PIN CODE TERMINAL MANUAL

Date: May 2012

PIN CODE TERMINAL MANUAL

PIN CODE TERMINAL
MANUAL

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.

This pin code terminal is a product which can be used both indoors and outdoors. The product features its own power source and can thus be operated as a completely stand-alone system. Installation is a very easy task as no wiring whatsoever is required.

Thanks to its modularity, this component is seamlessly integrated into the SimonsVoss System 3060 and, like all SimonsVoss components, it can be programmed using the locking plan software LSM 3.1 SP1 or higher.

1.2 Order code

TRA.PC.TERMINAL

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 keypad 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 Operating modes

The pin code terminal operates in five different operating modes:

Mode:	Explanation:
Standby	The pin code terminal is on standby and consumes very little power.
Open	After the correct PIN has been entered, the lock device is activated via the wireless network and can now be operated.
Programming	This mode allows • the different individual PINs • or the associated, integrated transponder to be programmed or reset.
Battery warning	A two-level battery warning system signals in good time when batteries need to be changed.
Manipulation alarm	A manipulation alarm is integrated to prevent PINs being tried out on a systematic basis. When in this mode, the pin code terminal cannot be operated for a defined period of time.

3.3 How to use

Once the pin code terminal has been put into operation and configured, it forms together with a SimonsVoss lock device a so-called intelligent lock within the 3060 System. Basic configuration is completed using the SimonsVoss software while the different PINs and integrated transponders are programmed directly on the terminal. The exact approaches for programming individual PIN codes or the associated transponder datasets, selecting the different modes and using the pin code terminal are described in the following sections.

3.4 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 Change 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 **Fehler! Verweisquelle konnte nicht gefunden werden.**

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.

Also see Section 7.0 OPERATING TYPE MODES.

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 the terminal as follows:

1. Edit → Locking system properties
2. Select "PIN code terminal" tab
3. Select "Operating type" (see Section 7.0 MODES)
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 operating mode can be used per locking system.

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 $\text{PIN}_{\textbf{variable}}$ + TID (5 digits)

Users can choose the user $\text{PIN}_{\textbf{variable}}$ 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 twenty-one 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 one-time 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 PIN$_{\text{variable}}$"**
5. Repeat **"New user PIN$_{\text{variable}}$"**

*****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 PIN$_{\text{variable}}$ that they chose themselves twice.

The new user PIN$_{\text{variable}}$ must feature the corresponding length as specified or configured according to Section 5.3 SETTING THE USER PIN LENGTH.

A check is made to ensure that the user PIN$_{\text{variable}}$ is not a trivial PIN. If it is, the system rejects the user PIN$_{\text{variable}}$.

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

7.1.4 Changing a user PIN$_{\text{variable}}$

Users can change their PIN at any time.

Programme as follows:

1. Enter **"0"**
2. Enter **"05"**
3. Enter **"Old user PIN$_{\text{variable}}$"**
4. Enter **"Transponder ID"**
5. Enter **"New user PIN$_{\text{variable}}$"**
6. Repeat **"New user PIN$_{\text{variable}}$"**

7.1.5 Changing a forgotten user PIN

If a user forgets their user PIN, a new user PIN can be issued using a "Replacement PIN" generated by the administrator.

Programme as follows:

1. Enter **"0"**
2. Enter **"03"**
3. Enter **"Replacement PIN"**
4. Enter **"New user PIN$_{\text{variable}}$"**
5. Repeat **"New user PIN$_{\text{variable}}$"**

This means that the user enters their complete 24-digit number and then the user PIN$_{\text{variable}}$ that they chose themselves twice.

A check is made to ensure that the PIN is not a trivial PIN or a replacement PIN which has already been used. If it is, the system rejects the change of user PIN$_{\text{variable}}$.

7.1.6 Overview of programming functions

Preamble:	User input:	Meaning:
0 01	IPIN UP UP	New PIN using IPIN
0 03	Replacement PIN UP UP	Replacement for existing PIN
0 05	Upo TID UPn UPn	Change existing PIN

Explanation of abbreviations:

Abbreviation:	Description:
IPIN	Initial PIN
UP	User PIN
UPo	User PIN old
UPn	User PIN new
TID	Transponder ID

7.2 Verification (flexible pin)

In order to improve security at main entrances, for example, it is possible to select "Verification" (knowledge-possession mode) on the pin code terminal. In this mode, the use of a transponder or smart card is made more secured by using a user PIN. The door is only opened if the two - the TID and the user PIN - match.
There is thus no security risk if the transponder is stolen or lost as the user also needs to know the user PIN to activate the lock device.

7.2.1 Firmware versions

When using the knowledge possession-based system, the lock device and the pin code terminal must both support the G2 protocol. Both need to be specially configured in the LSM for this mode.

This mode can be configured and used for the following lock device firmware versions and higher:

- Smart Relay.G2 (2.3.07 and later)
- Cylinder.G2 (2.3.07 and later)
- Smart Handle.G2 (standard)
- Smart Handle SC (standard)
- Cylinder SC (standard)
- Smart Relay 2 (standard)

7.2.2 Entering a user

In this mode, a user is not added using the IPIN, but the user's corresponding transponder is required instead. The lock device, transponder and pin code terminal all need to be programmed beforehand.

