PIN code terminal

Manual

13.11.2026

Simons Voss technologies

Contents

1. Intended use ... 4
2. General safety instructions ... 5
3. Product-specific safety instructions ... 8
4. Meaning of the text formatting ... 9
5. Description of functions ... 10
   5.1 Operating modes ... 10
   5.2 Concept ... 11
6. Setup: ... 12
   6.1 Prerequisites ... 12
   6.2 Trivial PIN ... 12
   6.3 Changing the master PIN ... 12
   6.4 Determining the PIN length ... 13
   6.5 Set mode ... 14
   6.6 Preparing locking devices in LSM ... 15
   6.7 Programming the PIN code terminal ... 16
   6.8 Programme locking device ... 17
7. Fastening ... 18
8. Mode overview ... 20
9. Management ... 22
   9.1 Knowledge = PIN (knowledge) ... 22
      9.1.1 Creating users ... 22
      9.1.2 Unlock user with initial PIN ... 23
      9.1.3 Changing the user PIN ... 25
      9.1.4 Change forgotten user PIN with replacement PIN ... 25
      9.1.5 Delete user ... 27
   9.2 Verification (flexible PIN) = Transponder + PIN (possession and knowledge) ... 28
      9.2.1 Creating users ... 28
      9.2.2 Activating users with identification media ... 28
      9.2.3 Changing the user PIN ... 29
      9.2.4 Change forgotten user PIN ... 30
      9.2.5 Delete user ... 30
   9.3 Verification with fixed PIN = Transponder + PIN 2 (possession and knowledge - unchangeable PIN) ... 31
      9.3.1 Creating users ... 31
      9.3.2 Issue user PIN ... 31

9.3.3 Changing the user PIN ... 32
9.3.4 Delete user ... 32
9.4 Reading out the PIN code terminal ... 33
10. Opening ... 35
10.1 Knowledge mode ... 35
10.2 Verification mode ... 35
11. Battery management ... 36
11.1 Battery warning levels ... 36
11.2 Battery replacement ... 36
12. Protection against systematic testing ... 39
13. Double-click simulation (block lock operation on block lock 3066) ... 40
14. Reset ... 42
14.1 Resetting with LSM ... 42
14.2 Hardware reset ... 43
15. Overview of all programming codes ... 44
16. Signalling ... 46
17. Technical specifications ... 47
17.1 Scale drawing ... 48
17.2 Drilling template ... 49
18. Declaration of conformity ... 50
19. Help and other information ... 51

1. Intended use

The PIN code terminal can be used to activate respective SimonsVoss locking devices *(such as locking cylinders, SmartHandles or SmartRelays)* by entering a numerical code.

- Up to 500 User PINs
- User PINs between 4 and 8 character
- After entering the Master PIN: User PINs configurable directly on the PIN code terminal
- Overarching transponder level possible

The PIN code terminal is weatherproof and suitable for both indoor and outdoor use. Battery operation and wireless operation make installation wireless and very easy. Like your other locking devices, you can manage the PIN code terminal in the corresponding locking system software (LSM).

2. General safety instructions

Signal word: Possible immediate effects of non-compliance
WARNING: Death or serious injury (possible, but unlikely)
CAUTION: Minor injury
IMPORTANT: Property damage or malfunction
NOTE: Low or none



WARNING

Blocked access

Access through a door may stay blocked due to incorrectly fitted and/or incorrectly programmed components. SimonsVoss Technologies GmbH is not liable for the consequences of blocked access such as access to injured or endangered persons, material damage or other damage!

Blocked access through manipulation of the product

If you change the product on your own, malfunctions can occur and access through a door can be blocked.

- Modify the product only when needed and only in the manner described in the documentation.

Do not swallow battery. Danger of burns from hazardous substances

This product contains lithium button cell batteries. Swallowing the button cell battery, in can result in severe internal burns leading to death in as little as two hours.

1. Keep new and used batteries away from children.
2. If the battery compartment does not close securely, cease using the product and keep it away from children.
3. If you think batteries have been swallowed or are in any part of the body, seek medical attention immediately.

Risk of explosion due to incorrect battery type

Inserting the wrong type of battery can cause an explosion.

- Only use the batteries specified in the technical data.



CAUTION

Fire hazard posed by batteries

The batteries used may pose a fire or burn hazard if handled incorrectly.

1. Do not try to charge, open, heat or burn the batteries.
2. Do not short-circuit the batteries.

IMPORTANT

Damage resulting from electrostatic discharge (ESD) when enclosure is open

This product contains electronic components that may be damaged by electrostatic discharges.

1. Use ESD-compliant working materials (e.g. Grounding strap).
2. Ground yourself before carrying out any work that could bring you into contact with the electronics. For this purpose, touch earthed metallic surfaces (e.g. door frames, water pipes or heating valves).

Damage resulting from liquids

This product contains electronic and/or mechanic components that may be damaged by liquids of any kind.

Damage resulting from aggressive cleaning agents

The surface of this product may be damaged as a result of the use of unsuitable cleaning agents.

- Only use cleaning agents that are suitable for plastic surfaces.

Damage as a result of mechanical impact

This product contains electronic components that may be damaged by mechanical impacts of any kind.

1. Avoid touching the electronics.
2. Avoid other mechanical influences on the electronics.

Damage due to polarity reversal

This product contains electronic components that may be damaged by reverse polarity of the power source.

- Do not reverse the polarity of the voltage source (batteries or mains adapters).

Operational malfunction due to radio interference

This product may be affected by electromagnetic or magnetic interference.

- Do not mount or place the product directly next to devices that could cause electromagnetic or magnetic interference (switching power supplies!).

Communication interference due to metallic surfaces

This product communicates wirelessly. Metallic surfaces can greatly reduce the range of the product.

- Do not mount or place the product on or near metallic surfaces.



NOTE

Intended use

SimonsVoss-products are designed exclusively for opening and closing doors and similar objects.

- Do not use SimonsVoss products for any other purposes.

Malfunctions due to poor contact or different discharge

Contact surfaces that are too small/contaminated or different discharged batteries can lead to malfunctions.

1. Only use batteries that are approved by SimonsVoss.
2. Do not touch the contacts of the new batteries with your hands.
3. Use clean and grease-free gloves.
4. Always replace all batteries at the same time.

Qualifications required

Installation and initial operation require specialist knowledge.

- Only trained specialist personnel may install and put the product into operation.

Incorrect installation

SimonsVoss Technologies GmbH accepts no liability for damage caused to doors or components due to incorrect fitting or installation.

Modifications or further technical developments cannot be excluded and may be implemented without notice.

The German language version is the original instruction manual. Other languages (drafting in the contract language) are translations of the original instructions.

Read and follow all installation, installation, and commissioning instructions. Pass these instructions and any maintenance instructions to the user.

3. Product-specific safety instructions

IMPORTANT

Master PIN loss

The Master PIN is an essential, integral part of the security concept. No more administrative changes can be made to the device if the Master PIN is lost.

1. Keep the Master PIN in a safe place.
2. Make the Master PIN visible for authorized persons at any time.



NOTE

PIN code terminal not compatible with SmartRelay 3 or AX products

The PIN code terminal cannot be used together with SmartRelay 3 or AX products (e.g. SmartHandle AX).

PIN structure in knowledge mode: User PIN and TID

In knowledge mode, the PIN to be input consists of User PIN and TID. While the users choose User PIN freely, they must remember the TID specified by the LSM, i.e. a total of 9-13 digits (depending on the length of the User PIN).

4. Meaning of the text formatting

This documentation uses text formatting and design elements to facilitate understanding. The table explains the meaning of possible text formatting:

Example	button
☑ Example ☐ Example	checkbox
◉ Example	Option
[Example]	Tab
"Example"	Name of a displayed window
| Example |	Upper programme bar
Example	Entry in the expanded upper programme bar
Example	Context menu entry
▼ Example	Name of a drop-down menu
"Example"	Selection option in a drop-down menu
"Example"	Area
Example	Field
Example	Name of a (Windows) service
Example	Commands (e.g. Windows CMD commands)
`Example`	Database entry
[Example]	MobileKey type selection

5. Description of functions

The PIN code terminal is divided into two parts:

PIN entry

Here you enter the PIN, which is then checked.



Transponder

The integrated transponder opens the corresponding lock the PIN is correct.

You can use it to address all SimonsVossG2 locking devices (e.g. locking cylinders, SmartRelays, activation units, etc.) with a PIN at any time.

You have up to 500 User PINs available. depending on the mode you have configured (see*Mode overview [▸ 20]*), users can change their PINs themselves.

Combination with SimonsVossZK locking devices (with access control and time zone control) also enables the following functions:

- Temporary authorisations for persons or groups of persons.
- Recording of when the corresponding locking device was opened with which PIN.

5.1 Operating modes

The PIN code terminal is in one of these five operating states:

Status	Explanation
Standby	The PIN code terminal is in a idle state where very little energy is consumed.
Opening	After entering a correct PIN, the PIN code terminal responds to the locking device, which can then be activated.
Programming	In this operating state: - The individual different PINs are programmed or reset. - Integrated transponder programmed or reset.
Battery warning	A two-stage battery warning system signals in good time when the batteries need to be replaced.

Status	Explanation
Manipulation alarm	The manipulation alarm prevents a systematic attempt at possible PINs. The PIN code terminal cannot be operated in this (time-defined) state.

