die Verwendung des/der Terminals, des-halb ist hier eine sorgfältige Planung im Vorfeld durchzuführen.

6.0 PROGRAMMIERUNG

6.1 ZUWEISUNG SCHLIESSUNG

Das PinCodeTerminal wird fest einer G2 Schließung zugewiesen, und kann (aus Sicherheitsgründen) auch nur diese öffnen. Zur Konfiguration bitte folgende Schritte durchführen:

1. G2 Schließung erstellen
2. G2 Schließung markieren (z.B. Schließzylinder G2)
3. „Bearbeiten -> Schließung Eigenschaften“ anklicken
4. Reiter „Tür“ anwählen
5. Im Feld „Türattribute“ beim Punkt „PIN-Code Terminal“ Haken setzen
6. Mit „Übernehmen“ bestätigen

Somit wurde an dieser G2 Schließung das Terminal konfiguriert, und die Tür kann bei Berechtigung über das Terminal geöffnet werden (bitte die unterschiedlichen Modi beachten).

6.2 PROGRAMMIERUNG DER SCHLIESSANLAGENDATEN

6.2.1 PINCODETERMINAL

Das PinCodeTerminal muss nur einmalig mit den Schließenanlagendaten programmiert werden. Bitte für die Programmierung folgendermaßen vorgehen:

1. Bearbeiten -> Schließenanlage Eigenschaften
2. Reiter „PIN-Code Terminal“ anwählen
3. „Betriebsart“ auswählen (siehe hierzu Kapitel 7.0 MODI)
4. „PIN-Code Länge“ festlegen
5. Übernehmen anklicken!
6. „Programmieren / Zurücksetzen“ anwählen
7. Entsprechende Schließung unter „Türen mit PIN-Code Terminals“ markieren
8. Programmierbefehl in der Software starten (Button „Programmierung“)
9. Beliebige Taste (außer die „0“) auf dem PinCodeTerminal für 3 Sekunden gedrückt halten

*Achtung: In der LSM 3.1 SP1 wird derzeit noch dazu aufgefordert die „0“ zu betätigen, es können aber alle Tasten bis auf die „0“ verwendet werden.

6.2.2 PIN-CODE BENUTZER

Im „Wissens-Modus“ alle Nutzer bzw. Transponder als Typ „PIN-CodeBenutzer“ anlegen, ein zusätzlicher Transponder wird in diesem Modus nicht benötigt.

6.2.3 SCHLIESSUNG

Vor der Programmierung der Schließung wird im „Wissens-Modus“ empfohlen zuerst alle Nutzer als „PIN-Code Benutzer“ anzulegen und dann erst die Schließung zu programmieren. Ansonsten müssen neue Nutzer an der verbauten Schließung erneut einprogrammiert werden.

Empfehlung: Um den Programmieraufwand in einer installierten Schließenanlage an der Tür zu minimieren bzw. komplett zu vermeiden wie folgt vorgehen:

- a) Transpondergruppe erstellen (z.B. PinCodeTerminal)

- b) Transponder (Typ: PIN-Code Benutzer) anlegen
- :: Ohne neue Person anlegen
- :: ohne Benutzer (kein auswählen)
- :: Transpondergruppe (unter a)) zuweisen

Diese Transponder können dann im Vorfeld in die entsprechende Schließung einprogrammiert werden. Wenn neue Nutzer an der Schließung das PinCodeTerminal verwenden sollen, können diese dann verwendet werden.

7.0 BETRIEBSART MODI

Beim PinCodeTerminal stehen drei unterschiedliche Programmiermodi zur Verfügung:

1. Wissen-Modus (PIN)
2. Wissen-Besitz mit flexibler PIN
Verifikation -> Transponder/SmartCard + PIN
3. Wissen-Besitz mit fester PIN
Verifikation -> Transponder/SamrtCard + PIN

In einer Schließanlage kann jeweils nur einer der Modi verwendet werden. Nähere Informationen zu den Modi 2 und Modi 3 (Verifikation) finden Sie im Handbuch.

7.1 WISSEN-MODUS

Im Wissen-Modus kann eine Tür bei richtiger Eingabe der PIN geöffnet werden. Ein zusätzlicher Transponder wird hierfür nicht benötigt.

Der Nutzer muss aber, über die Software als „PIN Code Benutzer“ angelegt werden, um eine TID zu erhalten!

7.1.1 AUFBAU USERPIN

Der UserPIN setzt sich aus einem variablen und einem festen Teil zusammen:

UserPIN = UserPINvariabel + TID(5 stellig)

Die UserPINvariable kann vom Nutzer frei gewählt werden, nur die Vorgabe der Länge ist zu beachten, die TID wird dem Nutzer fest vom Administrator bzw. der Programmiersoftware zugeteilt.

7.1.2 INITIAL-PIN (IPIN)

Die Initial-PIN (IPIN) ist ein 24stelliger Zahlwert, welcher in der LSM erstellt wird. Mit Hilfe der IPIN kann der Nutzer selbstständig am PinCodeTerminal sein User Profil freischalten und einen eigenen UserPIN vergeben.

Der Initial-PIN setzt sich folgendermaßen zusammen:

- a) 1. Stelle: Programmiermodus (Wechsel in den Programmiermodus)
- b) 2.+3 Stelle: Programmierfunktion (z.B. Einlernen eines neuen Users)
- c) 4.-24. Stelle: IPIN (wobei bei der 4.-8. Stelle die TID abgebildet wird)

Zur Erstellung der IPIN, zuerst muss eine G2 Schließung als auch ein PIN-Code Benutzer angelegt werden, bitte folgendermaßen vorgehen:

1. Konfiguration des PinCodeTerminal öffnen (Bearbeiten -> Schließenanlage Eigenschaft -> PIN-Code Terminal)
2. PIN-Code Benutzer/Transponder auswählen
3. Button „Initial-PINs“ anwählen
4. Es öffnet sich ein neues Fenster mit einem Formular
5. Ausdruck und Aushändigung an den Nutzer

Die ersten drei Ziffern bzw. Zahlen stehen für den Programmiermodus für die Neuanlage des Nutzers am Terminal, die letzten 21 Stellen sind die Zahlen die zum Einlernen benötigt werden.

Die IPIN kann nur einmal verwendet werden, und wird danach deaktiviert. Somit ist sichergestellt, dass mit einer IPIN nur ein User-PIN an einem vorgegebenen Terminal erstellt werden kann.

7.1.3 NEUANLAGE EINES USERS

Die User-PIN sind individuell an die Transponder-IDs (TID) des Nutzers und der Schließanlage gebunden. Neue User-Datensätze im Terminal werden automatisch angelegt,

wenn der Nutzer einmalig seine Initial-PIN (IPIN) eingibt. Der Nutzer kann sich selber mittels seiner IPIN im PinCodeTerminal anlegen, und eine eigene PIN vergeben (siehe hierzu auch Kapitel „Trivial-PIN“).

Bitte für die Programmierung folgendermaßen vorgehen:

1. Eingabe „0“ (länger als 3 Sek.)
2. Eingabe „01“
3. Eingabe „IPIN“ (21-stellig*)
4. Eingabe „Neue User-PINvariabel“
5. Wiederholung „Neue User-PINvariabel“

*Bitte hier die letzten 21 Stellen der IPIN aus dem Ausdruck verwenden.

Für den Nutzer bedeutet das, dass er die komplette Nummer (24stellig) eingibt, und dann zweimal seine selber gewählte User-PINvariabel. Die neue User-PINvariabel muss die entsprechende Länge nach der Vorgabe bzw. Konfiguration nach Kapitel 5.3 Einstellen der USERPIN Länge aufweisen. Es wird geprüft ob es sich bei dem User-PINvariabel um ein Trivial-PIN handelt. Ist die-ses der Fall, wird der User-PINvariabel vom System abgewiesen.

Für Informationen und Aufbau des kompletten User-PIN schauen Sie bitte in das Kapitel 7.1.1 Aufbau UserPIN.

8.0 ÖFFNUNG

8.1 WISSEN-MODUS

Um die zugehörige Schließung mit Hilfe des PinCodeTerminal zu öffnen, bitte wie folgt vorgehen: Die TID (5 stellig) + programmierten PIN eingeben. Zwischen den Eingaben der einzelnen Nummern dürfen maximal 5 Sekunden verstreichen.

Bei korrekter Eingabe und Programmierung des integrierten Transponders leuchtet die LED 2x GRÜN und es ertönt ein Signal. Anschließend öffnet der integrierte Transponder die Schließung.

9.0 BATTERIEWARNUNG

Um einen definierten Zustand des PinCodeTerminal zu erreichen und um Bedienungsfehler zu minimieren, wurde ein 2-stufiges Batteriewarnsystem integriert. Auf nachlassende Batteriekapazität wird frühzeitig aufmerksam gemacht, ein Batteriewechsel kann so rechtzeitig in die Wege geleitet werden.

Batteriewarnstufe 1:

Der Öffnungsvorgang wird zeitlich versetzt durchgeführt. Die Diode blinkt GELB und der Summer ertönt für 5 Sekunden. Erst nach Ablauf der 5 Sekunden versendet die PinCodeTerminal den Öffnungsbefehl.

Batteriewarnstufe 2:

Der Öffnungsvorgang wird zeitlich versetzt durchgeführt. Die Diode blinkt GELB und der Summer ertönt nun für 10 Sekunden. Erst nach Ablauf der 10 Sekunden versendet die PinCodeTerminal den Öffnungsbefehl. Spätestens zu diesem Zeitpunkt muss ein Batteriewechsel erfolgen, anderenfalls verliert das System nach kurzer Zeit seine Funktionsfähigkeit.

Achtung: Es ist nicht möglich, bei Batteriewarnung in den Programmiermodus zu gelangen, d.h. dass bei schwacher Batterie keine Funktionen geändert oder gelöscht werden können. Erst nach erfolgreichem Batteriewechsel (siehe Kapitel Batteriewechsel) steht der Programmiermodus wieder zur Verfügung.

10.0 BATTERIEWECHSEL

Generell darf der Batteriewechsel nur von geschultem Fachpersonal durchgeführt werden. Hierbei bitte wie folgt vorgehen:

1. Die beiden Schrauben im Gehäuseboden komplett herausschrauben (TORX TX6).
2. Die Vorderseite des Gehäuses abnehmen.
3. Die Batteriebügel vorsichtig aus der Platine lösen (Bild 2).
4. Beide Batterien entnehmen (Bild 1).

5. Die neuen Batterien einsetzen; der Pluspol muss hierbei nach oben schauen (Bild 2). Bitte die neuen Batterien nur mit sauberen fettfreien Handschuhen oder ähnlichem berühren.
6. Die Batteriebügel wieder vorsichtig in die Platine einhaken (Bild 3).
7. Das Gehäuse wieder aufstecken.
8. Die beiden Gehäuseschrauben von unten wieder in das Gehäuse schrauben.
9. Um den Batterie-Alarm-Zustand wieder zurückzusetzen bitte folgende Schritte durchführen:
 - a) Eingabe „0“
 - b) Eingabe „99“
 - c) Eingabe „99999“

Nach dem Batteriewechsel stehen alle Funktionen wieder zur Verfügung. Bitte immer beide Batterien erneuern, da diese ungefähr gleich stark entladen werden. Beim Batteriewechsel unbedingt darauf achten, dass kein Wasser in das Gehäuse eindringen kann bzw. die Elektronik nicht mit Wasser in Berührung kommt. Bei Notwendigkeit das an der Wand befestigte Gehäuseteil sorgfältig trocknen. Bitte verwenden Sie immer nur Batterien, die von SimonsVoss freigegeben sind.

11.0 MANIPULATIONSWARNUNG

Um das systematische Ausprobieren von User-PINs zu vermeiden, ist eine Manipulationswarnung in das PinCodeTerminal integriert. Nach der 5. Falscheingabe einer PIN (User-PIN, MasterPIN etc.) ertönt für 60 Sekunden ein Warnsignal und die LED blinkt gleichzeitig rot. In dieser Zeit kann das Terminal nicht bedient werden.

Bei einer weiteren Fehleingabe wechselt das Terminal sofort wieder in den Manipulationsmodus. Erst nach Eingabe einer richtigen PIN wird der Zähler wieder auf 0 gesetzt.

12.1 TECHNISCHE DATEN

Abmessungen: B x H x T 96 mm x 96 mm x 14 mm

Gewicht: 102 g (incl. Batterien)

Material: Kunststoff

Farbe: Grau mit transparentem Ring

Maximale Anzahl Betätigungen mit einem Batteriesatz: Bis zu 100.000 Betätigungen
bzw. bis zu 10 Jahre Standby

Betätigungsentfernung Zylinder: Bis zu 40 cm

Betätigungsentfernung Smart Relais: Bis zu 120 cm

Schutzklasse: IP 65

Arbeitstemperaturbereich: -20°C bis +50°C

Batterietyp: 2 x 3 V DC Lithium Batterie Typ CR2032

Batteriewechsel: Nur durch geschultes Fachpersonal

1.0 PRODUCT DESCRIPTION

1.1 GENERAL INFORMATION

Pin Code Terminal 3068 is a digital 'key' (transponder) which opens SimonsVoss G2 lock devices after a correct PIN code has been entered using contactless communication in a wireless network.

At least one PIN needs to be pre-assigned to configure the system and the associated integrated transponder needs to be programmed for the lock device. After programming, the lock device can then be released after a correct PIN code has been entered.