1. Activate the transponder on the lock device (the lock device will not engage)

   Then complete the following steps on the pin code terminal:

2. Enter **"0"**
3. Enter **"02"**
4. Enter **"User PIN"**
5. Repeat **"User PIN"**
   - Terminal carries out opening protocol with the lock device
   - TID not available → New dataset is saved
6. TID available → Terminal rejects process

The lock device and the pin code terminal should be installed, so that they are within communication range of one another.

The lock device is not activated during the programming process. To open the door, first activate the transponder on the lock device and then enter the programmed PIN code.

7.2.3 Changing a user PIN in possession-knowledge mode

Users can change their PIN at any time.

Programme a change as follows:

1. Activate transponder on the lock device
2. Enter **"0"**
3. Enter **"06"**
4. Enter **"Old user PIN"**
5. Enter **"New user PIN"**
6. Repeat **"New user PIN"**

7.2.4 Changing a forgotten user PIN

If a user forgets their user PIN, the administrator can reset the corresponding TID on the pin code terminal.

This can be done as follows:

1. Enter **"0"**
2. Enter **"04"**

3. Enter **"Master PIN"**
4. Enter **"TID"**

The entry has thus been reset for the TID and the user can re-programme the new PIN themselves. Also see 7.2.2 Entering a users.

7.3 Verification (fixed pin)

In order to improve security at main entrances, for example, it is possible to select "Verification" (knowledge-possession mode) on the pin code terminal. In this mode, the use of a transponder or smart card is made more secured by using a user PIN. The door is only opened if the two - the TID and the user PIN - match.

Unlike verification mode (flexible PIN), the user PIN is issued by the system in this case and cannot be changed.

There is thus no security risk if the transponder is stolen or lost as the user also needs to know the user PIN to activate the lock device.

7.3.1 Firmware versions

When using the knowledge possession-based system, the lock device and the pin code terminal must both support the G2 protocol. Both need to be specially configured in the LSM for this mode.

This mode can be configured and used for the following lock device firmware versions and higher:

- Smart Relay.G2 (2.3.07 and later)
- Cylinder.G2 (2.3.07 and later)
- Smart Handle.G2 (standard)
- Smart Handle SC (standard)
- Cylinder SC (standard)
- Smart Relay 2 (standard)

7.3.2 Programming a user

There is no need to create a user on the pin code terminal in this mode. The G2 lock device, G2 transponder and pin code terminal need to be programmed beforehand.

The lock device and the pin code terminal should be installed, so that they are within communication range of one another.

7.3.3 Issuing a user PIN

The fixed PIN is predetermined by the LSM and can be provided to the user as described below.

This is done as follows:

1. Open locking system properties (Edit → Locking system properties)
2. Select "PIN code terminal" tab
3. Select the corresponding transponder from the list
4. Press the "PINs" button
5. A new window will open with the user PIN, which can be printed out and given to the user.

7.3.4 Issuing a forgotten user PIN

If a user forgets their user PIN, the administrator can print out the issued fixed user pin again and give it to the user.

Also see Section 7.3.3. Issuing a user PIN.

7.4 General programming options

7.4.1 Deleting a user

If an employee leaves the company, for example, the TID can be deleted. This is a good idea if the TID is not to be re-issued or is not going to be used for the time being.

Programme the deletion as follows:

1. Enter **"0"**
2. Enter **"04"**
3. Enter **"Master PIN"**
4. Enter **"TID"**

This programming option is available in all three modes.

8.0 READOUT FROM TERMINAL

Proceed as follows to obtain a readout from the pin code terminal:

1. Open locking system properties (Edit → Locking system properties)
2. Select "PIN code terminal" tab
3. Once under the "PIN code terminal" tab, select “Programme / Reset” button
4. A new window will open
5. Press the "Readout" button
6. Hold down any key <>0 on the pin code terminal for 2 seconds when requested to do so by the software.

This function is available in all three modes.

9.0 CHANGING THE MASTER PIN

The master PIN can be changed at any time. The valid master PIN is required whenever you wish to change the master PIN.

Please proceed as follows:

Specifications for the master PIN:

- 8 digits
- Please also observe Section **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**

Your personal master PIN is required to validate a number of programming procedures. Please keep it in a safe place where it cannot be accessed by unauthorised persons.

1. Enter **"0"**
2. Enter **"09"**
3. Enter **"Old 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 master PIN remains valid and the process must be started again.

10.0 MASTER RESET

The master reset allows you to delete all information in the pin code terminal and to reset components to their original delivery settings. Only use this function in case of real need, because the terminal will no longer be able to function in the locking system after a reset. All data must be reprogrammed after a master reset.

Programme the master reset as follows:

1. Enter **"0"**
2. Enter **"010"**
3. Enter **"Master PIN"**
4. Repeat **"Master PIN"**

All data in the terminal have now been permanently deleted. To re-programme the components, you will need to start by putting the terminal into operation again.