5.2 Concept

After commissioning and configuration, the PIN code terminal and SimonsVosslocking device form a so-called "intellectual lock" within System 3060.

Basic settings are programmed with LSM, while PINs and the integrated transponder are programmed directly at the PIN code terminal.

6. Setup:



NOTE

Programming aborted due to timeout

The PIN code terminal cancels the entry after five seconds without pressing a button. The entry will then not be accepted or the previous settings will be retained.

1. You can cancel the entry by no longer pressing any keys.
2. In this case, start the input from the beginning.

6.1 Prerequisites

You will need the following for programming:

- LSM 3.1 SP1 or higher
- SMARTCD.G2
- Locking device to be opened with the PIN code terminal.

6.2 Trivial PIN

Very simple PINs ("trivial PINs") are insecure. The PIN code terminal therefore does not permit such PINs in order to increase security.

The following criteria apply to trivial PINs:

- Increasing number sequence (example: **12345678**)
- Descending number sequence (example: **87654321**)
- PINs with the same number repeated more than twice in succession **11112222**)

PINs that meet one or more of these criteria are automatically rejected.

6.3 Changing the master PIN

At initial start-up, replace the factory Master PIN (12345678) with your ownMaster PIN. Otherwise, you will not be able to use all other functions.

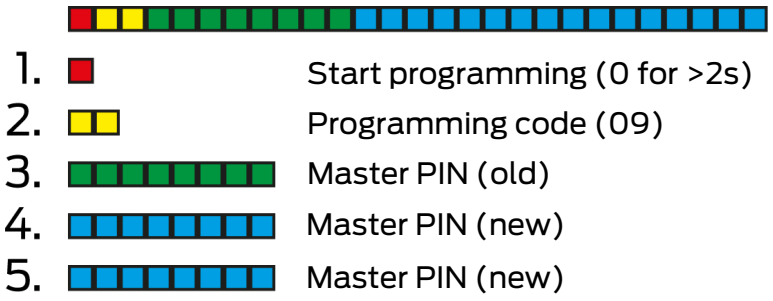
The Master PIN must be eight digits and must not be a trivial PIN (see *Trivial PIN [▸ 12]*).

IMPORTANT

Master PIN loss

The Master PIN is an essential, integral part of the security concept. No more administrative changes can be made to the device if the Master PIN is lost.

1. Keep the Master PIN in a safe place.
2. Make the Master PIN visible for authorized persons at any time.



1. Press `0` for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter `09`.
3. Enter the previous or factory Master PIN.
4. Enter the new Master PIN.
5. Re-enter the new Master PIN.
   ↳ PIN code terminal beeps and flashes green twice.

↳ Master PIN is changed.

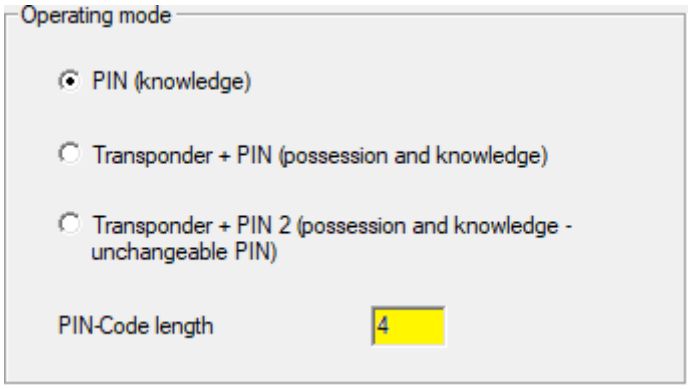
6.4 Determining the PIN length

The length of the User PIN is set once in LSM during commissioning (4 to 8 digits) and applies to all User PINs.

✓ LSM open.

1. Open the properties of your locking system using | Edit | - Locking system properties.
2. Change to the [PIN-Code Terminal] tab.

3. Enter the desired length in the field *PIN-Code length*.



4. Click on the Apply button.

↳ Length of User PIN changed.

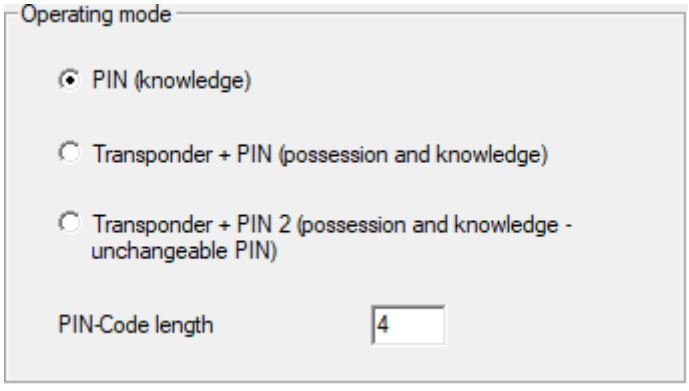
NOTE

Subsequent modification of the length of the User PIN

The length of the User PIN applies to the entire locking system. If it is subsequently changed, considerable effort is required (programming requirement at all PIN code terminals available in the system, allocation of new onesUser PINs, ...).

- Do not change the length of the User PIN after programming the first PIN code terminal in the locking system.

6.5 Set mode

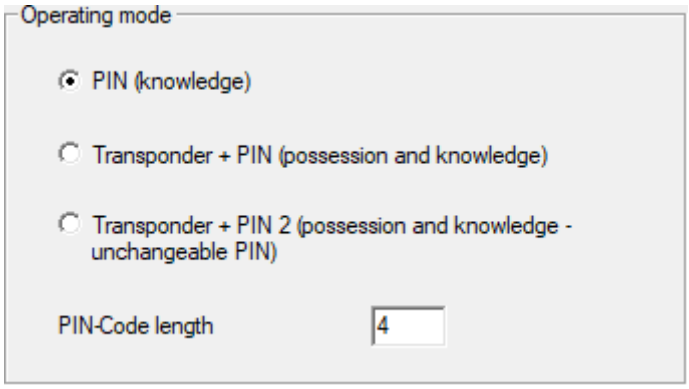


The mode is set once in LSM during commissioning and applies to all PIN code terminals (see also *Mode overview [▸ 20]*).

✓ LSM open.

1. Open the properties of your locking system using | Edit | - Locking system properties.
2. Change to the [PIN-Code Terminal] tab.

3. In the area "Operating mode" select the mode.



4. Click on the Apply button.

↳ Mode.

NOTE

Subsequent change of mode

The mode applies to the entire locking system. If it is subsequently changed, there is considerable effort involved (programming requirement at all PIN code terminals in the system, issuing new User PINs, issuing new transponders, etc.).

1. Carefully plan beforehand which mode you want to use.
2. Do not change the mode after programming the first PIN code terminal in the locking system.

6.6 Preparing locking devices in LSM

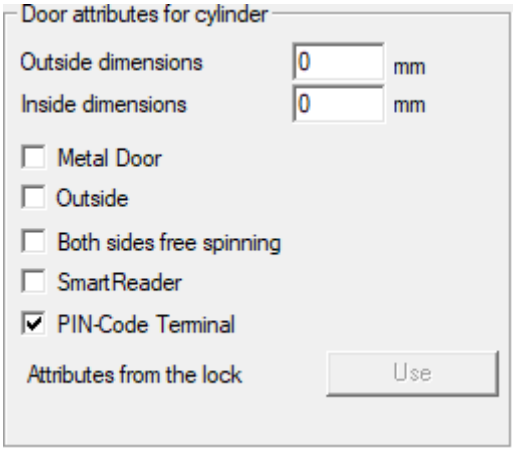
The PIN code terminal is assigned to a SimonsVoss locking device and can only open this device for security reasons. To do so, you must configure the locking device for use with a PIN code terminal:

✓ LSM open.

✓ Locking device to be assigned has already been created.

1. Select your locking device to be assigned.
2. Open the properties of your locking device using | Edit | - Lock properties (alternative: Double click).
3. Change to the "[Door]" tab.

4. Activate the checkbox in "Door attributes for cylinder" the area ☑ PIN-Code Terminal.



5. Click on the Apply button.

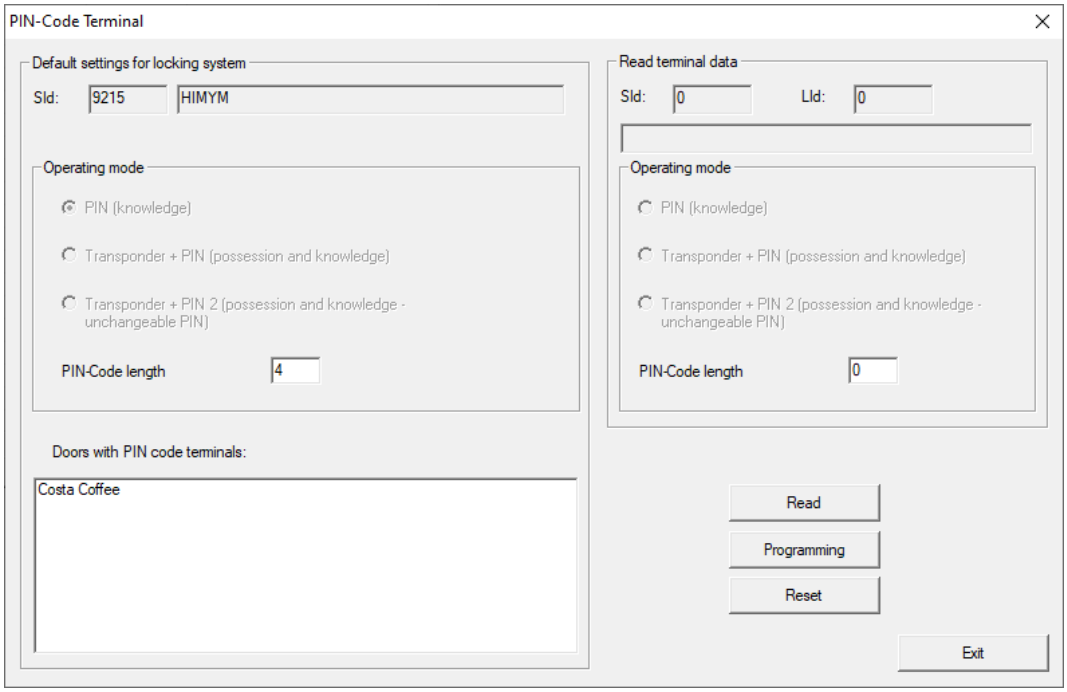
↳ PIN code terminal can be assigned to this locking device.