2.0 PRECAUTIONS

2.1 SAFETY INSTRUCTIONS

- :: Only trained specialists may fit and install the terminal.
- :: Do not allow the pin code terminal to come into contact with oil, paint, acids or similar.
- :: Only use batteries which have been approved by SimonsVoss.
- :: Warning: the batteries used in this product may pose a fire or burn hazard if handled incorrectly. Do not recharge, open or burn these batteries, or heat them to over 100°C.
- :: When replacing the batteries, use clean gloves free of fat or grease to handle new batteries.
- :: Dispose of old and used batteries in the proper manner and store them out of children's reach.
- :: Damage may be caused to the pin code terminal if you reverse the polarity.
- :: Always replace all batteries when changing batteries.
- :: The pin code terminal must always be operated with two batteries.
- :: Do not allow the pin code terminal to become dirty or scratched. Ensure that the key-pad does not fall onto the floor and is not exposed to any other type of impact.
- :: When replacing the batteries, make sure that the electronics are not subject to

- mechanical load or damp, and are not damaged in any other way.
- :: Also ensure that the terminal is programmed with a PIN code immediately after it is put into operation!
 - :: Specialist knowledge is required to handle a SimonsVoss pin code terminal and the SimonsVoss software. That is why only trained specialists may programme the pin code terminal.
 - :: Please keep the selected master PIN in a safe place as it cannot be reproduced for security reasons.
 - :: SimonsVoss Technologies AG accepts no liability for damage caused by incorrect programming.
 - :: Access through a door may be blocked due to defective or incorrectly programmed pin code terminals. SimonsVoss AG is not liable for consequences such as blocked access to injured persons or those at risk, physical damage or any other losses.
 - :: The casing is secured with two Torx screws (TX6). This offers greater protection against unauthorised opening.
 - :: SimonsVoss Technologies AG reserves the right to make changes to the product or implement technical further developments without prior notice.
 - :: This documentation has been compiled in accordance with the best knowledge available to us. However, errors cannot be ruled out. No liability is accepted in such cases.
 - :: Should there be differences in the content of other language versions of this documentation, the German version applies in cases of doubt.

3.0 MODE OF OPERATION

3.1 GENERAL DESCRIPTION

The pin code terminal consists of the following components:

- :: PIN code input and validation
- :: Integrated, digital key (transponder) which opens the corresponding lock device when authorised after positive PIN code validation.

The pin code terminal enables you to operate all SimonsVoss G2 lock devices, such as Cylinder G2, Smart Relay G2 and activation units using a PIN code. There are up to 500 different PINs available. Users themselves can modify their PIN at any time, depending on the configured modes. There is no need to include the system administrator to do so. SimonsVoss G2 locking systems (with an access control function, i.e. access and time zone control) also allow system operators to authorise a person or a user group to access a building on a time-limited basis and also log which particular PIN gains access at a particular time.

3.2 PROGRAMMING / SOFTWARE

The following components and software are required to programme and use the pin code terminal:

- :: LSM 3.1 SP1 or higher
- :: SmartCD.G2
- :: G2 lock devices

4.0 GENERAL PROGRAMMING

4.1 TRIVIAL PIN

The system does not allow very simple PIN codes to ensure that the pin code terminal offers a high level of security.

The following trivial PINs are not permitted:

- :: PINs with an ascending sequence of numbers
- :: PINs with a descending sequence of numbers
- :: PINs with the same number repeated more than twice in succession

If a PIN is selected with such a sequence of numbers, the system automatically rejects the PIN.

4.2 TIME OUT

If no key is pressed for 5 seconds while the PIN is being programmed, programming is aborted and an error message displayed. The new PIN is not accepted or the existing one remains valid and the process must be started again.

4.3 PROCEDURE

To start the programming mode on the pin code terminal, you need to press down „0“ for more than 2 seconds. The programming function is then selected using a code (01 to 99). The corresponding programming functions are described in detail in the following sections.

Please always press down a key <>0 for longer than three seconds to start programming with the software.

5.0 PUTTING INTO OPERATION

5.1 GENERAL PROGRAMMING MODE

You need to press down the „0“ key for longer than 2 seconds to enter programming mode. The changeover into programming mode is signalled by the indicator light flashing yellow briefly and a short tone being emitted.

5.2 CHANGING THE MASTER PIN

When placing the terminal into operation for the first time, you must change the factory default master PIN 1 2 3 4 5 6 7 8 to a personal master PIN. If the master PIN is not changed, none of the other functions may be used.

Specifications for the master PIN:

:: 8 digits

:: Please also observe Section 4.1.

A personal master PIN is required for authentication for a variety of programming procedures. Please keep it in a safe place where it cannot be accessed by unauthorised

persons.

1. Enter“0” -> (press down for longer than 2 seconds)
2. Enter „09“
3. Enter „Default master PIN“
4. Enter „New master PIN“
5. Repeat „New master PIN“

If no key is pressed for 5 seconds while the PIN is being programmed, programming is aborted and an error message displayed. The existing master PIN remains valid and the process must be started again.

If you wish to change an existing master PIN, please use the same procedure described above. You should enter the current master PIN when asked to enter the „Default master PIN“.

5.3 SETTING THE USER PIN LENGTH

The system administrator is able to specify the user PIN length just once for the whole system when placing the terminal into operation. This length can be set at between 4 and 8 digits and will apply to all PINs. The master PIN always features 8 digits.

Please proceed as follows:

1. Open locking system
2. Open the pin code terminal configuration (Edit -> Locking system properties -> PIN code terminal)
3. Select PIN length under „PIN code length“
4. Confirm by pressing „Accept“.

CAUTION: the user PIN length cannot be changed once the first pin code terminal in the locking system has been programmed, otherwise all terminals in the system must be reprogrammed, new PINs must be issued and so on.

5.4 SETTING THE OPERATING TYPE

The system administrator is able to specify the operating type in the LSM just once for the whole system when placing the terminal into operation. Only one operating type can be used per locking system.

You will find more detailed information on Modes 2 and 3 (verification) in the manual.

CAUTION: The operating type cannot be changed once the first pin code terminal in the locking system has been programmed, otherwise all terminals in the system must be reprogrammed, new PINs and transponders must be issued and so on. This also affects the use of the terminal(s) in general. You should therefore plan programming carefully in advance.

6.0 PROGRAMMING

6.1 ASSIGNMENT TO A LOCK DEVICE

The pin code terminal is assigned to a G2 lock device on a permanent basis and can only open this device for security reasons. Complete the following steps to configure the terminal:

1. Create G2 lock device
2. Highlight G2 lock device (e.g. Locking Cylinder G2)
3. Click on „Edit -> Lock device properties“
4. Select „Door“ tab
5. Check the „PIN code terminal“ box in the „Door attribute“ field
6. Confirm by pressing „Accept“.

The terminal has thus now been configured for this G2 lock device and authorised users can now open the door using the terminal (please take into account the different modes).

6.2 PROGRAMMING THE LOCKING SYSTEM DATA

6.2.1 PIN CODE TERMINAL

The pin code terminal only needs to be programmed with the locking system data once.

Programme as follows:

1. Edit -> Locking system properties
2. Select „PIN code terminal“ tab
3. Select „Operating type“ (see Section 7.0 MODI)
4. Define „PIN code length“
5. Click to accept
6. Select “Programme / Reset”
7. Highlight corresponding lock device under „Doors with PIN code terminals“
8. Launch programming command in the software („Programming“ button)
9. Hold down any key (except the „0“) on the pin code terminal for 3 seconds

*CAUTION: LSM 3.1 SP1 currently asks you to press „0“ as well. However, any key can be used except „0“.

6.2.2 PIN CODE USER

Add all users or transponders as a „PIN code user“ in „Knowledge mode“; there is no need for an additional transponder in this mode.

6.2.3 LOCK DEVICE

Before programming the lock device, it is recommended to add all users as a „PIN code user“ first and only then programme the lock device. If you do not, new users for the fitted lock device will need to be programmed again.

Recommended: in order to minimise or completely avoid programming at the door in an installed locking system, proceed as follows:

- a) Create transponder group (e.g. pin code terminal)
- b) Add transponder (type: PIN code user)

- :: Add without new person
- :: Without user (select none)
- :: Assign transponder group (in a))

These transponders can then be programmed into the corresponding lock device in advance. When new users for the lock device are to use the pin code terminal, they can use these transponders.

7.0 OPERATING TYPE MODES

Three different programming modes are available for the pin code terminal:

1. Knowledge mode (PIN)
2. Knowledge-possession mode with flexible PIN
Verification -> Transponder / smart card + PIN
3. Knowledge-possession mode with fixed PIN
Verification -> Transponder / smart card + PIN

Only one of the operating modes may be used per locking system. You will find more detailed information on Modes 2 and 3 (verification) in the manual.

7.1 KNOWLEDGE MODE

In knowledge mode, a door can be opened when the correct PIN is entered. There is no need for an additional transponder.

However, the user must be added as a „PIN code user“ in the software in order to receive a TID!

7.1.1 USER PIN FORMAT

The user PIN consists of a variable and a fixed part:

User PIN = User PINvariable + TID (5 digits)

Users can choose the user PINvariable themselves as only the length is specified; they

are permanently assigned a TID by the administrator or the programming software.

7.1.2 INITIAL PIN (IPIN)

The initial PIN (IPIN) is a 24-digit number which is generated in the LSM. Users can use the IPIN to activate their user profile themselves and issue their own user PIN on the pin code terminal.

The initial PIN consists of the following:

- a) 1st digit: Programming mode (change into programming mode)
- b) 2nd +3rd digit: Programming function (e.g. entering a new user)
- c) 4th-24th digit: IPIN (in which the 4th-8th digits correspond to the TID)

A G2 lock device and a PIN code user need to be added in the software first before an IPIN can be generated. Proceed as follows to do so:

1. Open the pin code terminal configuration (Edit -> Locking system properties -> PIN code terminal)
2. Select PIN code user / Transponder
3. Press „Initial PINs“ button
4. A new window will open with a form
5. Print and give to the user

The first three digits represent the programming mode for creating the user in the terminal, the last twentyone digits are the numbers required for entering the new user.

The IPIN can only be used once and is then deactivated. This ensures that only one single user PIN can be created with an IPIN at a specified terminal.

7.1.3 CREATING A USER

The user PIN is linked to the user's transponder ID (TID) and the locking system separately. New user datasets in the terminal are automatically added when the user enters their onetime initial PIN (IPIN). Users can add themselves to the pin code terminal using their IPIN and issue their own user PIN (also see section on „Trivial PIN“).

Programme as follows:

1. Enter „0“ (longer than 3 sec)
2. Enter „01“
3. Enter „IPIN“ (21 digits*)
4. Enter „New user PINvariable“
5. Repeat „New user PINvariable“

*Please use the last 21 digits in the IPIN from the printout.

This means that the user enters their complete 24-digit number and then the user PINvariable that they chose themselves twice.

The new user PINvariable must feature the corresponding length as specified or configured according to Section 5.3 Einstellen der USERPIN Länge.

A check is made to ensure that the user PINvariable is not a trivial PIN. If it is, the system rejects the user PINvariable.

Look at Section 7.1.1 for further information and the format of a full user PIN.

8.0 OPENING

8.1 KNOWLEDGE MODE

Proceed as follows to open the associated lock device using the pin code terminal:
Enter the TID (5 digits) + the programmed PIN. You have a maximum of 5 seconds to enter each individual number. The LED will flash GREEN twice and an acoustic signal will sound if you entered the right numbers and programmed the integrated transponder correctly. The integrated transponder will then open the lock device.

9.0 BATTERY WARNING

A two-level battery warning system has been integrated to achieve a defined status for the pin code terminal and minimise operating errors. This system signals decreasing battery capacity at an early stage, so that action can be taken to replace batteries in good time.

Battery warning level 1:

The opening procedure is delayed slightly. The diode flashes yellow and the buzzer sounds for 5 seconds. The pin code terminal delays sending the open command for 5 seconds.

Battery warning level 2:

The opening procedure is delayed. The diode flashes yellow and the buzzer sounds for 10 seconds. The pin code terminal delays sending the open command for 10 seconds. Batteries must be replaced at this stage at the latest. If not, the system will no longer be able to function after a short period of time.

CAUTION: it is not possible to access programming mode when the battery warning is active. This means no functions can be changed or deleted while the battery is low. Programming mode will only become available once the batteries have been successfully replaced (see section on Battery replacement).

10.0 BATTERY REPLACEMENT

As a general rule, only trained personnel may replace batteries. Proceed as follows to do so:

1. Remove the two screws (Torx TX6) from the casing base.
2. Detach the front of the casing.
3. Carefully unfasten the battery holder on the circuit board (Fig. 2).
4. Remove both batteries (Fig. 1).
5. Insert the new batteries; the positive pole must point upwards (Fig. 2). Only use clean gloves free of fat or grease to handle the new batteries.

6. Carefully refasten the battery holder on the circuit board (Fig. 3).
7. Put the casing back into position.
8. Fasten the two casing screws into the casing base again
9. Carry out the following steps to reset the battery alarm status:
 - a) Enter „0“
 - b) Enter „99“
 - c) Enter „99999“

All functions are ready to be used again once the battery replacement is complete. Always replace both batteries as they basically discharge at the same rate. While replacing the battery, ensure that no water can get inside the casing and the electronics do not come into contact with the electronics. If needed, carefully dry the section of the casing fastened to the wall.
Only ever use batteries approved by SimonsVoss.

11.0 MANIPULATION WARNING

A manipulation warning is integrated into the pin code terminal to prevent user PINs being tried out on a systematic basis. When five unsuccessful attempts have been made to enter a PIN (user PIN, master PIN and similar), a warning signal will sound for 60 seconds while the LED flashes red. The terminal cannot be operated during this time.

If another incorrect PIN is entered, the terminal will immediately change to manipulation mode. The counter will only reset to 0 when a correct PIN is entered.

12.0 APPENDIX

12.1 TECHNICAL DATA

Dimensions W x H x D: 96 mm x 96 mm x 14 mm

Weight: 102 g (including batteries)

Material: Plastic

Colour: Grey with transparent ring

Maximum number of operations performed by battery set: Up to 100,000 operations or up to 10 years on standby

Cylinder activation range: Up to 40 cm

Smart relay activation range: Up to 120 cm

Protection rating: IP65

Working temperature range: -20°C to +50°C

Battery type: 2 x 3 V DC lithium batteries, type CR2032

Battery replacement: By trained specialist personnel only

1.0 DESCRIPTION DU PRODUIT

1.1 GENERALITES

Le PINCodeTerminal 3068 est une « clé » (transpondeur) numérique qui ouvre par radio, sans contact, les fermetures SimonsVoss, après que les codes chiffrés corrects aient été entrés.

La configuration du système requiert qu'au moins un PIN ait été préconfiguré et que le transpondeur intégré associé ait été programmé. Ensuite la saisie d'un code PIN correct, provoque la libération de la fermeture associée.