11.0 OPENING

11.1 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.

11.2 Verification

Proceed as follows to open the associated lock device in possession-knowledge mode (verification):

1. Activate transponder on the lock device
2. Enter user PIN on the pin code terminal

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 lock device will then open or activate.

12.0 MEANING OF LED SIGNALS

Signal	Description	Duration
Key confirmation	Brief, high-pitched tone and green flashing	Split seconds
OK	Two long, high-pitched tones and green flashing (synchronised)	Second
Error	Long, deep tone and yellow flashing	Seconds
Low battery	Long, deep tone and yellow flashing	5 seconds
Batteries empty	Long, deep tone and yellow flashing	10 seconds
Manipulation	Long, deep tone and red flashing	60 seconds

13.0 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).

14.0 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.

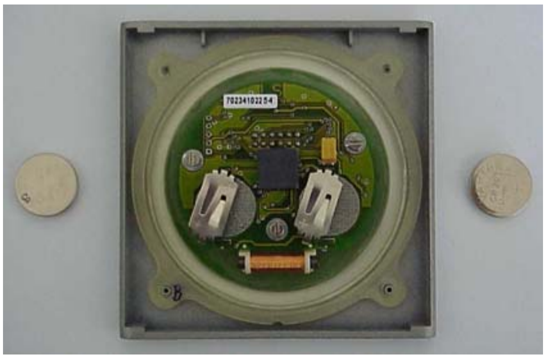

Fig 1

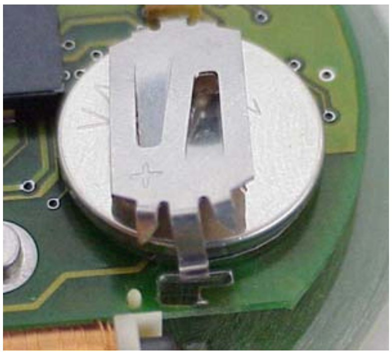

Fig 2

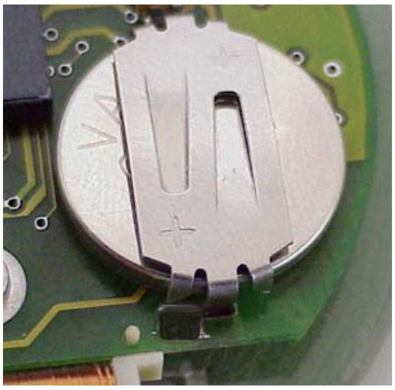

Fig 3

15.0 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.

16.0 SPECIAL FUNCTIONS

The pin code terminal can be used to activate SimonsVoss activation units (VdS Block Lock 3066). To do so, the terminal is installed within the activation unit's transmission range. After the correct PIN has been entered, the activation unit is enabled and the alarm system can now be armed or disarmed. This function is only available in Mode 1 (knowledge).

The SimonsVoss VdS-certified activation units require a double opening protocol for arming and disarming switch operations (double click if the system is to be activated or deactivated using a transponder).

The section below explains how to configure the pin code terminal, so that it emulates the "double click" and is thus suitable to perform arming and disarming switching operations. Proceed as follows:

1. Enter **"0"**
2. Enter **"07"**
3. Enter **"Master PIN"**
4. Enter:
   - **"1"** Block lock mode is activated
   - **"0"** Block lock mode is deactivated

If configured correctly, the pin code terminal saves the change and a positive feedback signal is emitted (LED and buzzer).

This programming option is only available in knowledge mode.

Important: only ever set the double opening protocol (double click) when using a SimonsVoss VdS Block Lock 3066. If you do otherwise, malfunctions or unwanted effects may arise as no doors can be opened in block lock mode.

It is also possible to switch between the two configurations at any 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).

17.0 APPENDIX

17.1 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□ to +50□
Battery type	2 x 3 V DC lithium batteries, type CR2032
Battery replacement	By trained specialist personnel only

17.2 TERM DEFINITIONS

Term	**Explanation**
Access list	List of entry/exit events which are saved in the lock device
Access profile	Defines the lock devices which can be activated using a transponder which contains this profile
IPIN	Initial PIN to add a new user on the pin code terminal
IPIN NP	Additional initial PIN required to re-programme a forgotten user PIN.
LID	Lock ID: unambiguous identifier for a lock device within a SimonsVoss locking system
Lock device	General term for all products which can be activated using a transponder
Locking system	Lock devices and transponders which belong together and are managed as a group.
Locking system password	Password to secure locking system
LSM	Locking System Management: Database-driven PC software used to manage a SimonsVoss locking system
Network	SimonsVoss WaveNet network used to operate lock devices in online modus
SID	Locking system ID: ID number for a locking system
Smart CD	Programming device: device needed to pro-

	gramme SimonsVoss components
TID	Transponder ID: unambiguous identifier number for a transponder
Transponder	Medium used to communicate with a lock device
Time zone groups	Groups which are part of a time zone plan
Time zone plans	time zone plan which can be saved to a lock device