6.7 Programming the PIN code terminal

You only need to programme the PIN code terminal once with the locking system data.

✓ LSM open.
✓ Programming device (SmartCD.G2) connected.
✓ Length of User PIN the set (see *Determining the PIN length [▸ 13]*).
✓ Mode selected (see *Set mode [▸ 14]*).
✓ Locking device prepared in LSM (see *Preparing locking devices in LSM [▸ 15]*).
✓ If knowledge mode is used: User already created (in stock) and authorized (see *Creating users [▸ 22]*).
✓ If a different mode is used: If necessary, user created and authorised for the locking device.

1. Open the properties of your locking system using | Edit | - Locking system properties.
2. Change to the [PIN-Code Terminal] tab.
3. Click on the Program / Reset button.
   ↳ The window "PIN-Code Terminal" opens.



4. Select your locking device in the area "Doors with PIN code terminals".
5. Align the PIN code terminal and the programming device (distance 10 cm to 20 cm).
6. Click on the Programming button.
7. When prompted, press **1** for more than two seconds.
   ↳ PIN code terminal beeps and flashes green twice.
   ↳ Programming starts.

↳ PIN code terminal is programmed.

6.8 Programme locking device

✓ LSM open.
✓ Programming device (SmartCD.G2) connected.
✓ If knowledge mode is used: User already created (in stock) and authorized (see *Creating users [▸ 22]*).
✓ If a different mode is used: If necessary, user created and authorised for the locking device.

1. Select the locking device to be programmed.
2. Programme the locking device as usual.

↳ The locking device and PIN code terminal form an "intellectual lock" and can be used together.

7. Fastening

Mounting material is included in the scope of delivery. Choose a mounting that is right for you.

Bond (quick and easy)

✓ Surface dry, free of dust and grease.

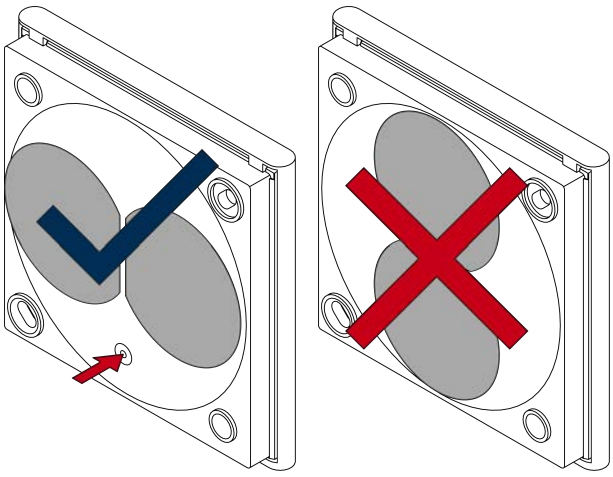
1. Glue the supplied adhesive pad centrally onto the transparent base part.
2. Align the unit without touching the ground.
3. Press the device to mount it.

IMPORTANT

Uneven keypad caused by a covered valve

There is a pressure-equalising valve on the back. If this is covered with adhesive, temperature fluctuations can lead to overpressure or underpressure inside the unit. This can cause the keypad to become uneven.

- Position the adhesive pads so that the pressure-equalising valve remains uncovered.



Screws (secure)

✓ Screwdriver (Torx TX6) present.
✓ If necessary, drilling machine present.

1. Unscrew the screws holding the cover in place.



2. Remove the cover.
3. Position the base plate.
4. Screw or anchor the base plate tightly.
5. Replace the cover.
6. Press the cover against the base plate and screw the cover back in place.



8. Mode overview

The mode is a locking system-wide setting. You can therefore only use one mode per locking system.

	Knowledge	Verification (flexible PIN)	Verification (fixed PIN)
LSM designation	PIN (Wissen)	Transponder + PIN (Besitz und Wissen)	Transponder + PIN 2 (Besitz und Wissen - unveränderlicher PIN)
User remembers	▪ User PIN (user selectable) ▪ Transponder ID (specified by LSM)	▪ User PIN (can be selected by the user)	▪ User PIN (specified by LSM)
User opens with	▪ User PIN ▪ Transponder ID (specified by LSM) as virtual identification medium	▪ User PIN ▪ Physical identification medium (e.g. transponder)	▪ User PIN ▪ Physical identification medium (e.g. transponder)
Opening procedure	1. User enters User PIN. 2. User enters transponder ID (virtual identification medium). 3. Locking device engages when transponder ID and User PIN match.	1. User activates identification medium on the locking device. 2. User enters User PIN. 3. Locking device engages when identification medium and User PIN match.	1. User activates identification medium on the locking device. 2. User enters User PIN. 3. Locking device engages when identification medium and User PIN match.
	LSM generates virtual identification media when users are created in the drop-down menu ▼ **Type** as "G2 PIN code user" (see *Creating users [▸ 22]*).	Lost or stolen transponders are not yet a security risk, as the User PIN must also be known.	

Prerequisites

	Knowledge	Verification (flexible PIN)	Verification (fixed PIN)
Logs in the locking system	▪ G1 ▪ G2 ▪ G2+G1	▪ G2 ▪ G2+G1	▪ G2 ▪ G2+G1
Firmware of the programming device	9.10.4.34 or higher		
Firmware of the locking devices	▪ G1: Firmware independent ▪ G2: 2.3.01 or higher	2.3.05 or higher	2.3.07 or higher

Supported locking devices	▪ G1 locking devices
	▪ G2 locking devices
	  ▪ Active or hybrid
		▪ G2 locking devices
		  ▪ Active or hybrid	

The following products are not supported:

- SmartRelay 3
- AX locking devices
- CompactReader

9. Management

NOTE

Leading zeros for transponder IDs

Some tasks require you to enter a five-digit transponder ID. It may be that transponder IDs may only be displayed in four digits and therefore cannot be entered this way.

- Add leading zeros if necessary (example: Transponder-ID `1230` is entered as `01230`).

Programming aborted due to timeout

The PIN code terminal cancels the entry after five seconds without pressing a button. The entry will then not be accepted or the previous settings will be retained.

1. You can cancel the entry by no longer pressing any keys.
2. In this case, start the input from the beginning.

9.1 Knowledge = PIN (knowledge)

9.1.1 Creating users

Create all users and authorise users to the locking device before programming.

- Create a transponder group to simplify handling.
- Create all users as members of this transponder group.
- Create users even if you don't need them yet. This "stock" saves you programming later. Instead, the authorised users stored in the reserve are simply activated with the initial PIN (see *Unlock user with initial PIN [▸ 23]*).

Creating a transponder group

✓ LSM open.

1. Right-click on Transponder groups.
   ↳ The context menu opens.
2. Select "Update" in the context menu New.

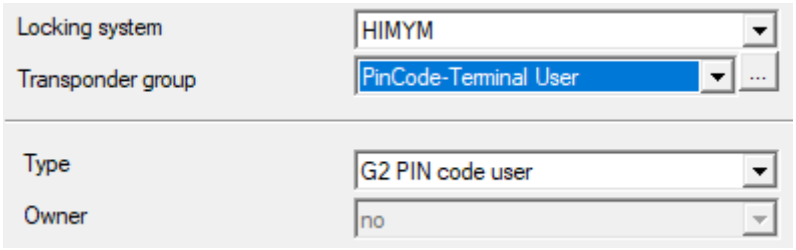


↳ The window for creating a transponder group opens.

3. Create a transponder group with a suitable name, e.g. PIN code terminal user.

Creating users in the transponder group

1. Open the form for new users with the button .
2. Select the transponder group you have created.
3. From the drop-down menu ▼ **Type**, select "G2 PIN code user".



4. Fill in the rest of the form. Leave free fields when you create users on stock.
   ↳ User created in LSM.
5. Authorise the entire transponder group for the locking device.
6. Continue with the programming (see *Programming the PIN code terminal [▸ 16]*).

9.1.2 Unlock user with initial PIN

Provide a message with initial PINs for each user. With this initial PIN, your users activate themselves at the PIN code terminal and select their own User PIN.