2.0 MISE EN GARDE

2.1 CONSIGNES DE SECURITE

- :: Le montage et l'installation doivent être exclusivement effectués par le personnel qualifié.
- :: Le PINCodeTerminal ne doit pas entrer en contact avec de l'huile, de la peinture, des acides, etc.
- :: Seules les piles préconisées par SimonsVoss doivent être utilisées.
- :: Attention ! – en cas d'erreur de manipulation, les piles utilisées dans ce produit peuvent faire courir un risque d'incendie ou de brûlure. Ne pas les recharger, les ouvrir, les porter à plus de 100 °C, ni les jeter au feu.
- :: Lors du remplacement des piles, utiliser des gants non gras.
- :: Jeter les vieilles piles de façon appropriée et les garder hors de la portée des enfants.
- :: Inverser la polarité peut endommager le PINCodeTerminal.
- :: Remplacer toujours la totalité des piles.
- :: Le PINCodeTerminal doit être alimenté par deux piles.
- :: Veillez à ce que le PINCodeTerminal ne soit ni encrassé, ni rayé ; ne le laissez pas tomber et évitez tout choc violent.
- :: Lors du remplacement des piles, s'assurer que les appareils électroniques ne sont pas exposés à des tensions mécanique ou à l'humidité et respectivement à

d'autres dommages.

- : : Sachez également que vous devrez programmer le clavier avec un code PIN aussitôt après sa mise en service !
- : : L'utilisation d'un PINCodeTerminal, de SimonsVoss, suppose des connaissances sur le maniement du produit et du logiciel de SimonsVoss. C'est pourquoi la programmation du PINCodeTerminal doit être réservée aux techniciens formés à cet effet.
- : : Veuillez conserver le Master-PIN avec précaution car il ne peut pas être reproduit pour des raisons de sécurité.
- : : SimonsVoss Technologies AG n'est pas responsable des dommages causés par une programmation incorrecte.
- : : La mauvaise programmation ou la programmation défectueuse du PINCodeTerminal, peuvent empêcher le franchissement d'une porte. SimonsVoss n'est pas responsable de conséquences qui pourraient s'en suivre telles que le blocage de l'accès, les dommages aux biens ou aux personnes et autres dommages.
- : : Le boîtier est équipé de deux vis Torx (TX6). Cela augmente la sécurité contre toute ouverture non autorisée.
- : : SimonsVoss Technologies AG se réserve le droit d'effectuer des modifications ou modernisations techniques sans préavis.
- : : La documentation a été préparée en toute bonne foi, des erreurs ne peuvent toutefois pas être exclues. Cela n'engage aucune responsabilité.
- : : Si le contenu de la documentation devait varier en fonction des versions en langues étrangères, alors la version allemande reste la seule pertinente en présence de doute.

3.0 FONCTIONNEMENT

3.1 DESCRIPTION GENERALE

Le PINCodeTerminal est doté des deux composants suivants :

- : : le module de saisie et de traitement du code PIN
- : : la clé numérique intégrée (transpondeur) qui déclenche la libération de la fermeture

associée, lorsque le code PIN a été reconnu.

Le PINCodeTerminal vous permet donc à tout moment de déclencher tous les types de fermetures SimonsVoss G2 (par ex. cylindre G2, SmartRelais G2, etc.) au moyen du code PIN.

Vous disposez d'environ 500 différents. La modification du code PIN peut être effectuée à tout moment par les utilisateurs, en fonction des modes configurés. L'intervention de l'administrateur du système n'est pas requise. Il est en outre possible dans les fermetures SimonsVoss G2 (avec fonction contrôle d'accès, c.-à-d. contrôle d'accès et pilotage par plage horaires), d'accorder un accès limité dans le temps à une personne et respectivement à un groupe de personnes, et d'obtenir le protocole consignait quel PIN a accédé à l'immeuble et à quel moment.

3.2 PROGRAMMATION / LOGICIEL

Pour programmer et utiliser le PINCodeTerminal les composants / logiciels suivants sont nécessaires :

- :: LSM 3.1 SP1 ou plus
- :: SmartCD.G2
- :: Fermetures G2

4.0 PROGRAMMATION - GENERALITES

4.1 TRIVIAL-PIN

Pour augmenter la sécurité du PINCodeTerminal, les codes PIN très simples ne sont pas autorisés par le système.

Les Trivial PIN suivants ne sont pas autorisés :

- :: PIN avec ordre numérique croissant
- :: PIN en ordre décroissant
- :: PIN avec plus de deux chiffres se suivant identiques

Si ce genre de PIN est toutefois choisi, ils seront alors automatiquement rejetés par le

système.

4.2 TIME OUT

Si au cours de la programmation du code PIN, aucune touche n'est saisie pendant 5 secondes, la programmation est alors interrompue avec un message d'erreur. Le nouveau code PIN ne sera pas accepté et respectivement l'ancien code sera conservé ; la procédure doit alors être entièrement recommencée.

4.3 PROCEDURE A SUIVRE

Pour démarrer le mode de programmation au PINCodeTerminal, garder la touche « 0 » enfoncée pendant plus de 2 secondes, à l'issue d'un préambule, la fonction de programmation sera alors sélectionnée (01 à 99). Les fonctions de programmation correspondantes sont décrites en détail dans les prochains chapitres.

Pour démarrer le programme avec le logiciel, veuillez toujours appuyer sur la touche « 0 » pendant plus de trois secondes.

5.0 MISE EN SERVICE

5.1 MODE DE PROGRAMMATION - GENERALITES

Pour entrer dans le mode de programmation, il est nécessaire de garder la touche « 0 » enfoncée pendant plus de 2 secondes. Le changement dans le mode de programmation est signalisé par un clignotement court jaune et par un bip court.

5.2 MODIFICATION DU MASTER-PIN

Lors de la première mise en service, il est impératif de remplacer le code par défaut suivant

Master-PIN : 1 2 3 4 5 6 7 8

par votre Master-PIN personnel. Si le Master-PIN n'est pas changé, toutes les autres fonctionnalités ne fonctionneront pas.

Spécification pour le Master-PIN :

:: 8 chiffres

:: Consulter également le Chapitre 4.1.

Le Master-PIN personnel est requis pour les différentes étapes de programmation nécessaires à l'authentification. Conserver ce code hors de la portée des personnes non autorisées.

1. Garder la touche « 0 » ->enfocée (pendant plus de 2 secondes)
2. Entrer « 09 »
3. Entrer « Default-Master-PIN »
4. Entrer « Nouveau Master-PIN »
5. Répéter « Nouveau Master-PIN »

Si au cours de la saisie du Master-PIN, aucune touche n'est enfocée pendant 5 secondes, le Terminal est alors interrompu avec un message d'erreur. Le Master-PIN ne sera conservé et la procédure doit alors être entièrement recommencée.

Si un Master-PIN existant doit être changé, veuillez procéder comme expliqué ci-dessus. Lors de la saisie du « Master-PIN par défaut » veuillez alors entrer le Master-PIN actuel.

5.3 REGLAGE DE LA LONGUEUR DU USER-PIN

L'administrateur du système peut fixer une seule fois au cours de la mise en marche, la longueur du User-PIN dans le LSM. Cette longueur sélectionnable entre 4 - 8 chiffres vaut alors pour tous les PIN. Le Master-PIN a toujours 8 chiffres.

Suivre la procédure suivante :

1. Désactiver le verrouillage
2. Ouvrir la configuration du PINCodeTerminal (Éditer ->Propriétés de verrouillage ->PINCodeTerminal)
3. Sélectionner la longueur du PIN sous « Longueur du code PIN »
4. Confirmer en appuyant sur « Appliquer »

Attention : la longueur du User-PIN doit pas être changée après la programmation du premier PINCodeTerminal dans le système de verrouillage, sinon tous les terminaux du système devront être reprogrammés, de nouveaux PIN attribués, nouveaux PIN attribués, etc.

5.4 REGLAGE DU MODE DE FONCTIONNEMENT

L'administrateur du système peut fixer une seule fois le mode de fonctionnement au cours de la mise en service dans le LSM. Un système de verrouillage peut avoir un seul mode de fonctionnement.

Pour plus d'informations sur les modes 2 et 3 (vérification) veuillez consulter le Manuel.

Attention : le mode de fonctionnement ne peut pas être changé après la programmation du premier PINCodeTerminal, sinon tous les terminaux du système devront être reprogrammés, de nouveaux PIN attribués, des transpondeurs distribués, etc. Cela a également des implications sur l'utilisation générale de/des terminaux, c'est pourquoi il est recommandé de procéder à une bonne planification.

6.0 PROGRAMMATION

6.1 INSTRUCTION DE FERMETURE

Le PINCodeTerminal sera attribué à une fermeture G2, et ne peut (pour des raisons de sécurité) n'ouvrir que celle-ci. Pour la configuration, veuillez suivre les étapes suivantes :

1. Créer une fermeture G2
2. Marquer la fermeture G2 (par ex. cylindre de fermeture G2)
3. Cliquer sur « Éditer -> Propriétés de fermeture »
4. Sélectionner l'onglet « Porte »
5. Crocher le point « code PIN Terminal » dans le champ « Attributs de la porte »
6. Confirmer en appuyant sur « Appliquer »

7. Ainsi, le Terminal de cette fermeture G2 est configuré et la porte peut être ouverte à partir du Terminal en présence de l'autorisation correspondante (veuillez considérer les différents modes).

6.2 PROGRAMMATION DES DONNEES DU SYSTEME DE FERMETURE

6.2.1 PINCODETERMINAL

Le PINCodeTerminal ne doit être programmé qu'une seule fois avec les données du système de fermeture.

Pour programmer, veuillez procéder comme suit :

1. Éditer -> Propriétés de fermeture
2. Sélectionner l'onglet « PINCodeTerminal »
3. Sélectionner « Mode de fonctionnement » (voir Chapitre 7.0 MODES)
4. Déterminer la « longueur du code PIN »
5. Cliquer sur Accepter !
6. Sélectionner « Programmer / Réinitialiser »
7. Marquer la fermeture appropriée sous « Portes avec code PIN Terminal »
8. Démarrer la programmation de commande dans le logiciel (bouton « Programmation »), appuyer sur n'importe quelle touche (sauf « 0 »*) sur le
9. PinCodeTerminal pendant 3 secondes

*Attention : Dans le LSM 3.1 SP1, il est en outre requis d'appuyer sur la touche « 0 », toutes les touches à l'exception du « 0 » peuvent toutefois être utilisées.

6.2.2 UTILISATEUR DU CODE PIN

Créer dans le « Mode connaissance », tous les utilisateurs et respectivement tous les transpondeurs en tant qu'« Utilisateur code PIN », un transpondeur supplémentaire n'est pas nécessaire dans ce mode.

6.2.3 FERMETURE

Avant de programmer la fermeture, il est d'abord recommandé dans le « Mode connaissance », de créer tous les utilisateurs en tant qu'« Utilisateurs code PIN », et ensuite de programmer la fermeture. Sinon, les nouveaux utilisateurs de la fermeture devront à nouveau être programmés.

Recommandation : Afin de minimiser l'effort de programmation d'une fermeture installée dans une porte ou de l'éviter complètement, procéder comme suit :

- a) Créer le groupe de transpondeurs (par ex. PINCodeTerminal)
 - b) Créer les transpondeurs (type : Utilisateur code PIN)
- :: Sans créer de nouvelles personnes
:: sans Utilisateurs (n'en choisir aucun)
:: Attribuer le groupe de transpondeurs (sous a)

Ces transpondeurs peuvent être programmés à l'avance dans la fermeture appropriée. Lorsque de nouveaux utilisateurs doivent utiliser la fermeture depuis le PINCodeTerminal, ces derniers peuvent alors être utilisés.

7.0 MODES DE FONCTIONNEMENT

Trois modes de programmation différents sont disponibles sur le PINCodeTerminal :

1. Mode connaissance (PIN)
2. Possession de connaissances avec PIN plus souple
Vérification -> Transponder/SmartCard + PIN
3. Possession de connaissances avec PIN fixe
Vérification -> Transpondeur/SmartCard + PIN

Un système de verrouillage peut avoir un seul mode de fonctionnement. Pour plus d'informations sur les modes 2 et 3 (vérification) veuillez consulter le Manuel.

7.1 MODE CONNAISSANCE

Dans le Mode connaissance, une porte peut être ouverte si le bon PIN est entré. Un

transpondeur supplémentaire n'est pas nécessaire.

L'utilisateur doit cependant avoir été créé dans le logiciel en tant qu'« Utilisateur code PIN » pour obtenir un TID !

7.1.1 CRÉATION D'UN USER-PIN

Le User-PIN est composé d'une partie variable et d'une partie fixe :

User-PIN = User-PINvariable + TID(5 chiffres)

La User-PINvariable peut être librement choisie par l'utilisateur, seule la longueur par défaut doit être respectée, le TID sera attribué à l'utilisateur par l'administrateur et respectivement le programmeur du logiciel. {0}

7.1.2 INITIAL-PIN (IPIN)

Le Initial-PIN (IPIN) est une valeur numérique de 24 chiffres, qui est créé dans le LSM. Avec l'aide de l'IPIN, l'utilisateur peut activer à partir du PINCodeTerminal, son profil d'utilisateur de façon autonome et définir son propre User-PIN.

Le Initial-PIN se compose de la manière suivante :

- a) 1ère position: Mode de programmation (changement dans le mode de programmation)
- b) 2ème + 3ème positions: Fonction de programmation (par ex. apprentissage d'un nouvel utilisateur)
- c) 4ème – 24ème position: IPIN (bien que les positions 4 - 8 représentent le TID)

Pour créer le IPIN, il convient en premier lieu de créer une fermeture G2 et un Utilisateur code PIN ; veuillez procéder comme suit :

1. Ouvrir la configuration du PINCodeTerminal (Éditer ->Propriétés de fermeture-> code PIN Terminal)
2. Sélectionner Utilisateur code PIN/ Transpondeur
3. Sélectionner le bouton « Initial-PINs »
4. Une nouvelle fenêtre contenant un nouveau formulaire s'ouvre alors
5. Impression et délivrance à l'utilisateur

Les trois premiers numéros et respectivement chiffres correspondent au mode de programmation pour la création d'un nouvel utilisateur à partir du Terminal, les 21 autres chiffres sont ceux qui sont nécessaires à l'apprentissage.

Le IPIN peut être utilisé une seule fois et sera ensuite désactivé. Cela garantit qu'avec un IPIN, un seul utilisateur PIN à un terminal déterminé peut être créé.