- Individual for each user
- Can be used once, then blocked

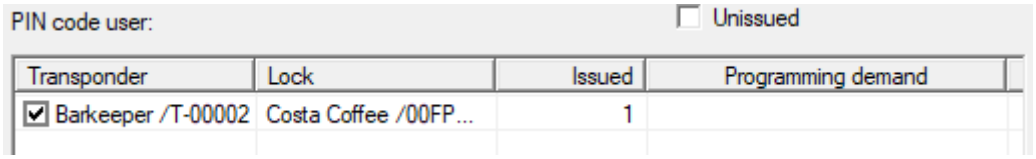
  (Exactly one specific user can unlock themselves with exactly one specific initial PIN at exactly one specific PIN code terminal.)

Issue message with initial PINs

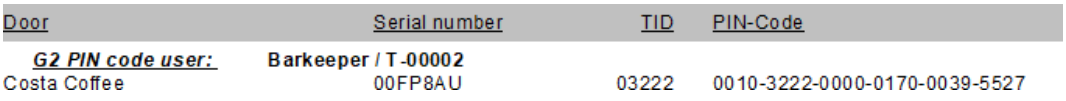
✓ LSM open.
✓ User created (see *Creating users [▸ 22]*).
✓ Locking device created and configured for PIN code terminal (see *Preparing locking devices in LSM [▸ 15]*).

1. Open the properties of your locking system using | Edit | - Locking system properties.
2. Change to the [PIN-Code Terminal] tab.

3. In the section "PIN code user", select all entries of the user whose initial PINs are to be issued in the message.

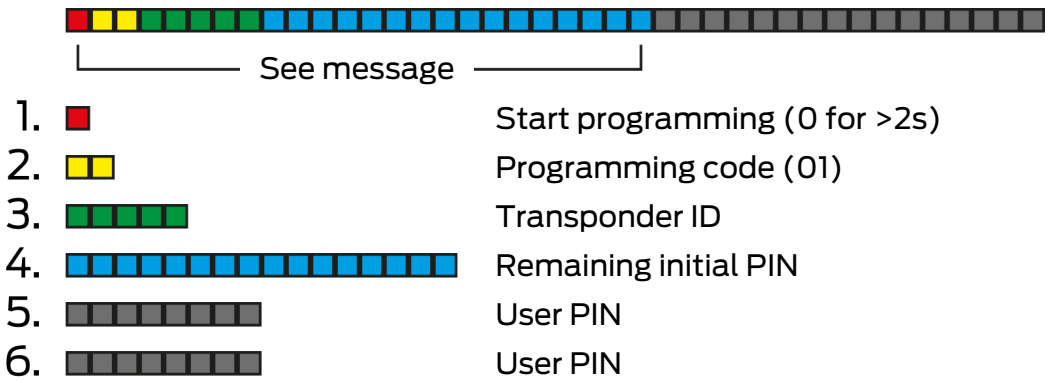


4. Click on the Initial-PINs button.
   ↳ Message with initial PINs is issued.
5. Give the user the message with their initial PINs.



Activating users

Previously created users (see *Creating users [▸ 22]*) are enabled with a numerical code:



The user selects their User PIN themselves. The User PIN must meet the following requirements:

- Length as specified in LSM (see *Determining the PIN length [▸ 13]*)
- No trivial PIN (see *Trivial PIN [▸ 12]*)

The example shows the activation for a User PIN with eight digits. If the length of the is User PIN not eight digits, then the length of the numerical code is different.

✓ Message with matching initial PIN is available.
✓ Master PIN changed (see *Changing the master PIN [▸ 12]*).

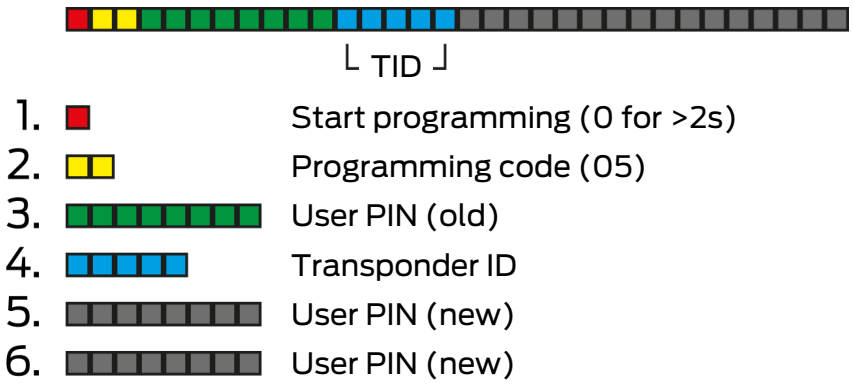
1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter **01**.
3. Enter the transponder ID from the message.
4. Enter the remaining initial PIN from the message.

5. Enter your desired User PIN.
6. Re-enter your desired User PIN.
   ↳ PIN code terminal beeps and flashes green twice.

↳ User PIN is ready for use.

9.1.3 Changing the user PIN

Your users can change the User PINs themselves at the PIN code terminal:



The user selects their User PIN themselves. The User PIN must meet the following requirements:

- Length as specified in LSM (see *Determining the PIN length [▸ 13]*)
- No trivial PIN (see *Trivial PIN [▸ 12]*)

The example shows the change of a user PIN with eight digits. If the length of the user PIN is not eight digits, the length of the numerical code will differ.

✓ Master PIN changed (see *Changing the master PIN [▸ 12]*).

1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter **05**.
3. Enter the old User PIN.
4. Enter the transponder ID.
5. Enter the new User PIN.
6. Re-enter the new User PIN.
   ↳ PIN code terminal beeps and flashes green twice.

↳ User PIN is changed.

9.1.4 Change forgotten user PIN with replacement PIN

In this case, you will return a report with the required replacement PIN. Your users can use this replacement PIN to change the User PIN themselves at the PIN code terminal.

- Individual for each user

- Can be used once, then blocked

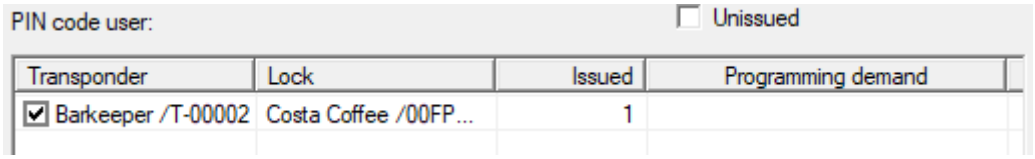
  (Exactly one specific user can change exactly one forgotten User PIN at exactly one particular PIN code terminal with a replacement PIN.)

Issue message with replacement PIN

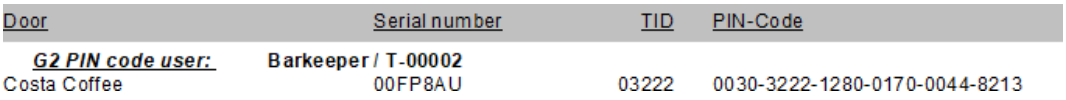
✓ LSM open.

✓ Locking device created and configured for PIN code terminal (see *Preparing locking devices in LSM [▸ 15]*).

1. Open the properties of your locking system using | Edit | - Locking system properties.
2. Change to the [PIN-Code Terminal] tab.
3. In the area, "PIN code user" select the entry of the User PIN (user and door) to be changed.

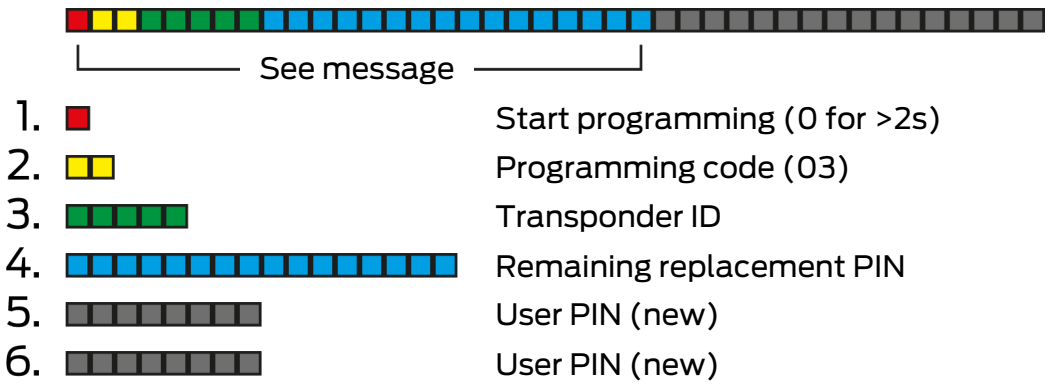


4. Click on the Replacement PINs button.
   ↳ Message with replacement PINs is issued.
5. Give the user the message with their replacement PIN.



change User PIN

Users who have forgotten their User PIN can assign a new User PIN:



The user selects their User PIN themselves. The User PIN must meet the following requirements:

- Length as specified in LSM (see *Determining the PIN length [▸ 13]*)
- No trivial PIN (see *Trivial PIN [▸ 12]*)

The example shows the activation for a User PIN with eight digits. If the length of the User PIN is not eight digits, then the length of the numerical code is different.