7.1.3 AJOUT D'UN NOUVEL UTILISATEUR

Les utilisateurs PIN sont individuellement liés à l'ID du transpondeur (TID) et au système de fermeture. Les données du nouvel utilisateur sont automatiquement créées dans le terminal lorsque l'utilisateur entre une fois son code Initial-PIN (IPIN). L'utilisateur peut créer lui-même son IPIN sur le PINCodeTerminal, et s'attribuer un propre PIN (voir sur ce point le Chapitre « Trivial-PIN »).

Pour programmer, veuillez procéder comme suit :

1. Entrer « 0 » (plus de 3 sec.)
2. Entrer « 01 »
3. Entrer « IPIN » (21 chiffres*)
4. Entrer « Nouvelle User-PINvariable»
5. Répéter « Nouvelle User-PINvariable»

* Veuillez utiliser ce pour se faire les 21 derniers chiffres de l'IPIN de l'imprimé.

Pour l'utilisateur, cela signifie qu'il entre le numéro complet (24 chiffres), puis à deux reprises sa propre User-PINvariable.

La nouvelle User-PINvariable utilisateur doit respecter la longueur prévue en fonction de la spécification. Et respectivement de la configuration du Chapitre 5.3 Réglage de la longueur du USERPIN.

Il sera vérifié si la User-PINvariable correspond à un Trivial-PIN. Si tel est le cas, la User-PINvariable sera rejetée par le système.

Pour plus d'informations et concernant la création d'un User-PIN complet, veuillez vous référer au Chapitre 7.1.1 Création d'un User-PIN.

8.0 OUVERTURE

8.1 MODE CONNAISSANCE

Pour ouvrir la fermeture associée à l'aide du PINCodeTerminal, procédez comme suit : Entrer le TID (5 chiffres) + PIN programmé. L'entrée de chaque numéro individuels ne doit pas durer plus de 5 secondes.

Si la saisie et la programmation du transpondeur intégré sont correctes, la DIODE clignote 2x VERT et un signal sonore retentit. Ensuite, le transpondeur intégré libère la fermeture.

9.0 ALERTE CONCERNANT LES PILES

Afin d'obtenir un état défini du PINCodeTerminal et de minimiser les erreurs de commande, un système d'alerte des piles à 2 niveaux, a été implémenté. Le système avertit dès que la capacité des piles commence à fléchir, ce qui permet de procéder en temps voulu au remplacement nécessaire.

Niveau d'alerte 1 : le processus d'ouverture s'effectue avec un décalage dans le temps. La diode clignote en JAUNE et le vibreur retentit pendant 5 secondes. C'est seulement à l'issue de ces 5 secondes que le PINCodeTerminal envoie l'ordre d'ouverture.

Niveau d'alerte 2 : là encore le processus d'ouverture est décalé dans le temps. La diode clignote en JAUNE et le vibreur retentit alors pendant 10 secondes. C'est seulement à l'issue de ces 10 secondes que le PINCodeTerminal envoie l'ordre d'ouverture.

C'est au plus tard à ce moment qu'il faut effectuer le remplacement des piles, faute de quoi, après un bref laps de temps, le système sera dans l'impossibilité de fonctionner.

Attention : en cas d'alerte des piles il est impossible de passer en mode programmation. Autrement dit, si les piles sont faibles, vous ne pouvez plus modifier ni supprimer un transpondeur. C'est seulement lorsque vous aurez remplacé correctement les piles (voir chapitre Remplacement des piles) que le mode programmation sera à nouveau disponible.

10.0 REMPLACEMENT DES PILES

En général, seuls des techniciens formés à cet effet sont autorisés à remplacer les piles. Il convient de procéder de la manière suivante :

1. Dévisser complètement les deux vis situées sur le fond du boîtier (TORX TX6).
2. Ôter la partie avant du boîtier.
3. Retirer avec précaution les attaches de la pile de la platine (image 2).
4. Retirer les deux piles (image 1).
5. Placer les nouvelles piles ; le pôle positif doit être vers le haut (image 2). Lors du remplacement des piles, utiliser des gants non gras.
6. Réenclencher avec précaution les attaches de la pile dans la platine (image 3).
7. Replacer le boîtier.
8. Revisser les deux vis au bas du boîtier.
9. Pour réinitialiser l'état de l'alarme, veuillez suivre les étapes suivantes :
 - a) Entrer « 0 »
 - b) Entrer « 99 »
 - c) Entrer « 99999 »

Une fois le remplacement des piles effectué, toutes les fonctionnalités sont à nouveau disponibles.

Remplacez toujours les deux piles à la fois, car elles se déchargent de manière à peu près identique.

Quand vous remplacez les piles, veuillez impérativement à ce qu'il n'y ait pas de pénétration d'eau dans le boîtier et/ou que l'électronique ne soit jamais en contact avec de l'eau. Si nécessaire, frottez soigneusement la partie du boîtier fixée au mur pour enlever toute trace d'humidité. Utiliser uniquement les piles préconisées par SimonsVoss.

11.0 AVERTISSEMENT CONCERNANT LA MANIPULATION

Pour éviter l'essai systématique des User-PIN, un avertissement de manipulation est intégré dans le PINCodeTerminal. Après la 5ème entrée incorrecte d'un PIN (User-PIN, Master-PIN, etc.) un signal d'alarme retentit pendant 60 secondes et la LED clignote en rouge simultanément. Le Terminal ne peut pas être utilisé pendant cette période. En présence d'une autre erreur, le Terminal revient immédiatement au Mode de manipulation. Ce n'est qu'après avoir entré le PIN correct que le compteur sera remis à 0.

12.0 ANNEXE

12.1 DONNEES TECHNIQUES

Dimensions l x h x p : 96 mm x 96 mm x 14 mm

Poids : 102 g (piles comprises)

Matériau : Plastique

Couleur : Gris avec anneau transparent

Nombre maximum d'actionnements avec un jeu de piles : Jusqu'à 100.000 actionnement et respectivement jusqu'à 10 ans en mode veille

Distance d'actionnement du cylindre : Jusqu'à 40 cm

Distance d'actionnement au SmartRelais : Jusqu'à 120 cm

Classe de protection : IP 65

Température de fonctionnement : -20°C jusqu'à +50°C

Types de piles : Piles 2 x 3 V DC Lithium, Type CR2032

Remplacement des piles : Réservé au personnel qualifié

1.0 DENOMINAZIONE DEL PRODOTTO

1.1 INFORMAZIONI GENERALI

Il PinCodeTerminal 3068 è una „chiave“ digitale (transponder) in grado di aprire via radio i sistemi di chiusura SimonsVoss G2 con l'immissione dei codici numerici corretti. Ai fini della configurazione del sistema, è necessario configurare almeno un PIN e il rispettivo transponder integrato abbinato al sistema di chiusura. Quindi, dopo l'immissione del PIN corretto, il sistema di chiusura verrà sbloccato.

2.0 AVVISI DI PERICOLO

2.1 AVVISI DI SICUREZZA

- :: Il montaggio e l'installazione devono essere eseguiti solo da personale specializzato e addestrato.
- :: Non porre il PinCodeTerminal a contatto con olio, vernice, acidi o sostanze simili.
- :: Utilizzare solo batterie approvate da SimonsVoss.
- :: **Attenzione!** – Le batterie utilizzate in questo prodotto possono costituire un pericolo di incendio o combustione in caso di utilizzo scorretto. Non ricaricare, aprire, riscaldare oltre i 100 °C o bruciare le batterie.
- :: In caso di sostituzione delle batterie, toccare le nuove batterie solo con guanti puliti privi di grasso.
- :: Smaltire le batterie esauste in modo corretto e conservarle fuori dalla portata dei bambini.
- :: L'inversione di polarità può causare danni al PinCodeTerminal.
- :: In caso di sostituzione delle batterie, cambiare sempre tutte le batterie.
- :: Il PinCodeTerminal funziona con due batterie.
- :: Prestare attenzione che il PinCodeTerminal non sia sporco o graffiato, che la tastiera non cada a terra e che non subisca altri urti violenti.
- :: Nel sostituire le batterie, badare che l'elettronica non sia sottoposta a carichi meccanici, sia esposta ad umidità o venga danneggiata in altro modo.
- :: Tenere altresì presente che dopo la messa in funzione nel terminale deve essere

programmato immediatamente un codice PIN!

- :: L'uso di un SimonsVoss PinCodeTerminal presuppone conoscenze sul prodotto e sul software SimonsVoss. Pertanto, la programmazione del PinCodeTerminal deve essere effettuata esclusivamente da personale specializzato e addestrato.
- :: Conservare con cura il MasterPIN scelto poiché questo non è riproducibile per ragioni di sicurezza.
- :: SimonsVoss Technologies AG declina ogni responsabilità per danni dovuti ad un'errata programmazione.
- :: L'errata programmazione o un difetto al PinCodeTerminal può determinare l'impossibilità di transito attraverso una porta. SimonsVoss AG declina ogni responsabilità per conseguenze quali il mancato accesso a persone ferite o in pericolo, danni materiali o altri tipi di danni.
- :: L'alloggiamento è chiuso con due viti Torx (TX6). In questo modo la protezione dall'apertura non autorizzata risulta maggiore.
- :: SimonsVoss Technologies AG si riserva il diritto di apportare modifiche al prodotto o miglioramenti tecnici senza preavviso.
- :: La documentazione è stata redatta scrupolosamente, tuttavia non si possono escludere eventuali errori. A tale riguardo non si assume alcuna responsabilità.
- :: In presenza di divergenze di contenuto nelle versioni in lingua straniera della documentazione, fa fede l'originale in tedesco.

3.0 FUNZIONAMENTO

3.1 DESCRIZIONE GENERALE

Il PinCodeTerminal è formato dai seguenti componenti:

- :: Immissione e valutazione codice PIN
- :: Chiave digitale integrata (transponder) che apre il rispettivo sistema di chiusura se attivata in seguito alla valutazione positiva del codice PIN.

Con il PinCodeTerminal l'utente è sempre in grado di interagire con tutti i sistemi di chiusura SimonsVoss G2 (ad es. cilindri G2, Smart Relais G2, unità di attivazione ecc.) tramite il codice PIN. Sono disponibili fino a 500 diversi PIN. A seconda del

modo configurato, il PIN può essere modificato direttamente dall'utente in qualunque momento. A tale scopo non è necessario coinvolgere l'amministratore dell'impianto. Inoltre, nei sistemi di chiusura SimonsVoss G2 (con funzione ZK, ossia con gestione del controllo degli accessi e delle fasce orarie) è possibile consentire l'accesso temporaneo all'edificio ad una persona o a un gruppo di persone e registrare il PIN utilizzato e l'orario di accesso.

3.2 PROGRAMMAZIONE / SOFTWARE

Per la programmazione e l'uso del PinCodeTerminal sono necessari i seguenti componenti/software:

- :: LSM 3.1 SP1 o superiore
- :: SmartCD.G2
- :: Sistemi di chiusura G2

4.0 INFORMAZIONI GENERALI SULLA PROGRAMMAZIONE

4.1 TRIVIAL PIN

Per aumentare la sicurezza del PinCodeTerminal, il sistema non ammette PIN eccessivamente semplici.

Non sono consentiti i seguenti trivial PIN:

- :: PIN con sequenza di cifre crescente
- :: PIN con sequenza di cifre decrescente
- :: PIN con una o più cifre uguali successive

Se si sceglie un PIN di questo tipo, esso verrà automaticamente rifiutato dal sistema.

4.2 TIME OUT

Se durante la programmazione dei PIN trascorrono 5 secondi senza che venga azionato alcun tasto, la programmazione si interrompe e viene emesso un messaggio di errore. Il nuovo PIN non viene accettato o viene mantenuto quello esistente e la procedura deve essere eseguita di nuovo dall'inizio.

4.3 PROCEDURA

Per avviare il modo di programmazione sul PinCodeTerminal, tenere premuto lo „0“ per più di 2 secondi; con la successiva sequenza verrà selezionata la funzione di programmazione (da 01 a 99). Le rispettive funzioni di programmazione sono descritte dettagliatamente nei capitoli successivi.

Per avviare la programmazione con il software, tenere sempre premuto il tasto <>0 per più di tre secondi.

5.0 MESSA IN FUNZIONE

5.1 INFORMAZIONI GENERALI SULLA MODALITÀ DI PROGRAMMAZIONE

Per accedere al modo di programmazione, è necessario tenere premuto lo „0“ per più di 2 secondi. Il passaggio al modo di programmazione è indicato da un rapido lampeggiamento in giallo e un breve segnale acustico.

5.2 MODIFICA DEL MASTERPIN

Durante la prima messa in funzione è indispensabile modificare il

Master-PIN impostato in fabbrica: 1 2 3 4 5 6 7 8

con un MasterPIN di propria scelta. Tutte le altre funzionalità non possono essere utilizzate finché non viene modificato il MasterPIN.

Indicazioni per il MasterPIN:

:: a 8 cifre

:: Osservare anche il capitolo 4.1 Fehler! Verweisquelle konnte nicht gefunden werden.

Il MasterPIN personale è richiesto per varie operazioni di programmazione ai fini dell'identificazione. Conservarlo con cura e renderlo inaccessibile a persone non autorizzate.

1. Immissione „0“ -> (tenere premuto per oltre 2 secondi)
2. Immissione „09“
3. Immissione „MasterPIN predefinito“
4. Immissione „Nuovo MasterPIN“
5. Ripetizione „Nuovo MasterPIN“

Se durante l'immissione del MasterPIN non viene azionato alcun tasto per 5 secondi, il terminale si interrompe ed emette un messaggio d'errore. Il MasterPIN rimane inalterato e la procedura va ricominciata da capo.

Procedere come descritto sopra per modificare il MasterPIN esistente. In questo caso immettere come „MasterPIN predefinito“ il MasterPIN attuale.

5.3 IMPOSTAZIONE DELLA LUNGHEZZA DELLO USERPIN

In fase di messa in funzione, l'amministratore del sistema può definire la lunghezza dello UserPin nell'LSM una sola volta per tutto il sistema. Questa lunghezza, che può essere di 4-8 cifre, viene quindi applicata a tutti i PIN. Il MasterPIN ha invece sempre 8 cifre.