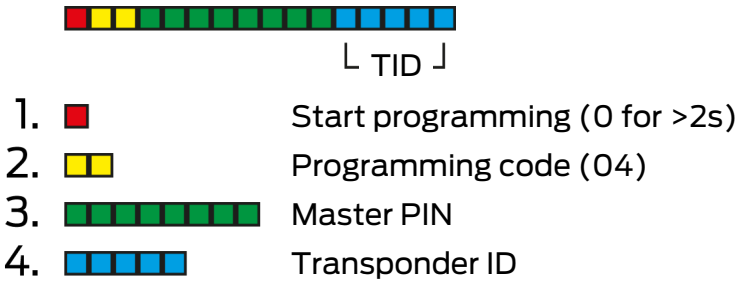
✓ Message with matching replacement PIN is available.

1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter **03**.
3. Enter the transponder ID from the message.
4. Enter the remaining replacement PIN from the message.
5. Enter your desired User PIN.
6. Re-enter your desired User PIN.
   ↳ PIN code terminal beeps and flashes green twice.

↳ User PIN is ready for use.

9.1.5 Delete user

If an employee leaves the company and the user is no longer needed or re-assigned in the PIN code terminal for a longer period of time, you can delete the user (or their transponder ID) from the PIN code terminal:



Deleting a user is the same in all modes. If the transponder ID is not available: You can display the required transponder ID in LSM by double-clicking on the user's entry.

1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter **04**.
3. Enter the transponder ID.
4. Enter the Master PIN.
   ↳ PIN code terminal beeps and flashes green twice.

↳ User (or their transponder ID) is deleted from the PIN code terminal.

9.2 Verification (flexible PIN) = Transponder + PIN (possession and knowledge)

9.2.1 Creating users

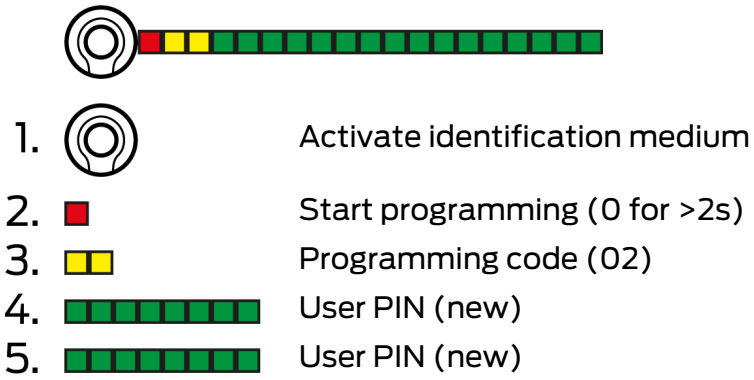
In this mode, you can authorise existing users in LSM or create new users ("G2 Transponder" or "G2 Card").

- ✓ LSM open.
- ✓ User is already created as "G2 Transponder" or "G2 Card".
- ✓ Identification medium already programmed.

1. Authorise all users to the locking device to be used with the PIN code terminal.
2. Then programme the locking device (see *Programme locking device [▸ 17]*).

9.2.2 Activating users with identification media

Users can activate themselves using their identification medium and User PIN on their own.



The user selects their User PIN themselves. The User PIN must meet the following requirements:

- Length as specified in LSM (see *Determining the PIN length [▸ 13]*)
- No trivial PIN (see *Trivial PIN [▸ 12]*)

The example shows the activation for a User PIN with eight digits. If the length of the User PIN is not eight digits, then the length of the numerical code is different.

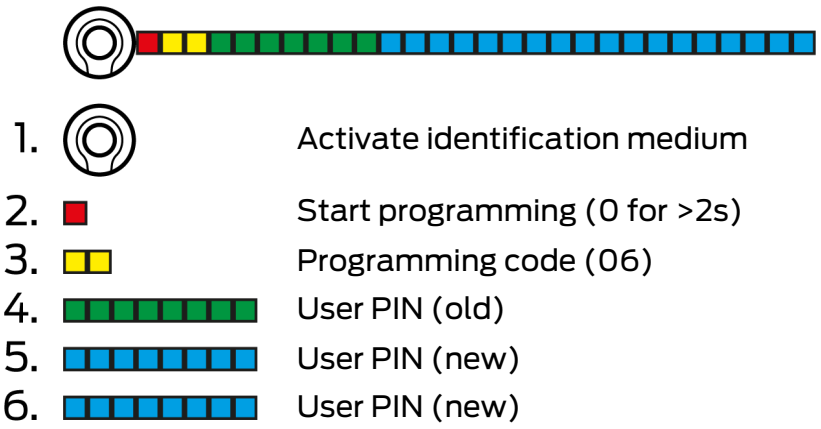
✓ User created and authorised (see *Creating users [▸ 28]*).
✓ PIN code terminal programmed (see *Programming the PIN code terminal [▸ 16]*).
✓ Locking device programmed (see *Programme locking device [▸ 17]*).
✓ Master PIN changed (see *Changing the master PIN [▸ 12]*).

1. Activate the identification medium on the locking device.
   ↳ The locking device does *not* engage, but beeps and flashes for a short time. This is normal in this case.
2. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
3. Enter **02**.
4. Enter the User PIN.
5. Re-enter the User PIN.
   ↳ PIN code terminal beeps and flashes green twice.
   ↳ PIN code terminal performs an opening on the locking device.

↳ If the user has not yet been activated: Data record is saved (beeps and flashes green-orange).
↳ If the user has already been activated: Terminal rejects (beeps and flashes green-orange followed by long red).

9.2.3 Changing the user PIN

Your users can change the User PINs themselves at the PIN code terminal:



The user selects their User PIN themselves. The User PIN must meet the following requirements:

- Length as specified in LSM (see *Determining the PIN length [▸ 13]*)
- No trivial PIN (see *Trivial PIN [▸ 12]*)

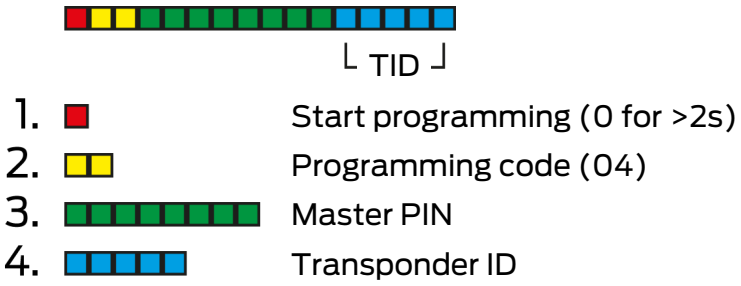
The example shows the change of a user PIN with eight digits. If the length of the user PIN is not eight digits, the length of the numerical code will differ.

1. Activate the identification medium on the locking device.
   ↳ The locking device does *not* engage, but beeps and flashes for a short time. This is normal in this case.
2. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
3. Enter **06**.
4. Enter the old User PIN.
5. Enter the new User PIN.
6. Re-enter the new User PIN.
   ↳ PIN code terminal beeps and flashes red-green.
   ↳ PIN code terminal beeps and flashes green twice.

↳ User PIN is changed.

9.2.4 Change forgotten user PIN

In this case, you reset the user or their transponder ID in the PIN code terminal. Your users can then reactivate themselves (see *Activating users with identification media [▸ 28]*).



1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter **04**.
3. Enter the Master PIN.
4. Enter the transponder ID.
   ↳ PIN code terminal beeps and flashes green twice.

↳ User PIN is reset. Your users can reactivate themselves (see *Activating users with identification media [▸ 28]*).

9.2.5 Delete user

If an employee leaves the company and the user is no longer needed or re-assigned in the PIN code terminal for a longer period of time, you can delete the user (or their transponder ID) from the PIN code terminal:



1. Start programming (0 for >2s)
2. Programming code (04)
3. Master PIN
4. Transponder ID

Deleting a user is the same in all modes. If the transponder ID is not available: You can display the required transponder ID in LSM by double-clicking on the user's entry.

1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter **04**.
3. Enter the transponder ID.
4. Enter the Master PIN.
   ↳ PIN code terminal beeps and flashes green twice.

↳ User (or their transponder ID) is deleted from the PIN code terminal.

9.3 Verification with fixed PIN = Transponder + PIN 2 (possession and knowledge - unchangeable PIN)

9.3.1 Creating users

In this mode, you can authorise existing users in LSM or create new users ("G2 Transponder" or "G2 Card").

✓ LSM open.
✓ User is already created as "G2 Transponder" or "G2 Card".
✓ Identification medium already programmed.

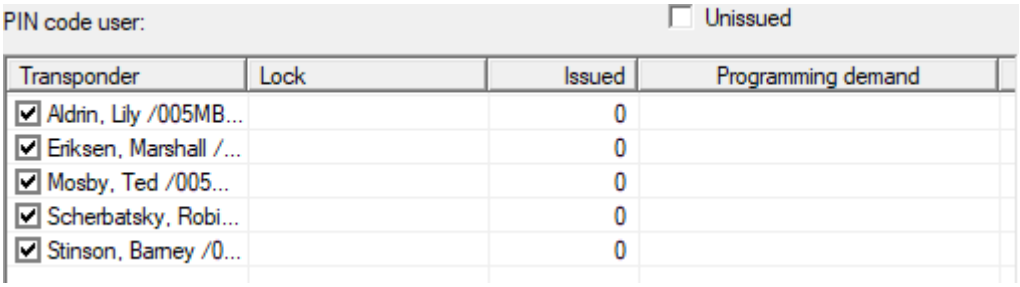
1. Authorise all users to the locking device to be used with the PIN code terminal.
2. Then programme the locking device (see *Programme locking device [▸ 17]*).