Procedere come segue:

1. Aprire l'impianto di chiusura
2. Aprire la configurazione del PinCodeTerminal (Modifica -> Proprietà impianti di chiusura -> PIN-Code Terminal)
3. In „Lunghezza PIN-Code“ selezionare la lunghezza del PIN
4. Confermare con „Applica“

Avviso: la lunghezza dello UserPIN non deve essere modificata dopo la programmazione del primo PinCodeTerminal; in caso contrario, tutti i terminali presenti nel sistema dovranno essere riprogrammati, si dovranno assegnare nuovi PIN e così via.

5.4 IMPOSTAZIONE DELLA MODALITÀ OPERATIVA

In fase di messa in funzione, l'amministratore del sistema può definire la modalità operativa nell'LSM una sola volta per tutto il sistema. In ogni impianto di chiusura si può

utilizzare una sola modalità operativa.

Per maggiori informazioni sui Modi 2 e 3 (verifica), consultare il manuale.

Avviso: la modalità operativa non deve essere modificata dopo la programmazione del primo PinCodeTerminal; in caso contrario, tutti i terminali presenti nel sistema dovranno essere riprogrammati, si dovranno assegnare nuovi PIN, emettere i transponder e così via. Ciò influisce anche in modo generale sull'uso del/dei terminale/i, pertanto va eseguita un'attenta pianificazione preliminare.

6.0 PROGRAMMAZIONE

6.1 ASSEGNAZIONE SISTEMA DI CHIUSURA

Il PinCodeTerminal è assegnato in modo fisso ad un sistema di chiusura G2 e, per motivi di sicurezza, può aprire solo questo sistema. Per effettuare la configurazione procedere come segue:

1. Creare un sistema di chiusura G2
2. Selezionare il sistema di chiusura G2 (ad es. cilindro di chiusura G2)
3. Fare clic su „Modifica -> proprietà sistema di chiusura“
4. Selezionare la scheda „Porta“
5. Nel campo „Attributi porta“, mettere il segno di spunta alla voce „PIN-Code Terminal“
6. Confermare con „Applica“

In questo modo si è configurato il terminale nel sistema di chiusura G2 e la porta può essere aperta tramite il terminale in caso di autorizzazione (osservare i diversi modi).

6.2 PROGRAMMAZIONE DEI DATI DELL'IMPIANTO DI CHIUSURA

6.2.1 PINCODETERMINAL

Il PinCodeTerminal va programmato una sola volta con i dati dell'impianto di chiusura.

Per eseguire la programmazione, procedere come segue:

1. Modifica -> Proprietà impianto di chiusura
2. Selezionare la scheda „PIN-Code Terminal“
3. Selezionare „Modalità operativa“ (vedere a tale scopo il capitolo 7.0 MODI)
4. Definire la „Lunghezza PIN-Code“
5. Fare clic su „Applica“.
6. Selezionare „Programma / Azzera“
7. Selezionare il rispettivo sistema di chiusura in „Porte con PIN-Code Terminal“
8. Avviare il comando di programmazione nel software (pulsante „Programmazione“)
9. Tenere premuto per 3 secondi un qualsiasi tasto (tranne lo „0“) sul PinCode-Terminal

*Avviso: nell'LSM 3.1 SP1 l'utente viene ancora invitato ad azionare lo „0“. Possono essere utilizzati però tutti i tasti tranne lo „0“.

6.2.2 UTENTE CODICE PIN

Se in „Modo conoscenza“ tutti gli utenti o transponder vengono creati come „Utenti codice PIN“, non è necessario un transponder aggiuntivo in questo modo.

6.2.3 SISTEMA DI CHIUSURA

Prima della programmazione del sistema di chiusura in „Modo conoscenza“, si consiglia di creare tutti gli utenti come „Utenti codice PIN“ e quindi di eseguire la programmazione del sistema di chiusura. In caso contrario, i nuovi utenti del sistema di chiusura installato dovranno essere riprogrammati.

Suggerimento: Per ridurre al minimo o eliminare completamente le operazioni di programmazione nella porta di un impianto di chiusura installato, procedere come segue:

- a) Creare il gruppo di transponder (ad es. PinCodeTerminal)
- b) Creare i transponder (tipo: Utente codice PIN)
:: Impostare Senza nuova persona
:: Senza utente (selezionare Nessuno)
:: Assegnare il gruppo transponder (alla voce a)

I transponder possono quindi essere programmati preliminarmente nel rispettivo sistema di chiusura. Questi possono essere utilizzati nel caso in cui altri utenti del sistema di chiusura debbano utilizzare il PinCodeTerminal.

7.0 MODALITÀ OPERATIVA MODI

Nel PinCodeTerminal esistono tre diversi modi di programmazione.

1. Modo Conoscenza (PIN)
2. Possesso conoscenza con PIN flessibile
Verifica -> Transponder/SmartCard + PIN
3. Possesso conoscenza con PIN fisso
Verifica -> Transponder/SmartCard + PIN

In un impianto di chiusura può essere utilizzato solo uno dei modi disponibili. Per maggiori informazioni sui Modi 2 e 3 (verifica), consultare il manuale.

7.1 MODO CONOSCENZA

Nel modo Conoscenza una porta può essere aperta inserendo il PIN corretto. A tale scopo non è necessario un transponder aggiuntivo.

Tuttavia, per poter ottenere un TID, l'utente deve essere creato come „Utente codice PIN“ tramite il software!

7.1.1 STRUTTURA DELLO USERPIN

Lo UserPIN è composto da una parte variabile e una parte fissa:

UserPIN = UserPINvariabile + TID (a 5 cifre)

Lo UserPINvariabile può essere scelto liberamente dall'utente (l'unica prescrizione riguarda la lunghezza), mentre il TID è assegnato all'utente in modo fisso dall'amministratore o dal software di programmazione.

7.1.2 INITIAL PIN (IPIN)

L'Initial PIN (IPIN) è un valore numerico a 24 cifre creato nell'LSM. Tramite l'IPIN, l'utente può sbloccare autonomamente il proprio profilo utente sul PinCodeTerminal e assegnare un proprio UserPIN.

L'Initial PIN si compone come segue:

- a) 1. Cifra: Modo di programmazione (passaggio al modo di programmazione)
- b) 2+3 cifra: Funzione di programmazione (ad es. apprendimento di un nuovo utente)
- c) 4.-24. Cifra: IPIN (laddove nella 4.-8 cifra è rappresentato il TID)

Per la creazione dell'IPIN, deve essere creato dapprima un sistema di chiusura G2 e un utente codice PIN. Procedere come segue:

1. Aprire la configurazione del PinCodeTerminal (Modifica -> Proprietà impianto di chiusura -> PIN-Code Terminal)
2. Selezionare Utente codice PIN/transponder
3. Selezionare il pulsante „Initial PIN“
4. Si aprirà una nuova finestra con un modulo
5. Stampa e consegna all'utente

Le prime tre cifre o numeri rappresentano il modo di programmazione per la nuova creazione dell'utente nel terminale, le ultime 21 cifre servono invece per l'apprendimento.

L'IPIN può essere utilizzato solo una volta, dopodiché viene disattivato. In questo modo si garantisce che con un IPIN possa essere creato solo un User PIN in uno specifico terminale.

7.1.3 NUOVA CREAZIONE DI UN UTENTE

Gli User PIN sono collegati individualmente ai Transponder ID (TID) dell'utente e dell'impianto di chiusura. Una volta inserito il proprio Initial PIN (IPIN), i nuovi record dati utente nel terminale verranno creati automaticamente. L'utente può creare il proprio profilo utente nel PinCodeTerminal tramite l'IPIN e assegnare il PIN personale (vedere a tale scopo anche il capitolo „Trivial PIN“).

Per eseguire la programmazione, procedere come segue:

1. Immissione „0“ (per più di 3 sec.)
2. Immissione „01“
3. Immissione „IPIN“ (a 21 cifre*)
4. Immissione „Nuovo User PINvariabile“
5. Ripetizione „Nuovo User PINvariabile“

*Utilizzare qui le ultime 21 cifre dell'IPIN stampato.

Per l'utente ciò significa immettere il numero completo (a 24 cifre) e poi per due volte lo User-PINvariabile prescelto.

Il nuovo User-PINvariabile deve essere della lunghezza prescritta o indicata nella configurazione al capitolo 5.3.

Viene verificato se lo User-PINvariabile è un Trivial PIN. In questo caso, lo User-PINvariabile verrà rifiutato dal sistema.

Per maggiori informazioni e indicazioni sulla struttura dello User PIN completo, vedere il capitolo 7.1.1.

8.0 APERTURA

8.1 MODO CONOSCENZA

Per aprire il rispettivo sistema di chiusura tramite il PinCodeTerminal, procedere come segue:

Immettere il TID (a 5 cifre) + il PIN programmato. Fra le operazioni di immissione dei singoli numeri non devono trascorrere più di 5 secondi.

Se l'immissione e la programmazione del transponder integrato sono state effettuate correttamente, il LED si accenderà 2 volte con LUCE VERDE e si udirà un segnale acustico. Quindi il transponder integrato aprirà il sistema di chiusura.

9.0 AVVISO BATTERIA

Per ottenere uno determinato stato del PinCodeTerminal e ridurre al minimo gli errori di comando, è stato integrato un sistema di avviso batteria a 2 livelli. Il sistema avvisa per tempo della riduzione della capacità delle batterie per permettere la tempestiva sostituzione delle batterie stesse.

Livello avviso batteria 1:

L'operazione di apertura viene posticipata. Il diodo lampeggia con luce GIALLA e la sirena emette un segnale acustico per 5 secondi. Il PinCodeTerminal emette il comando di apertura dopo che sono trascorsi 5 secondi.

Livello avviso batteria 2:

L'operazione di apertura viene posticipata. Il diodo lampeggia con luce GIALLA e la sirena emette ora un segnale acustico per 10 secondi. Il PinCodeTerminal emette il comando di apertura dopo che sono trascorsi 10 secondi.

In seguito è necessario effettuare la sostituzione delle batterie, poiché, in caso contrario, il sistema perderà dopo poco la capacità di funzionamento.

Avviso: in caso di avviso batteria non è più possibile accedere al modo di programmazione. Ciò significa che se il livello delle batterie è basso, non è possibile modificare o cancellare alcuna funzione. Il modo di programmazione è nuovamente disponibile una volta sostituite correttamente le batterie (vedere capitolo Sostituzione delle batterie).

10.0 SOSTITUZIONE DELLE BATTERIE

La sostituzione delle batterie va generalmente eseguita solo da personale specializzato e addestrato. A tale scopo, procedere come segue:

1. Svitare completamente le due viti (TORX TX6) del fondo dell'alloggiamento.
2. Rimuovere il lato anteriore dell'alloggiamento.
3. Allentare con cautela la staffa della batteria dalla scheda (Figura 2).
4. Rimuovere entrambe le batterie (Figura 1).

5. Inserire le nuove batterie; il polo positivo deve essere rivolto verso l'alto (Figura 2).
Toccare le nuove batterie solo con guanti puliti privi di grasso o simili.
6. Agganciare nuovamente la staffa della batteria nella scheda (Figura 3).
7. Reinserire l'alloggiamento.
8. Riavvitare nell'alloggiamento dal basso le due rispettive viti.
9. Per azzerare l'allarme batteria, eseguire le seguenti operazioni:
 - a) Immissione „0“
 - b) Immissione „99“
 - c) Immissione „99999“

Una volta eseguita la sostituzione delle batterie, tutte le funzioni sono nuovamente disponibili. Sostituire sempre entrambe le batterie, poiché si scaricano pressappoco in egual misura. Durante la sostituzione della batteria prestare attenzione che non penetri acqua nell'alloggiamento o che l'elettronica non entri in contatto con acqua. All'occorrenza, asciugare accuratamente la parte dell'alloggiamento fissata alla parete. Utilizzare sempre e soltanto batterie approvate da SimonsVoss.

11.0 AVVISO MANIPOLAZIONE

Per evitare tentativi ripetuti di immissione dello User PIN, nel PinCodeTerminal è integrato un avviso manipolazione. Dopo il 5° tentativo fallito di immissione di un PIN (User PIN, MasterPIN ecc.) verrà emesso per 60 secondi un segnale di avviso e contemporaneamente il LED lampeggerà con luce rossa. In questo intervallo il terminale non potrà essere utilizzato.

In caso di ulteriore errore, il terminale ritorna immediatamente nel modo Manipolazione. Il contatore viene azzerato solo dopo l'immissione del PIN corretto.

12.0 APPENDICE

12.1 DATI TECNICI

Dimensioni L x A x P: 96 mm x 96 mm x 14 mm

Peso: 102 g (incl. batterie)

Materiale: Plastica

Colore: Grigio con anello trasparente

Numero massimo di azionamenti con un set di batterie: Fino a 100.000 azionamenti o fino a 10 anni in stand-by

Distanza di azionamento cilindro: Fino a 40 cm

Distanza di azionamento Smart Relais: Fino a 120 cm

Classe di protezione: IP65

Campo di temperature di esercizio: Da -20 °C a +50 °C

Tipo batteria: 2 batterie al litio 3 V CC tipo CR2032

Sostituzione delle batterie: Solo a cura di personale specializzato e addestrato

1.0 PRODUCTAANDUIDING

1.1 ALGEMEEN

De PinCodeTerminal 3068 is een digitale „sleutel“ (transponder) die na het invoeren van de juiste cijfercode zonder aanraking op afstand SimonsVoss G2-sloten opent.

Voor de configuratie van het systeem moet minimaal één PIN voorgeconfigureerd zijn en de bijbehorende geïntegreerde transponder geprogrammeerd worden. Vervolgens wordt, na invoering van een juiste PIN, het bijbehorende slot vrijgegeven.