9.3.2 Issue user PIN

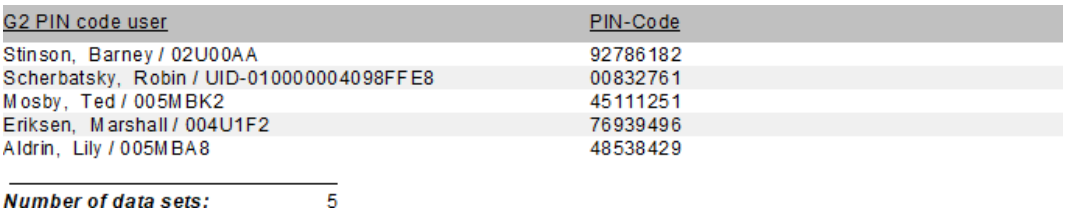
The User PIN is generated by LSM. The user cannot select or change the User PIN himself. Instead, output the User PINs as a message and only make the User PIN available to each user.

✓ LSM open.
✓ PIN code terminal programmed (see *Programming the PIN code terminal [▸ 16]*).
✓ Locking device (see *Programme locking device [▸ 17]*).

1. Open the properties of your locking system using | Edit | - Locking system properties.
2. Change to the [PIN-Code Terminal] tab.
3. In the section "PIN code user" select all users whose User PINs you want to output in the message.



4. Click on the PINs button.
   ↳ Message with User PINs is displayed.



5. Only inform each user of their own User PIN.

↳ Users can use the PIN code terminal with their User PINs.

9.3.3 Changing the user PIN

User PINs cannot be changed in this mode. If another User PIN required, create a new user (see *Creating users [▸ 31]*).

9.3.4 Delete user

If an employee leaves the company and the user is no longer needed or re-assigned in the PIN code terminal for a longer period of time, you can delete the user (or their transponder ID) from the PIN code terminal:



1. Start programming (0 for >2s)
2. Programming code (04)
3. Master PIN
4. Transponder ID

Deleting a user is the same in all modes. If the transponder ID is not available: You can display the required transponder ID in LSM by double-clicking on the user's entry.

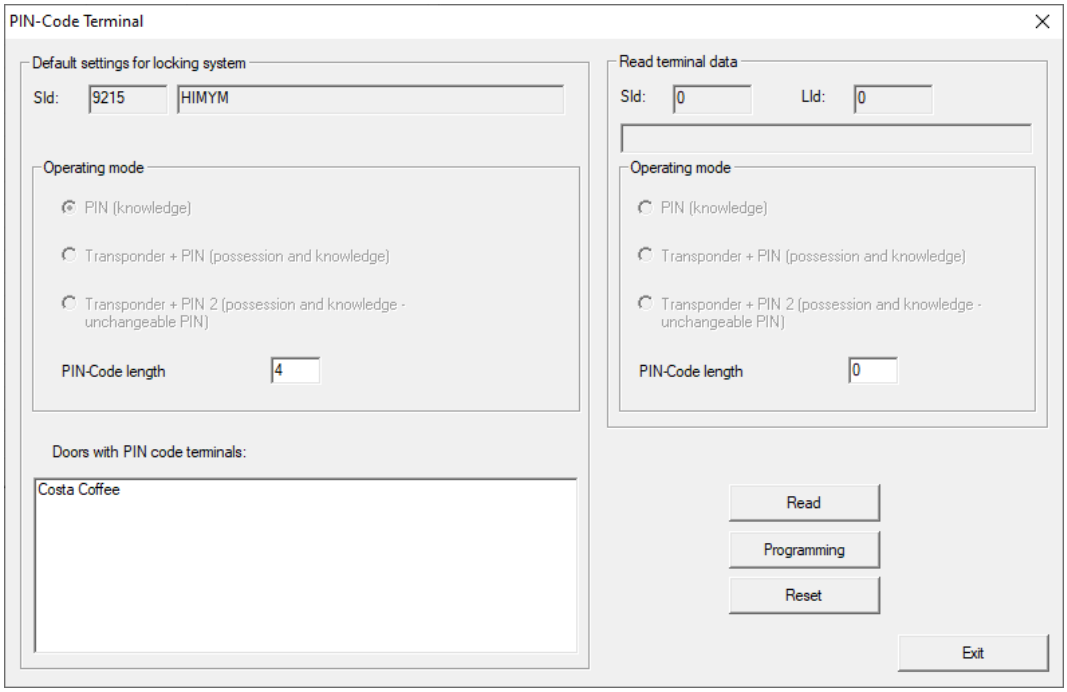
1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter **04**.
3. Enter the transponder ID.
4. Enter the Master PIN.
   ↳ PIN code terminal beeps and flashes green twice.

↳ User (or their transponder ID) is deleted from the PIN code terminal.

9.4 Reading out the PIN code terminal

✓ LSM open.
✓ Programming device (SmartCD.G2) connected.

1. Open the properties of your locking system using | Edit | - Locking system properties.
2. Change to the [PIN-Code Terminal] tab.
3. Click on the Program / Reset button.
   ↳ The window "PIN-Code Terminal" opens.



4. Align the PIN code terminal and the programming device (distance 10 cm to 20 cm).
5. Click on the Read button.
6. When prompted, press **1** for more than two seconds.
   ↳ PIN code terminal beeps and flashes green twice.
   ↳ PIN code terminal is read out.

↳ Read-out data is displayed in the window "PIN-Code Terminal".

10. Opening



NOTE

Programming aborted due to timeout

The PIN code terminal cancels the entry after five seconds without pressing a button. The entry will then not be accepted or the previous settings will be retained.

1. You can cancel the entry by no longer pressing any keys.
2. In this case, start the input from the beginning.

10.1 Knowledge mode



NOTE

Leading zeros for transponder IDs

Some tasks require you to enter a five-digit transponder ID. It may be that transponder IDs may only be displayed in four digits and therefore cannot be entered this way.

- Add leading zeros if necessary (example: Transponder-ID `1230` is entered as `01230`).

1. Enter your User PIN.
2. Enter your transponder ID.
   ↳ PIN code terminal beeps and flashes green twice.

↳ Locking device engages.

10.2 Verification mode

1. Activate your identification medium on the locking device.
2. Enter your User PIN.
   ↳ PIN code terminal beeps and flashes green twice.

↳ Locking device engages.

11. Battery management

11.1 Battery warning levels

Your PIN code terminal warns you of depleted batteries in two stages. Replace the battery.

warning level	Effect
1 (weak)	■ Opening is delayed 5 seconds. ■ During these five seconds, the PIN code terminal beeps and flashes yellow. ■ After the delay, the locking device engages.
2 (very weak)	■ Opening is delayed 10 seconds. ■ During these ten seconds, the PIN code terminal beeps and flashes yellow. ■ After the delay, the locking device engages. Change the batteries now at the latest. Otherwise, the PIN code terminal will fail after a short time.

NOTE

Battery warning disables programming mode

Programming mode cannot be used during an active battery warning. All functions for which programming mode must be entered are blocked.

1. Replace the battery (see *Battery replacement [▸ 36]*).
2. Reset the battery warning.

↳ Programming mode is accessible again.

11.2 Battery replacement

✓ Screwdriver present (Torx TX6).

1. Unscrew the screws holding the cover in place.

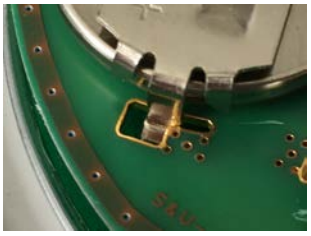


2. Remove the cover.
3. Using a screwdriver, slide one side of the battery clips into the opening provided.

IMPORTANT

Jumping out due to spring tension of clamps

Clamps are under tension. They may jump out and be lost when loosening.



4. Remove the battery.
5. Remove all other batteries in the same way.

NOTE

All batteries are discharged approximately the same. Therefore, replace all batteries at the same time.

6. Insert the new batteries with the positive terminal facing upwards (CR2032 (3V) batteries).
7. Carefully hook the battery clips back into the circuit board.
8. Replace the cover.
9. Press the cover against the base plate and screw the cover back in place.



↳ Batteries are replaced.

Reset battery warning



1.  Start programming (0 for >2s)
2.  Programming code (99)
3.  Input 99999
4.  Master PIN

✓ Batteries are replaced.

1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter **99**.
3. Enter **99999**.
4. Enter the Master PIN.
   ↳ PIN code terminal beeps and flashes green twice.

↳ Battery warning is reset.

12. Protection against systematic testing

Systematic testing of possible PINs is a way for unauthorised persons to find out a valid PIN and possibly misuse it.

Your PIN code terminal is protected against this:

- Tamper protection becomes active after the fifth incorrect PIN entry (User PIN, Master PIN etc.).
- Duration: 60 seconds).
- PinCode terminal beeps and flashes red in the meantime.
- PIN code terminal cannot be operated in the meantime.

Once tamper protection has expired, the PIN code terminal can be operated again.

- A PIN entered incorrectly again immediately reactivates tamper protection.
- A correctly entered PIN resets the tamper protection counter to 0.