2.0 WAARSCHUWINGEN

2.1 VEILIGHEIDSADVIEZEN

- :: De montage en het inbouwen mogen alleen uitgevoerd worden door deskundigen.
- :: De PinCodeTerminal niet in aanraking brengen met olie, verf, zuren, e.d.
- :: Er mogen uitsluitend batterijen worden gebruikt die SimonsVoss heeft vrijgegeven!
- :: Let op! – De batterijen die in dit product worden gebruikt, kunnen bij verkeerde behandeling tot brand- of verbrandingsgevaar leiden. Deze batterijen mogen niet worden opgeladen, geopend, boven 100° C verhit of verbrand.
- :: Bij vervanging mogen de batterijen alleen met schone, vetvrije handschoenen worden aangeraakt.
- :: Oude en verbruikte batterijen moeten op de juiste manier als afval worden behandeld en mogen niet binnen bereik van kinderen worden bewaard.
- :: Verwisseling van de polariteit kan leiden tot beschadiging van de PinCodeTerminal.
- :: Bij vervanging van de batterijen moeten altijd alle batterijen vervangen worden.
- :: De PinCodeTerminal moet bediend worden met twee batterijen.
- :: Let erop dat de PinCodeTerminal niet verontreinigd of bekrast wordt, het toetsenbord niet op de vloer valt of andere heftige klappen moet verduren.
- :: Bij vervanging van de batterijen moet er op gelet worden dat de elektronica niet mechanisch wordt belast of wordt blootgesteld aan vocht, dan wel op een andere manier wordt beschadigd.
- :: Verder dient u er op te letten dat de terminal onmiddellijk na inbedrijfstelling wordt geprogrammeerd met een PIN-code!

- :: Voor de omgang met een SimonsVoss PinCodeTerminal is kennis van de behandeling van het product en de SimonsVoss software vereist. Daarom mag alleen daartoe opgeleid deskundig personeel de PinCodeTerminal programmeren.
- :: Bewaar de gekozen MasterPIN goed en op een veilige plaats aangezien deze om veiligheidsredenen niet kan worden gereproduceerd.
- :: Voor beschadiging als gevolg van foutieve programmering aanvaardt SimonsVoss Technologies AG geen aansprakelijkheid.
- :: Door foutief geprogrammeerde of defecte PinCodeTerminals kan de doorgang door een deur geblokkeerd zijn. Voor gevolgen, zoals een geblokkeerde toegang tot ge-wonden of personen in gevaar, materiële of andere schade, is SimonsVoss AG niet aansprakelijk.
- :: De behuizing is beveiligd met twee Torx-schroeven (TX6). Daardoor is de beveiliging tegen onbevoegd openen nog verder verhoogd.
- :: De SimonsVoss Technologies AG behoudt zich het recht voor productaanpassingen of nieuwe technische ontwikkelingen zonder aankondiging vooraf uit te voeren.
- :: De documentatie werd te goeder trouw vervaardigd. Eventuele fouten kunnen niette-min niet worden uitgesloten. Voor dergelijke fouten wordt geen aansprakelijkheid aanvaard.
- :: Indien afwijkingen van de inhoud in vertaalde versies van de documentatie optreden, geldt in geval van twijfel de tekst van het Duitse origineel.

3.0 FUNCTIONEREN

3.1 ALGEMENE BESCHRIJVING

De PinCodeTerminal bestaat uit de volgende componenten:

- :: PIN-code invoeren en activeren
- :: Geïntegreerde digitale sleutel (transponder) die het bijbehorende sluitelement opent zodra de juiste PIN-code is ingevoerd.

Met de PinCodeTerminal kunt u zodoende te allen tijde alle SimonsVoss G2-sluitelementen (bijv. cilinder G2, Smart Relais G2 en scherpshakelunits, etc.) via de PIN-code

bedienen.

Er zijn maximaal 500 verschillende PIN's beschikbaar. Aanpassingen van de PIN kunnen op elk gewenst moment, afhankelijk van de geconfigureerde modi, door de gebruiker zelf worden uitgevoerd. Hierbij hoeft de systeembeheerder niet te worden betrokken. Bovendien is het mogelijk in SimonsVoss G2-sluitelementen (met ZK-functie, d.w.z. bediening van toegangscontrole en tijdzones) een bepaalde persoon of groep personen ook een tijdelijk beperkte toegang tot het gebouw te geven, alsook te registreren welke PIN op welk moment toegang had.

3.2 PROGRAMMERING / SOFTWARE

Voor de programmering en het gebruik van de PinCodeTerminal zijn de volgende componenten/software nodig:

- :: LSM 3.1 SP1 of hoger
- :: SmartCD.G2
- :: G2-sluitelementen

4.0 PROGRAMMERING ALGEMEEN

4.1 TRIVIAL PIN

Om de veiligheid van de PinCodeTerminal te verhogen, worden bijzonder eenvoudige PIN's door het systeem niet geaccepteerd.

De volgende Trivial PIN's zijn niet toegestaan:

- :: PIN met oplopende cijfervolgorde
- :: PIN met aflopende cijfervolgorde
- :: PIN met meer dan twee identieke cijfers achter elkaar

Als een PIN volgens een dergelijke constructie wordt gekozen, wordt deze automatisch door het systeem geweigerd.

4.2 TIME OUT

Als tijdens de programmering van de PIN 5 seconden lang geen toets wordt aangeraakt, wordt de programmering met een foutmelding afgebroken. De nieuwe PIN wordt in dat geval niet geaccepteerd of de oude blijft bestaan en er moet opnieuw begonnen worden.

4.3 HANDELWIJZE

Om de programmeermodus op de PinCodeTerminal te starten, moet de „0“ langer dan 2 seconden worden ingedrukt en vervolgens wordt de programmeerfunctie geselecteerd (01 tot 99). De bijbehorende programmeerfuncties worden in de volgende hoofdstukken uitgebreid beschreven.

Om de programmering met de software te starten altijd een toets <>0 langer dan drie seconden ingedrukt houden.

5.0 INBEDRIJFSTELLING

5.1 PROGRAMMEERMODUS ALGEMEEN

Om in de programmeermodus te komen, moet de „0“ langer dan 2 seconden worden ingedrukt. De overgang naar de programmeermodus wordt weergegeven door een kort geel knipperend signaal en een korte toon.

5.2 MASTERPIN AANPASSEN

Bij de eerste inbedrijfstelling is het absoluut vereist de door de fabriek ingestelde

Master-PIN: 1 2 3 4 5 6 7 8

te vervangen door een eigen MasterPin. Als de MasterPIN niet wordt aangepast, kunnen alle andere functies niet worden gebruikt.

Voorwaarde voor de MasterPIN:

:: 8 cijfers

:: Neem ook hoofdstuk 4.1 in acht. Fehler! Verweisquelle konnte nicht gefunden werden.

De persoonlijke MasterPIN is voor diverse programmeringen als legitimatie nodig. Bewaar deze op een veilige plaats, ontoegankelijk voor onbevoegden.

1. Kies „0“ -> (langer dan 2 seconden ingedrukt houden)
2. Kies „09“
3. Kies „Default-MasterPIN“
4. Kies „Nieuwe MasterPIN“
5. Herhaal „Nieuwe MasterPIN“

Als tijdens de programmering van de MasterPIN 5 seconden lang geen toets wordt aangeraakt, wordt de programmering met een foutmelding afgebroken. De MasterPIN blijft hetzelfde en de handeling moet opnieuw van begin af worden uitgevoerd.

Als een bestaande MasterPIN veranderd moet worden, gaat u als hierboven beschreven te werk. Als „Default-MasterPIN“ geeft u in dit geval de actuele MasterPIN op.

5.3 INSTELLEN VAN DE LENGTE VAN DE USERPIN

De systeembeheerder kan bij de inbedrijfstelling één keer de lengte van de UserPIN in de LSM aangeven. Deze lengte kan tussen 4 en 8 cijfers bedragen en geldt voor iedere PIN. De MasterPIN heeft altijd 8 cijfers.

Ga als volgt te werk:

1. Sluitsysteem openen
2. Configuratie van de PinCodeTerminal openen (Bewerken -> eigenschappen sluitsystemen -> PIN-Code Terminal)
3. Onder „Lengte PIN-code“ kiest u de lengte van de PIN
4. Bevestig uw keuze met „Aannemen“

Let op: De lengte van de UserPIN mag na de programmering van de eerste PinCode Terminal in het sluitsysteem niet meer veranderd worden omdat anders alle terminals in

het systeem geherprogrammeerd moeten worden, nieuwe PIN toekennen, etc.

5.4 INSTELLEN VAN GEBRUIKSWIJZE

De systeembeheerder kan bij de inbedrijfstelling één keer de gebruikswijze in de LSM aangeven. Binnen een sluitsysteem kan altijd maar één gebruikswijze worden toegepast.

Meer informatie over de modi 2 en 3 (Controle) vindt u in het handboek.

Let op: De gebruikswijze mag na de programmering van de eerste PinCodeTerminal in het sluitsysteem niet meer veranderd worden omdat anders alle terminals in het systeem geherprogrammeerd moeten worden, nieuwe PIN toekennen, verstrekking transponders, etc. Dat heeft ook algemene uitwerking op het gebruik van de terminal(s). Daarom moet op dit gebied zorgvuldig vooraf worden gepland.

6.0 PROGRAMMERING

6.1 TOEKENNING SLUITELEMENT

De PinCodeTerminal wordt vast aan een bepaald G2-sluitelement toegekend en kan (om veiligheidsredenen) alleen dit betreffende element openen. Voor de configuratie voert u de volgende stappen uit:

1. G2-sluitelement aanmaken
2. G2-sluitelement markeren (bijv. cilinder G2)
3. „Bewerken -> eigenschappen sluitelement“ aanklikken
4. Registertab „Deur“ selecteren
5. In het veld „Deurattributen“ bij het punt „PIN-CodeTerminal“ aanvinken
6. Bevestig uw keuze met „Aannemen“

Op die manier werd de terminal gekoppeld aan het G2-sluitelement geconfigureerd en de deur kan door bevoegden via de terminal geopend worden (let hierbij op de verschillende modi).

6.2 PROGRAMMERING VAN DE SLUITSYSTEEMGEGEVENS

6.2.1 PINCODETERMINAL

De PinCodeTerminal hoeft maar één keer geprogrammeerd worden met de gegevens van het sluitsysteem.

Voor de programmering gaat u als volgt te werk:

1. Bewerk -> eigenschappen sluitsysteem
2. Registertab „PIN-CodeTerminal“ selecteren
3. „Gebruikswijze“ selecteren (zie ook hoofdstuk 7.0 MODI)
4. „Lengte PIN-code“ bepalen
5. Aannemen aanklikken!
6. „Programmeren / resetten“ selecteren
7. Bijbehorende sluitelement onder „Deuren met PIN-CodeTerminals“ markeren
8. Programmeeropdracht in de software starten (button „Programmering“)
9. Willekeurige toets (behalve de „0“) op de PinCodeTerminal 3 seconden in-gedrukt houden

*Let op: In de LSM 3.1 SP1 wordt momenteel nog verlangd dat u de toets „0“ indrukt, maar alle andere toetsen behalve de „0“ mogen gebruikt worden.

6.2.2 PIN-CODE GEBRUIKERS

In de „Kennismodus“ worden alle gebruikers, dan wel transponders als „PIN-CodeGebruiker“ aangemaakt; een extra transponder is in deze modus niet nodig.

6.2.3 SLUITELEMENT

Voor de programmering van het sluitelement wordt in de „Kennismodus“ geadviseerd eerst alle gebruikers als „PIN-CodeGebruiker“ aan te maken en pas daarna het sluitelement te programmeren. Anders moeten nieuwe gebruikers bij reeds gemonteerde sluitelementen opnieuw worden geprogrammeerd.

Advies: Om de programmeerhandelingen in een geïnstalleerd sluitelement bij de deur te beperken, dan wel volledig te vermijden, gaat u als volgt te werk:

- a) Transpondergroep aanmaken (bijv. PinCodeTerminal)
- b) Transponder (type: PIN-CodeGebruiker) aanmaken
- :: Zonder nieuwe persoon aanmaken
- :: zonder gebruiker (geen enkele selecteren)
- :: Transpondergroep (onder a) toekennen

Deze transponders kunnen daarna vooraf in het bijbehorende sluitelement geprogrammeerd worden. Als nieuwe gebruikers bij het sluitelement gebruik moeten kunnen maken van de PinCodeTerminal kunnen zij worden toegekend.

7.0 GEBRUIKSWIJZE MODI

Bij de PinCodeTerminal kunt u gebruikmaken van drie verschillende programmeermodi:

1. Kennismodus (PIN)
2. Bezit van kennis met flexibele PIN
Controle -> Transponder/SmartCard + PIN
3. Bezit van kennis met vaste PIN
Controle -> Transponder/SmartCard + PIN

Binnen een sluitsysteem kan altijd maar één van de modi gebruikt worden. Meer informatie over de modi 2 en 3 (Controle) vindt u in het handboek.

7.1 KENNISMODUS

In de kennismodus kan een deur met een correcte PIN worden geopend. Een extra transponder is hiervoor niet nodig. De gebruiker moet echter via de software als „PIN-CodeGebruiker“ zijn aangemaakt om een TID te krijgen!

7.1.1 CONSTRUCTIE USERPIN

De UserPIN is samengesteld uit een variabel en een vast deel:

UserPIN = UserPINvariabel + TID(5-cijferig)

De UserPINvariabel kan vrij door de gebruiker gekozen worden, waarbij alleen de vast-gelegde lengte moet worden nageleefd. De TID krijgt de gebruiker vast door de beheerder, dan wel de programmeersoftware toegekend.

7.1.2 INITIAL-PIN (IPIN)

De Initial-PIN (IPIN) is een 24-cijferig getal dat in de LSM wordt aangemaakt. Met behulp van de IPIN kan de gebruiker zelfstandig op de PinCodeTerminal zijn profiel vrij-geven en een eigen UserPIN toekennen.

De Initial-PIN is als volgt samengesteld:

- a) 1e positie: Programmeermodus (overstap naar de programmeermodus)
- b) 2e + 3e positie: Programmeerfunctie (bijv. instuderen van een nieuwe gebruiker)
- c) 4e - 24e positie: IPIN (waarbij bij de 4e - 8e positie de TID wordt weergegeven)

Voor het aanmaken van een IPIN moet eerst een G2-sluitelement en een PIN-CodeGebruiker worden aangemaakt. Daarvoor gaat u als volgt te werk:

1. Configuratie van de PinCodeTerminal openen (Bewerken -> eigenschappen sluitsystemen -> PIN-Code Terminal)
2. PIN-CodeGebruiker/transponder selecteren
3. Button „Initial-PIN's" selecteren
4. Er gaat een nieuw venster met een formulier open
5. Uitprinten en overhandigen aan de gebruiker

De eerste drie tekens staan voor de programmeermodus voor het aanmaken van de gebruiker op de terminal, de laatste 21 posities zijn nodig om in te studeren.

De IPIN kan maar één keer worden gebruikt en wordt daarna gedeactiveerd. Op die manier is verzekerd dat met een bepaalde IPIN maar één User-PIN bij een vastgestelde terminal kan worden aangemaakt.