13. Double-click simulation (block lock operation on block lock 3066)

You can use the PIN code terminal to activate SimonsVoss activation units (VdS Block Lock 3066). The PIN code terminal must be programmed in knowledge mode.

If the PIN code terminal is within transmission range and a correct User PIN has been entered, the activation unit is activated. The block lock then activates or deactivates the alarm system (see block lock manual).

The VdS-certified SimonsVoss activation units require a double opening protocol for activation/deactivation processes (=double click if a transponder is to be activated or deactivated). The PIN code terminal can simulate this double click and thus perform arming/disarming operations. The double-click simulation is not activated ex works. You can activate and deactivate double-click simulation at any time.

IMPORTANT

Malfunctions due to double-click simulation

The double-click simulation is only intended for operation with a SimonsVoss Block Lock 3066. It can cause malfunctions on other components.

- Activate double-click simulation only if you are using a SimonsVoss Block Lock 3066!



NOTE

Battery warning locks programming

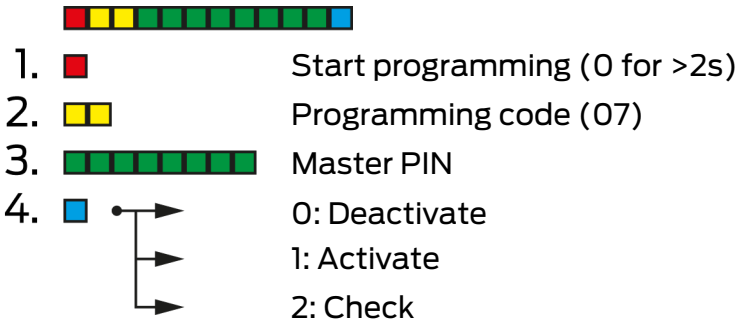
If one of the two battery warning levels is active, the programming cannot be changed.

1. Replace the batteries (see Battery replacement).
2. Change the programming as required.

Programming aborted due to timeout

The PIN code terminal cancels the entry after five seconds without pressing a button. The entry will then not be accepted or the previous settings will be retained.

1. You can cancel the entry by no longer pressing any keys.
2. In this case, start the input from the beginning.



Enable double-click simulation

1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter the Master PIN.
3. Enter **07**.
4. Enter **1**.
   ↳ PIN code terminal beeps and flashes green twice.

↳ Double-click simulation is activated.

Deactivate double-click simulation

1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter the Master PIN.
3. Enter **07**.
4. Enter **0**.
   ↳ PIN code terminal beeps and flashes green twice.

↳ Double-click simulation is disabled.

Check double-click simulation

1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter the Master PIN.
3. Enter **07**.
4. Enter **2**.
   ↳ PIN code terminal beeps and flashes green twice.

↳ If activated: PIN code terminal beeps and flashes green once.

↳ If deactivated: PIN code terminal beeps and flashes orange once.

14. Reset

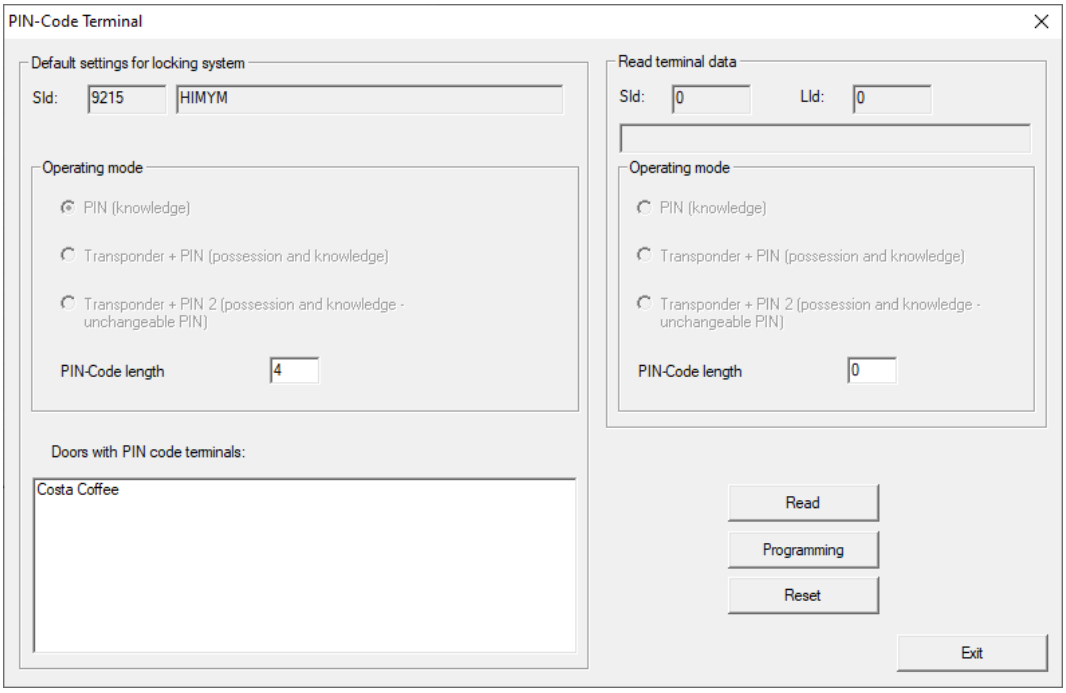
If possible, reset the PIN code terminal with LSM. This prevents deviations between the status of your locking system in LSM and in reality.

14.1 Resetting with LSM

✓ LSM open.

✓ Programming device (SmartCD.G2) connected.

1. Open the properties of your locking system using | Edit | - Locking system properties.
2. Change to the [PIN-Code Terminal] tab.
3. Click on the Program / Reset button.
   ↳ The window "PIN-Code Terminal" opens.



4. Align the PIN code terminal and the programming device (distance 10 cm to 20 cm).
5. Click on the Reset button.
6. Enter the locking system password if necessary.
7. When prompted, press **1** for more than two seconds.
   ↳ PIN code terminal beeps and flashes green twice.
   ↳ PIN code terminal is reset.

↳ PIN code terminal is reset.

14.2 Hardware reset



1. Start programming (0 for >2s)
2. Programming code (10)
3. Master PIN
4. Master PIN

✓ Master PIN changed (see *Changing the master PIN [▸ 12]*).

1. Press **0** for more than two seconds to activate programming mode.
   ↳ PIN code terminal beeps and flashes orange once.
2. Enter **10**.
3. Enter the Master PIN.
4. Re-enter the Master PIN.
   ↳ PIN code terminal beeps and flashes green twice.

↳ PIN code terminal is reset.

15. Overview of all programming codes

You already know the PIN code terminal and are you only looking for the programming code?

This list briefly describes all programming codes. Enter programming mode (press 0 for more than two seconds) and enter the rest.

Knowledge

Code	Function (knowledge)	Entire input
01	*Unlock user with initial PIN [▸ 23]*	0 long + 01 + initial PIN + User PIN (new) + User PIN (new)
03	*Change forgotten user PIN with replacement PIN [▸ 25]*	0 long + 03 + replacement PIN + User PIN (new) + User PIN (new)
04	*Delete user [▸ 27]*	0 long + 04 + Master PIN + transponder ID
05	*Changing the user PIN [▸ 25]*	0 long 05 + User PIN (old) + transponder ID + User PIN (new) + User PIN (new)
07	*Double-click simulation (block lock operation on block lock 3066) [▸ 40]* (Deactivate)	0 long + 07 + Master PIN + 0
07	*Double-click simulation (block lock operation on block lock 3066) [▸ 40]* (Activate)	0 long + 07 + Master PIN + 1
07	*Double-click simulation (block lock operation on block lock 3066) [▸ 40]* (Check)	0 long + 07 + Master PIN + 2
09	*Changing the master PIN [▸ 12]*	0 long + 09 + Master PIN (old) + Master PIN (new) + Master PIN (new)
10	*Hardware reset [▸ 43]*	0 long + 10 + Master PIN + Master PIN
99	*Battery replacement [▸ 36]*	0 long + 99 + 99999 + Master PIN

Verification with flexible PIN

Code	Function (verification with flexible PIN)	Entire input
02	*Activating users with identification media [▸ 28]*	Activate transponder + 0 long + 02 + User PIN (new) + User PIN (new)
04	*Change forgotten user PIN [▸ 30]* or *Delete user [▸ 27]*	0 long + 04 + Master PIN + transponder ID

Code	Function (verification with flexible PIN)	Entire input
06	*Changing the user PIN [▸ 29]*	0 long + 06 + User PIN (old) + User PIN (new) + User PIN (new)
09	*Changing the master PIN [▸ 12]*	0 long + 09 + Master PIN (old) + Master PIN (new) + Master PIN (new)
10	*Hardware reset [▸ 43]*	0 long 10 + Master PIN + Master PIN
99	*Battery replacement [▸ 36]*	0 long + 99 + 99999 + Master PIN

Verification with fixed PIN

Code	Function (verification with fixed PIN)	Entire input
04	*Delete user [▸ 27]*	0 long + 04 + Master PIN + transponder ID
09	*Changing the master PIN [▸ 12]*	0 long + 09 + Master PIN (old) + Master PIN (new) + Master PIN (new)
10	*Hardware reset [▸ 43]*	0 long + 10 + Master PIN + Master PIN
99	*Battery replacement [▸ 36]*	0 long + 99 + 99999 + Master PIN