7.1.3 AANMAKEN VAN EEN GEBRUIKER

De User-PIN's zijn individueel gebonden aan de transponder-ID (TID) van de gebruiker en het sluitsysteem. Nieuwe datasets van de gebruiker worden automatisch in de ter-

minal aangemaakt als de gebruiker eenmalig de Initial-PIN (IPIN) invoert. De gebruiker kan zichzelf via een IPIN in de PinCodeTerminal aanmaken en een eigen PIN toekennen (zie ook hoofdstuk „Trivial-PIN“)

Voor de programmering gaat u als volgt te werk:

1. Kies „0“ (langer dan 3 sec.)
2. Kies „01“
3. Voer „IPIN“ (21-cijferig*) in
4. Voer „Nieuwe User-PINvariabel“ in
5. Herhaal „Nieuwe User-PINvariabel“

*Hier de laatste 21 posities van de IPIN uit de print gebruiken.

Voor de gebruiker betekent dit dat het volledig nummer (24-cijferig) wordt ingevoerd en daarna twee keer de zelf gekozen User-PINvariabel.

De nieuwe User-PINvariabel moet over de juiste lengte volgens de voorwaarden, dan wel de configuratie conform hoofdstuk 5.3 beschikken.

Er wordt gecontroleerd of het bij de User-PINvariabel om een Trivial-PIN gaat. Als dat het geval is, wordt de User-PINvariabel door het systeem verworpen.

Voor informatie en constructie van de volledige User-PIN, zie hoofdstuk 7.1.1.

8.0 OPENING

8.1 KENNISMODUS

Om het bijbehorende sluitelement met behulp van de PinCodeTerminal te openen, gaat u als volgt te werk:

De TID (5-cijferig) + geprogrammeerde PIN invoeren. Tussen het invoeren van de afzonderlijke nummers mogen maximaal 5 seconden verstrijken.

Bij correct invoeren en programmeren van de geïntegreerde transponder licht de LED

2x GROEN op en er klinkt een signaal. Vervolgens opent de geïntegreerde transponder het sluitelement.

9.0 BATTERIJ-ALARM

Om een vastgestelde toestand van de PinCodeTerminal te realiseren en bedieningsfouten te beperken, werd een 2-traps batterij-alarm geïntegreerd.

Er wordt vroeg genoeg attent op gemaakt dat de batterijcapaciteit afneemt zodat de batterijen op tijd vervangen kunnen worden.

Batterij-alarm stap 1:

Het openen wordt uitgevoerd met een tijdvertraging. De diode knippert GEEL en de zoemer is 5 seconden lang te horen. Pas na het verstrijken van de 5 seconden verstuurt de PinCodeTerminal het commando.

Batterij-alarm stap 2:

Het openen wordt uitgevoerd met een tijdvertraging. De diode knippert GEEL en de zoemer is nu 10 seconden lang te horen. Pas na het verstrijken van de 10 seconden verstuurt de PinCodeTerminal het commando.

Uiterlijk op dit tijdstip moeten de batterijen worden vervangen, anders is het systeem korte tijd later buiten werking.

Let op: Bij een batterij-alarm is het niet mogelijk in de programmeermodus te komen. D.w.z. dat bij een zwakke batterij geen functies aangepast of gewist kunnen worden. Pas na het succesvol vervangen van de batterijen (zie hoofdstuk Batterijvervanging) is de programmeermodus weer beschikbaar.

10.0 BATTERIJVERVANGING

In het algemeen mogen batterijen alleen door geschoold, deskundig personeel worden vervangen. Hierbij gaat u als volgt te werk:

1. De beide schroeven in de onderkant van de behuizing volledig los schroeven (TORX TX6).

2. De voorkant van de behuizing verwijderen.
3. De batterijbeugel behoedzaam uit het bodemplaatje losmaken (afb. 2).
4. Beide batterijen verwijderen (afb. 1).
5. De nieuwe batterijen plaatsen; de pluspool moet hierbij naar boven wijzen (afb. 2)
De nieuwe batterijen mogen alleen met schone, vetvrije handschoenen o.i.d worden aangeraakt.
6. De batterijbeugel weer behoedzaam in het bodemplaatje haken (afb. 3).
7. De voorkant weer op de behuizing plaatsen.
8. De beide schroeven van de behuizing weer van onderen in de behuizing schroeven.
9. Om het batterij-alarm weer in de oude toestand terug te brengen, doet u de volgende stappen:
 - a) Kies „0“
 - b) Kies „99“
 - c) Kies „9999“

Na het vervangen van de batterijen zijn alle functies weer beschikbaar. Altijd beide batterijen tegelijk vervangen aangezien ze ongeveer even veel lading verliezen. Bij de vervanging van batterijen moet er beslist op gelet worden dat geen water in de behuizing binnendringt of de elektronica met water in aanraking komt. Indien nodig moet de behuizing die aan de wand bevestigd is zorgvuldig gedroogd worden. Uitsluitend batterijen gebruiken die door SimonsVoss zijn vrijgegeven.

11.0 MANIPULATIE-ALARM

Om het systematische uitproberen van User-PIN's tegen te gaan, is een manipulatiealarm in de PinCodeTerminal opgenomen. Na de 5e keer foutief invoeren van een PIN (User-PIN, MasterPIN, etc.) is 60 seconden lang een alarmsignaal te horen en knippert de LED tegelijk rood. Op dat moment kan de terminal niet worden bediend.

Bij een hernieuwde foutieve PIN gaat de terminal onmiddellijk over in de manipulatiemodus. Pas na het invoeren van een correcte PIN wordt de teller weer op 0 gezet.

12.0 BIJLAGE

12.1 TECHNISCHE GEGEVENS

Afmetingen: b x h x d: 96 mm x 96 mm x 14 mm

Gewicht: 102 g (incl. batterijen)

Materiaal: Kunststof

Kleur: Grijs met transparante ring

Maximaal aantal activeringen met één set batterijen: Tot max. 100.000 activeringen of maximaal 10 jaar standby

Bedienafstand cilinder: Tot max. 40 cm

Bedienafstand Smart Relais: Tot max. 120 cm

Beschermingsklasse: IP 65

Arbeidstemperatuurbereik: -20° C tot +50° C

Soort batterij: 2 x 3 V DC lithiumbatterije type CR2032

Batterijvervanging: Alleen door geschoold, deskundig personeel

1.0 DESCRIPCIÓN DEL PRODUCTO

1.1 GENERALIDADES

El terminal de código PIN 3068 es una «llave» digital (transpondedor) que, introduciendo un código numérico correcto, abre cierres SimonsVoss G2 vía radio sin contacto. Para configurar el sistema, se debe preconfigurar al menos un PIN y el transpondedor integrado correspondiente debe estar programado en concordancia con el cierre. A continuación, tras introducir un PIN correcto, se desbloquea el cierre correspondiente.

2.0 INDICACIONES DE ADVERTENCIA

2.1 INDICACIONES DE SEGURIDAD

- :: El montaje y la instalación solo pueden ser realizados por personal especialista cualificado.
- :: El terminal de código PIN no se debe poner en contacto con aceite, pintura, ácidos y similares.
- :: Solo se pueden utilizar pilas que hayan sido autorizadas por SimonsVoss.
- :: ¡Cuidado! : las pilas utilizadas en este producto pueden suponer peligro de incendio o de quemaduras en caso de mala utilización. Abstenerse de recargar, abrir, calentar por encima de 100 °C o quemar estas pilas.
- :: Al cambiar las pilas, las nuevas solo se deben tocar con guantes limpios y sin grasa.
- :: Las pilas viejas y usadas se deben eliminar de un modo profesional y deben mantenerse fuera del alcance de los niños.
- :: Si se intercambia la polaridad, se pueden producir desperfectos en el terminal de código PIN.
- :: Al cambiar las pilas, se deben sustituir todas ellas.
- :: El terminal de código PIN se debe hacer funcionar con dos pilas.
- :: Procure que el terminal de código PIN no se ensucie ni se raye, que el teclado no se caiga al suelo y no se vea sometido a ningún otro tipo de golpes fuertes.
- :: Al cambiar las pilas, procure que el sistema electrónico no se vea sometido a cargas mecánicas ni quede expuesto a la humedad ya que, de lo contrario, podría

sufrir daños.

- :: Además, tenga en cuenta que el terminal se debe programar con un código PIN inmediatamente después de su puesta en funcionamiento.
- :: La manipulación de un terminal de código PIN SimonsVoss requiere de conocimientos en el manejo del producto y en el software SimonsVoss. Por eso mismo, la programación del terminal de código PIN solo debe ser realizada por personal especialista cualificado.
- :: Le rogamos que guarde bien y en un lugar seguro el PIN maestro seleccionado, ya que por razones de seguridad no se puede reproducir.
- :: SimonsVoss Technologies AG no asume ningún tipo de responsabilidad por daños provocados por una programación incorrecta.
- :: El acceso por una puerta puede quedar bloqueado si el terminal de código PIN está incorrectamente programado o está averiado. SimonsVoss AG no asume ningún tipo de responsabilidad por las consecuencias derivadas de dicho bloqueo de acceso a personas heridas o en peligro, daños materiales o cualquier otro tipo de daños.
- :: La carcasa está protegida con dos tornillos Torx (TX6). Así se aumenta la seguridad contra una apertura no autorizada.
- :: SimonsVoss Technologies AG se reserva el derecho a efectuar modificaciones o mejoras técnicas en el producto sin previo aviso.
- :: Aunque la documentación ha sido elaborada según nuestro leal saber y entender, no se excluye la posibilidad de que pueda contener errores. En este sentido, tampoco se puede asumir ninguna responsabilidad.
- :: En caso de que existan discrepancias de contenido en las versiones en lenguas extranjeras de la documentación, la versión válida en caso de duda será el original alemán.

3.0 MODO DE FUNCIONAMIENTO

3.1 DESCRIPCIÓN GENERAL

El terminal de código PIN consta de los siguientes componentes:

- :: Introducción y comprobación de código PIN
- :: Llave digital integrada (transpondedor) que abre el cierre correspondiente si se dispara tras la correcta comprobación del código PIN.

Con el terminal de código PIN estará en condiciones de interactuar mediante código PIN en cualquier momento con todos los cierres SimonsVoss G2 (p. ej. cilindros G2, Smart Relés G2, así como unidades de activación, etc.).

Hay disponibles hasta 500 PIN diferentes. El usuario puede modificar el PIN por sí mismo en cualquier momento dependiendo de los modos configurados. Esto no requiere involucrar al administrador de la instalación. Además, en los cierres SimonsVoss G2 (con función ZK, es decir, control de acceso y control temporal de zonas) también se puede dar acceso a una persona o un grupo de personas por tiempo limitado, así como protocolizar que PIN tiene acceso en cada momento.

3.2 PROGRAMACIÓN / SOFTWARE

Para programar y usar el terminal de código PIN se necesitan los siguientes componentes/software:

- :: LSM 3.1 SP1 con superior
- :: SmartCD.G2
- :: Cierres G2

4.0 GENERALIDADES PROGRAMACIÓN

4.1 PIN TRIVIAL

Para aumentar la seguridad del terminal de código PIN, el sistema no admite PIN demasiado fáciles.

Los siguientes PIN triviales no están admitidos:

- :: PIN con sucesión ascendente de cifras
- :: PIN con sucesión descendente de cifras
- :: PIN con más de dos cifras iguales consecutivas

Si se elige un PIN que responda a estas estructuras, será automáticamente rechazado por el sistema.

4.2 TIME OUT

Si no se acciona ninguna tecla en un período de 5 segundos durante la programación del PIN, esta se cancelará con un mensaje de error. Por tanto, el nuevo PIN no será aceptado y seguirá siendo válido el anterior, por lo que se deberá repetir el proceso.

4.3 PROCEDIMIENTO

Para iniciar el modo de programación en el terminal de código PIN se debe mantener pulsado el «0» durante más de 2 segundos y seleccionar en el preámbulo que aparece a continuación la función de programación (01 al 99). Las funciones de programación correspondientes se describen minuciosamente en los siguientes capítulos.

Para iniciar la programación con el software, mantener pulsada una de las teclas <>0 durante más de tres segundos.

5.0 PUESTA EN FUNCIONAMIENTO

5.1 GENERALIDADES MODO DE PROGRAMACIÓN

Para acceder al modo de programación es necesario mantener pulsado el «0» durante más de 2 segundos. El paso al modo de programación se indica con un breve destello amarillo y un sonido breve.

5.2 CAMBIAR EL PIN MAESTRO

En la primera puesta en funcionamiento es absolutamente necesario sustituir el PIN maestro ajustado de fábrica

PIN maestro: 1 2 3 4 5 6 7 8

por un PIN maestro propio. Si no se modifica el PIN maestro, no se podrán utilizar el

resto de las funciones.

Norma para el PIN maestro:

:: 8 cifras

:: Le rogamos que también tenga en cuenta el capítulo 4.1

El PIN maestro personal es necesario para proceder a la autenticación en los diversos procesos de programación. Guárdelo en un lugar seguro y sin acceso a personas no autorizadas.

1. Entrada «0» -> (mantener pulsado más de 2 segundos)
2. Entrada «09»
3. Entrada «PIN maestro predeterminado»
4. Entrada «Nuevo PIN maestro»
5. Repetición «Nuevo PIN maestro»

Si no se acciona ninguna tecla en un período de 5 segundos durante la introducción del PIN maestro, el terminal la cancelará con un mensaje de error. El PIN maestro seguirá siendo válido y se deberá repetir el proceso desde el principio.

Si fuese necesario modificar un PIN maestro existente, se debe proceder como se explica más arriba. En este caso, se debe introducir el PIN maestro actual en lugar del «PIN maestro predeterminado».

5.3 AJUSTE DE LA LONGITUD DEL PIN DE USUARIO

En el curso de la puesta en funcionamiento del sistema, el administrador del sistema puede determinar una sola vez la longitud del PIN de usuario en el LSM. Esta longitud, a elegir entre 4 y 8 cifras, será entonces válida para todos los PIN. El PIN maestro siempre tiene 8 cifras.