16. Signalling

Signal	Description	Duration
key confirmation signal	Beep and flash green.	Split seconds
OK	Beep and flash green twice.	1 second
Wrong locking device or locking device not reached	Beeps and flashes green once and then red twice.	Seconds
Error	Beeps low and flashes yellow.	Seconds
Low battery	Beeps low and flashes yellow.	5 seconds
Battery very low	Beeps low and flashes yellow.	10 seconds
Protection against tampering	Beeps low and flashes red.	60 seconds

17. Technical specifications

Dimensions	96 mm × 96 mm × 14 mm
Operating temperature	-20 °C to +50 °C
Protection rating	IP 65
Battery type	2× CR 2032 (3V) *Always replace all batteries with new, approved, brand-name batteries when changing them!*
Battery life	Up to 100,000 operations or up to 10 years on standby

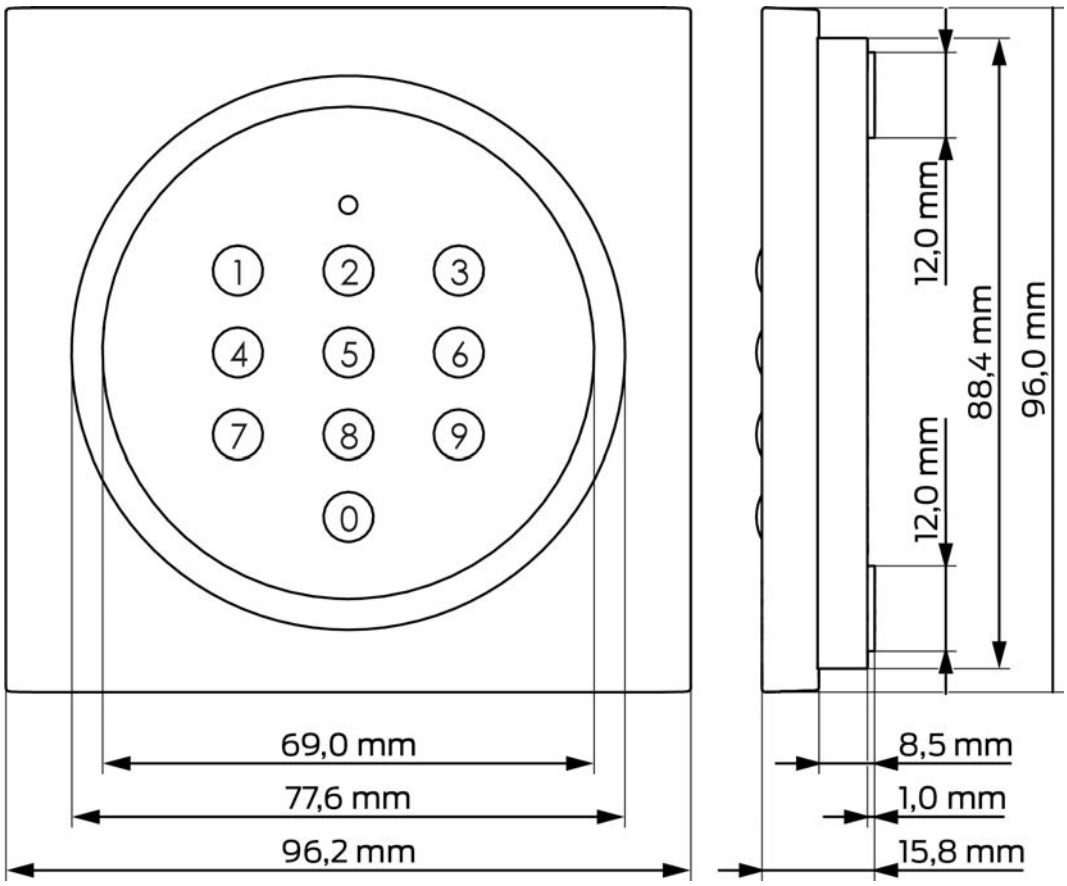
Approved battery manufacturers and further information	Latest information: *www.simons-voss.com/en/resources/information-about-batteries.html*

Distance to cylinder	Max. 20 cm to 40 cm (depending on type)
Distance to Smart-Handle	Max. 40 cm
Distance to SmartRelay	Max. 120 cm
Signal elements	Different colour LEDs (red, green, yellow) + audible signals
Labelling	PHI number (physical hardware identifier)
Colour (housing)	■ Silver-coloured ABS plastic housing, similar to RAL 9007 ■ semi-transparent rear panel/base plate
Colour (button labelling)	Anthracite grey similar to RAL 7016

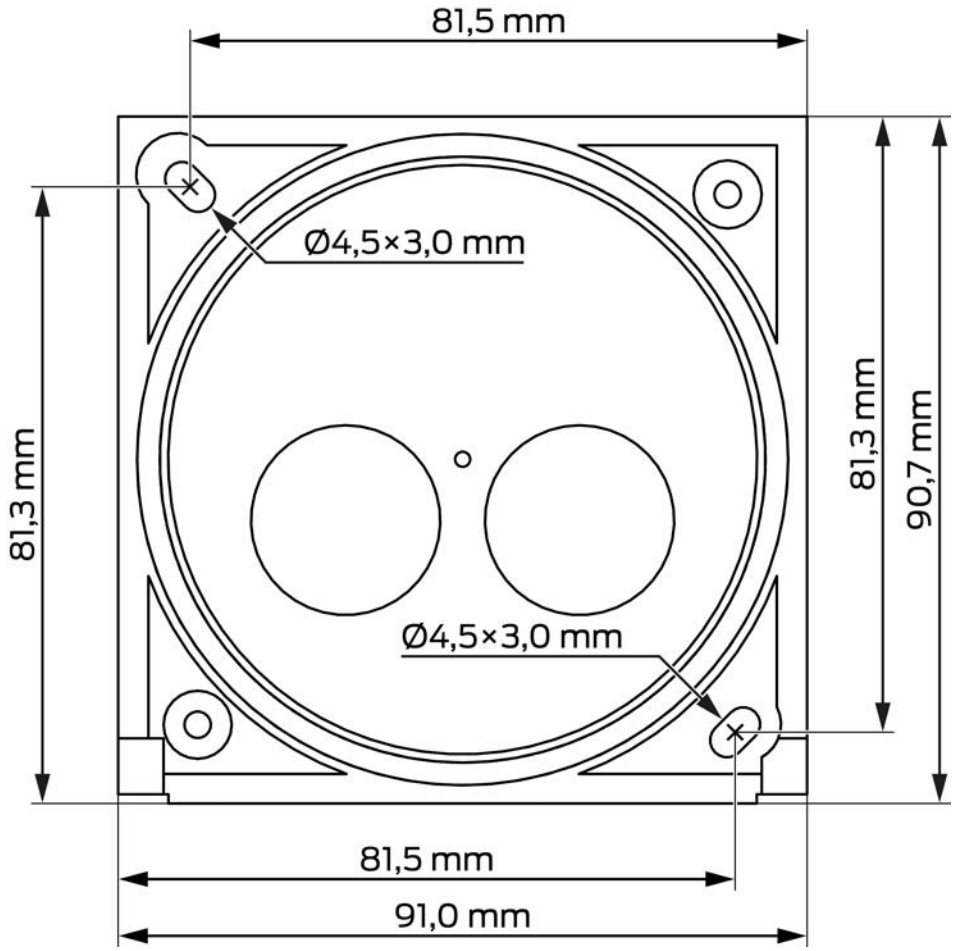
Radio emissions

24.50 kHz - 25.06 kHz	-20 dBµA/m (10 m distance)

17.1 Scale drawing



17.2 Drilling template



18. Declaration of conformity

The company SimonsVoss Technologies GmbH hereby declares that the articles (TRA.PC.TERMINAL) comply with the following guidelines:

- 2014/53/EU -RED-
- 2011/65/EU -RoHS-

CE

The full text of the EU Declaration of conformity is available at the following internet address: *www.simons-voss.com/en/certificates.html*.

19. Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

https://www.simons-voss.com/en/documents.html

Declarations of conformity

You will find declarations of conformity and other certificates on the website:

https://www.simons-voss.com/en/certificates.html

Information on disposal

- Do not dispose the device (TRA.PC.TERMINAL) in the household waste. Dispose of it at a collection point for electronic waste as per European Directive 2012/19/EU.
- Recycle defective or used batteries in line with European Directive 2006/66/EC.
- Observe local regulations on separate disposal of batteries.
- Take the packaging to an environmentally responsible recycling point.



Technical support

Our technical support will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

Email

You may prefer to send us an email.

support-simonsvoss@allegion.com

FAQs

You will find information and help in the FAQ section:

https://faq.simons-voss.com/otrs/public.pl

Address

SimonsVoss Technologies GmbH
Muenchner Str. 16
D-85774 Unterfoehring
Germany



This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide (www.allegion.com).

Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

© 2026, SimonsVoss Technologies GmbH, Unterföhring

All rights are reserved. Text, images and diagrams are protected under copyright law.

The content of this document must not be copied, distributed or modified. More information about this product can be found on the SimonsVoss website. Subject to technical changes.

SimonsVoss and MobileKey are registered brands belonging to SimonsVoss Technologies GmbH.

SimonsVoss technologies

Made in Germany

A BRAND OF ALLEGION