Proceda del siguiente modo:

1. Abrir la instalación de cierre
2. Abrir la configuración del terminal de código PIN (Editar -> Configuración instalaciones de cierre -> Terminal de código PIN)

3. Seleccionar la longitud del código PIN en «Longitud código PIN»
4. Confirmar con «Aceptar»

Atención: no se debe cambiar la longitud del PIN de usuario tras la programación del primer terminal de código PIN en la instalación de cierre ya que, de lo contrario, se deberían reprogramar todos los terminales del sistema, asignarles un nuevo PIN, etc.

5.4 AJUSTE DEL MODO OPERATIVO

En el curso de la puesta en funcionamiento del sistema, el administrador del sistema puede determinar una sola vez el modo operativo en el LSM. En una instalación de cierre, se puede utilizar respectivamente un modo operativo.

En el manual podrá encontrar más información sobre los modos 2 y 3 (Verificación)

Atención: no se debe cambiar el modo operativo tras la programación del primer terminal de código PIN ya que, de lo contrario, se deberían reprogramar todos los terminales del sistema, asignarles un nuevo PIN, emitir transpondedores, etc. Todo esto también tiene una repercusión general en la utilización del terminal o de los terminales, por lo que es necesario realizar una cuidadosa planificación previa.

6.0 PROGRAMACIÓN

6.1 ASIGNACIÓN DEL CIERRE

El terminal de código PIN está permanentemente asignado a un cierre G2 y (por motivos de seguridad) se limita a abrir solo este. Para su configuración, siga los pasos siguientes:

1. Generar cierre G2
2. Marcar cierre G2 (p. ej. cilindro de cierre G2)
3. Hacer clic en «Editar -> Configuración cierre»
4. Seleccionar pestaña «Puerta»

5. Marcar la casilla en el campo «Atributos de puerta» del punto «Terminal de código PIN»
6. Confirmar con «Aceptar»

De este modo, el terminal queda configurado en este cierre G2 y la puerta se puede abrir obteniendo autorización mediante el terminal (tenga en cuenta los diferentes modos).

6.2 PROGRAMACIÓN DE LOS DATOS DE LA INSTALACIÓN DE CIERRE

6.2.1 TERMINAL DE CÓDIGO PIN

El terminal de código PIN se debe programar una sola vez con los datos de la instalación de cierre.

Proceder del siguiente modo para la programación:

1. Editar -> Configuración instalación de cierre
2. Seleccionar pestaña «Terminal de código PIN»
3. Seleccionar «Modo operativo» (véase al respecto el capítulo 7.0 MODI)
4. Establecer «Longitud del código PIN»
5. Hacer clic en Aceptar
6. Seleccionar «Programar/Restaurar»
7. Marcar el cierre correspondiente en «Puertas con terminales de código PIN»
8. Iniciar la orden de programación en el software (botón «Programación»)
9. Mantener pulsada cualquier tecla (excepto el «0»*) durante 3 segundos en el terminal de código PIN

*Atención: en el LSM 3.1 SP1 se le pedirá todavía que accione el «0», pero se pueden utilizar todas las teclas excepto el «0».

6.2.2 USUARIO DE CÓDIGO PIN

En el «Modo conocimiento», poner todos los usuarios o transpondedores como modelo «Usuario de código PIN»; en este modo no se necesita un transpondedor adicional.

6.2.3 CIERRE

Antes de programar el cierre, en el «Modo conocimiento» se recomienda crear primero todos los usuarios como «Usuario de código PIN» y solo después proceder a programar el cierre. De lo contrario, habría que reprogramar los nuevos usuarios en el cierre bloqueado.

Recomendación: para reducir al mínimo o evitar por completo las exigencias de programación en una instalación de cierre montada en la puerta, proceder del modo siguiente:

- a) Generar grupo de transpondedores (p. ej. Terminal de código PIN)
 - b) Crear transpondedor (modelo: Usuario de código PIN)
- :: Crear sin nueva persona
:: Sin usuario (sin seleccionar)
:: Asignar grupo de transpondedores (en a))

Estos transpondedores pueden ser programados previamente en el cierre correspondiente. Estos se podrán utilizar cuando los nuevos usuarios tengan que utilizar el terminal de código PIN en el cierre.

7.0 MODO OPERATIVO MODOS

En el terminal de código PIN se dispone de tres modos de programación diferentes:

1. Modo conocimiento (PIN)
2. Conocimiento-propiedad con PIN flexible
Verificación -> Transpondedor/SmartCard + PIN
3. Conocimiento-propiedad con PIN fijo
Verificación -> Transpondedor/SmartCard + PIN

En cada instalación de cierre solo se puede utilizar respectivamente uno de los modos. En el manual podrá encontrar más información sobre los modos 2 y 3 (Verificación)

7.1 MODO CONOCIMIENTO

En el modo conocimiento se puede abrir una puerta introduciendo correctamente el PIN. Para esto no se necesita un transpondedor adicional.

No obstante, el usuario debe disponer de un TID creado con el software como «Usuario de código PIN».

7.1.1 ESTRUCTURA DEL PIN DE USUARIO

El PIN de usuario se compone de una parte variable y una parte fija:

PIN de usuario = PIN de usuariovariable + TID (5 cifras)

El PIN de usuariovariable puede ser elegido libremente por el usuario teniendo solo en cuenta la longitud predeterminada, mientras que el TID será asignado al usuario por el administrador o por el software de programación.

7.1.2 PIN INICIAL (IPIN)

El PIN inicial (IPIN) es un valor numérico de 24 cifras que se genera en el LSM. Con ayuda del IPIN, el usuario puede activar por sí mismo su perfil de usuario en el terminal de código PIN y adjudicarle un PIN de usuario propio.

El PIN inicial se compone de la siguiente manera:

- a) 1.^a cifra: Modo de programación (cambia al modo de programación)
- b) 2.^a + 3.^a cifra: Función de programación (p. ej. programar información de un nuevo usuario)
- c) 4.^a - 24.^a cifra: IPIN (que incluye el TID entre la 4.^a y la 8.^a cifra)

Para elaborar el IPIN, se debe crear primero un cierre G2 y un usuario de código PIN procediendo del siguiente modo:

1. Abrir la configuración del terminal de código PIN (Editar -> Configuración instalaciones de cierre -> Terminal de código PIN)
2. Seleccionar Usuario de código PIN/transpondedor
3. Pulsar botón «PIN inicial»

4. Se abre una nueva ventana con un formulario
5. Imprimir y entregar al usuario

Las tres primeras cifras con números hacen referencia al modo de programación del usuario de nueva creación en el terminal y las últimas 21 cifras son números necesarios para programar la información.

El IPIN solo se puede utilizar una vez y después se desactiva. De este modo se garantiza que solo se pueda crear un PIN de usuario en un terminal determinado con un IPIN.

7.1.3 NUEVA CREACIÓN DE UN USUARIO

Los PIN de usuario van individualmente ligados a los identificadores de transpondedor (TID) del usuario y de la instalación de cierre. Los nuevos juegos de datos de usuario se crean automáticamente en el terminal cuando el usuario introduce PIN inicial (IPIN). El usuario puede crearse a sí mismo en el terminal de código PIN mediante su IPIN, y asignarse un PIN propio (véase también al respecto el capítulo «PIN trivial»).

Proceder del siguiente modo para la programación:

1. Entrada «0» (más de 3 segundos)
2. Entrada «01»
3. Entrada «IPIN» (21 cifras*)
4. Entrada «Nuevo PIN de usuariovariable»
5. Repetición «Nuevo PIN de usuariovariable»

*Aquí se deben utilizar las 21 últimas cifras del IPIN del impreso.

Para el usuario esto significa que debe introducir el número completo (24 cifras) y después introducir dos veces el PIN de usuariovariable que haya seleccionado.

El nuevo PIN de usuariovariable debe presentar la longitud correspondiente a la norma o configuración conforme al capítulo 5.3. Se comprueba si el PIN de usuariovariable es un PIN trivial. En este caso, el sistema rechazará el PIN de usuariovariable.

Para más información sobre la estructura de todos los PIN de usuario, consulte el capítulo 7.1.1.

8.0 APERTURA

8.1 MODO CONOCIMIENTO

Para abrir el cierre correspondiente con la ayuda del terminal del código PIN, proceder del siguiente modo:

Introducir el TID (5 cifras) + PIN programado. Entre la introducción de cada uno de los números no pueden transcurrir más de 5 segundos.

En caso de una introducción y programación correctas del transpondedor integrado, el LED VERDE se iluminará dos veces y sonará una señal. A continuación, el transpondedor integrado abrirá el cierre.

9.0 AVISO DE CAMBIO DE PILAS

Para conseguir un estado definido del terminal de código PIN y reducir al mínimo los fallos de manejo, sea integrado un sistema de aviso de cambio de pilas en 2 fases.

Cuando la capacidad de las pilas disminuye, se advierte con tiempo suficiente para poder proceder oportunamente a cambiar las pilas.

Fase 1 de aviso de cambio de pila:

el proceso de apertura se ejecuta con retraso. El diodo parpadea en AMARILLO y el zumbador suena durante 5 segundos. El terminal de código PIN solo emite la orden de apertura después de transcurridos esos 5 segundos.

Fase 2 de aviso de cambio de pila:

el proceso de apertura se ejecuta con retraso. El diodo parpadea en AMARILLO y el zumbador suena durante 10 segundos. El terminal de código PIN solo emite la orden de apertura después de transcurridos esos 10 segundos.

El cambio de pilas se debe realizar como muy tarde en este momento ya que, de lo contrario, el sistema perderá su capacidad de funcionar en muy poco tiempo.

Atención: durante el aviso de cambio de pilas no se puede acceder al modo pro-

gramación, es decir, que con las pilas casi agotadas no se puede modificar o borrar ninguna función. El modo de programación volverá a estar disponible cuando se hayan sustituido con éxito las pilas (véase capítulo Cambio de pilas).

10.0 CAMBIO DE PILAS

Por regla general, el cambio de pilas solo puede ser realizado por personal especialista cualificado. En este caso, proceder del modo siguiente:

1. Destornillar por completo los dos tornillos de la base de la carcasa (TORX TX6).
2. Retirar la parte frontal de la carcasa.
3. Soltar cuidadosamente la patilla de las pilas de la platina (Fig. 2).
4. Extraer las dos pilas (Fig. 1)
5. Colocar las pilas nuevas; el polo positivo debe apuntar hacia arriba (Fig. 2). Las pilas nuevas solo se deben tocar con guantes limpios y sin grasa o similares.
6. Volver a enganchar cuidadosamente la patilla de las pilas en la platina (Fig. 3).
7. Poner de nuevo la carcasa.
8. Atornillar de nuevo en la carcasa los dos tornillos desde la parte inferior.
9. Para restaurar el estado de alarma de las pilas, ejecute los siguientes pasos:
 - a) Entrada «0»
 - b) Entrada «99»
 - c) Entrada «99999»

Tras el cambio de las pilas, vuelven a estar disponibles todas las funciones.

Sustituir siempre las dos pilas, ya que ambas suelen descargarse aproximadamente al mismo tiempo. Al cambiar las pilas asegúrese de que no penetre agua en la carcasa o de que el sistema electrónico no entre en contacto con el agua. En caso necesario, seque cuidadosamente la parte de la carcasa fijada a la pared. Utilizar siempre pilas autorizadas por SimonsVoss.

11.0 AVISO DE MANIPULACIÓN

Para impedir cualquier intento sistemático de prueba de PIN de usuario, en el terminal del código PIN va integrado un sistema de aviso de manipulación. Tras el 5.º intento erróneo de introducción de un PIN (PIN de usuario, PIN Maestro, etc.) sonará durante 60 segundos una señal de advertencia y el LED destellará al mismo tiempo en rojo. Durante ese tiempo, no se podrá usar el terminal.

Si se introduce nuevamente un PIN erróneo, el terminal cambiará inmediatamente de nuevo al modo de manipulación. El contador volverá a ponerse en 0 solo si se introduce un PIN correcto.

12.0 ANEXO

12.1 DATOS TÉCNICOS

Dimensiones A x H x P: 96 mm x 96 mm x 14 mm

Peso: 102 g (pilas incluidas)

Material: Plástico

Color: Gris con anillo transparente

Número máximo de activaciones con un juego de pilas: Hasta 100.000 activaciones o 10 años en espera

Distancia de activación del cilindro: Hasta 40 cm

Distancia de activación del Smart Relé: Hasta 120 cm

Clase de protección: IP 65

Rango de temperaturas de trabajo: De -20 °C a +50 °C

Modelo de pilas: 2 pilas de litio de 3 V modelo CR2032

Cambio de pilas: Solo por personal especialista cualificado

COMPANY
HEADQUARTERS
SimonsVoss
Technologies GmbH
Feringastrasse 4
85774 Unterfoehring
Germany
Tel. +49 89 992280
www.simons-voss.com

ÖSTERREICH
SimonsVoss
Technologies AG
Kärntner Ring 5-7
1010 Wien
Tel. +43 1 20511601146

SCHWEIZ
Simons Voss
Technologies AG
Dreikönigstrasse 31a
8002 Zürich
Tel. +41 44 208 3241

ITALY
SimonsVoss
Technologies AG
Via Torino, 2
Milano 20123
Tel. +39 02 72 54 67 63

FRANCE
SimonsVoss
Technologies SAS
Immeuble „Les Portes des
Paris“
1/3 Rue du Rempart
93160 Noisy le Grand
Tél. 01-48 15 14 80

SPAIN + PORTUGAL
Erkoch Ibérica SL
Avda. Lehendakari
Aguirre 38-40
48014 Bilbao
Spain
Tel. +34 94 4124900

UNITED KINGDOM
SimonsVoss
Technologies Ltd.
1200 Century Way
Thorpe Park : : Colton
Leeds : : LS15 8ZA
Phone 01132 515036

BENELUX
SimonsVoss
Technologies bv
Evert van de Beekstraat 1-104
1118 CL Schiphol
Tel. 020-6 54 18 82

NORDIC COUNTRIES
SimonsVoss Technologies AB
Ostermalmstorg 1
Stockholm 114 42
Sweden

MIDDLE EAST
SimonsVoss Technologies
(Middle East) FZE
P.O.Box 184220
Dubai
UAE
Phone +971 4 227 4851

ASIA
SimonsVoss
SecurityTechnologies
(Asia) Pte. Ltd.
151 Lorong Chuan
New Tech Park #05-02
Lobby B
Singapore 556741
Phone +65-62 27 73 18

