ACCO-KP2

Access control module ACCO

$C\,\epsilon$

USER MANUAL

IMPORTANT

Before you start using the module, please read carefully this manual in order to avoid mistakes that can lead to malfunction or even damage to the equipment.

Changes, modifications or repairs not authorized by the manufacturer shall void your rights under the warranty.

SATEL aims to continually improve the quality of its products, which may result in changes in their technical specifications and software. The current information on the introduced modifications is available on our website.

Please visit us:

https://support.satel.pl

The declaration of conformity may be consulted at www.satel.eu/ce

Factory default code:
Administrator code: 12345

The following symbols may be used in this manual:

i - note,

⚠ - caution.

CONTENTS

1.   Introduction

Thank you for choosing our product. We hope you will be satisfied with your choice. Please remember that we are always ready to provide you with professional assistance and information on our products. Visit our website **www.satel.eu** to find more information about the products offered by SATEL sp. z o.o.

The ACCO-KP2 module is used to control the access to a room, a building or an area. Its job is to control a single door. Only an authorized person will be able to open the door. Devices connected to the module, such as LCD keypads, keypads or readers, are used to identify which person is authorized. The person who is authorized to open the door has the right identifier (card / code). The access can be limited to particular hours on selected days.

In this manual you will find information on how to use the ACCO-KP2 module as a stand-alone device or as a part of the ACCO access control system.

2.   Glossary

Access denied – response to when an unauthorized user attempts to get access (the user has an unknown identifier or is not authorized to get access at the time).

Access granted – permission to open the door after the user is identified and the user rights are verified.

Access schedule – schedule that is assigned to the user and used to define the rules of access to a door. Days and hours during which the user has access to the door are specified in the access schedule.

Access time – time during which you will be able to open the door after you get access.

Alarm – warning of a situation that may compromise the operation of the access control module (e.g. door opened by force, tamper etc.). Action is required to address this situation. The alarm can be signaled in the LCD keypad, keypad or reader.

Anti Passback – function that prevents the user with access from passing back the identifier to other persons so that they can get access. The function prohibits repeated entry or exit by using the same identifier.

Anti-Scanner – function that prevents any attempts to test different code combinations / different cards or Dallas iButtons in order to get access. If 5 attempts are made within 3 minutes to get access by using an unknown identifier, the terminals will be blocked for 5 minutes.

Authorized entry – opening the door by the user when access was granted after using the entry terminal.

Authorized exit – opening the door by the user when access was granted after using the exit terminal.

Code – string of digits used to identify the user.

Dallas iButton – chip inside a metal can shaped like a button. Each Dallas iButton has a unique and fixed code used to identify the user.

Door – general name for a barrier that prevents unrestricted access to a protected area. This can be a hinged door, gate, turnstile, arm barrier etc.

Door blocked – module operating mode in which access to the door cannot be granted (the door is permanently locked).

Door opened by force – opening the door without getting access (when the door is locked).

Door status control – module that supervises the door status by using a sensor connected to the module input. The sensor reports it when the door is opened or closed.

Door unblocked – module operating mode in which access to the door is not controlled and anyone can open it (the door is permanently unlocked).

Door unlocking – response of the module when a user is granted access.

Identifier – card, Dallas iButton, key tag or code used to identify the user.

Input activation – change of the input status to another, different from that defined for the normal status.

Installer – the person who has installed and configured the access control module.

Long open door – it is interpreted by the module that the door is open for too long when the door is open for longer than the "Door open time" limit.

Mantrap / airlock – door that consists of at least two doors. In order to be able to open the next door in the mantrap / airlock, you must first close the previous door. Only one door at a time can be opened in the mantrap / airlock.

Normal door operating mode – module operating mode in which access to the door is controlled. It is the default operating mode of the door.

Proximity card – passive transponder in the form of a card, key tag etc. Each card has a unique and fixed code used to identify the user.

Quit entry / exit – not opening the door after the user is granted access.

Tamper – opening the enclosure of the module, LCD keypad, keypad etc.

Terminal – device used to identify the user, e.g. LCD keypad, keypad, proximity card reader or Dallas iButton reader. Ask the installer about the terminal if you want to find out if it acts as the entry terminal or the exit terminal.

Terminal blocked – terminal does not respond when an identifier is used. This happens when the "Anti-Scanner" function is at work.

Unlock button – button or external device connected to the module input that allows you to open the door without using the user identifier.

User – person registered in the module who gets access by using an identifier.

3. Users

Users can be added in the ACCO-SOFT-LT program.

3.1 User authorization

Identification of the user and verification of the user rights is required for the purpose of access control. The user can be identified based on:

- code,
- proximity card,
- Dallas iButton.

i *Do not make your code available to other people.*

If an unknown identifier is used five times, this can:
- *trigger an alarm,*
- *block the terminal for 5 minutes.*

3.2   Authorization by using two identifiers

The ACCO-KLCDR and ACCO-SCR keypads have a built-in proximity card reader. The installer can configure these devices so that the user must use two identifiers for authorization, both code and card.

3.3 Code

The code is a string of 4 to 12 digits.

i *If you use the code in the ACCO-KLCDR keypad, a message can be displayed asking you to change the code. The message will be displayed every time you use the code, until you change it.*

3.3.1   Factory default code

This code is programmed in the module by default: **12345**. The code is assigned to the "Administrator" user with ID number 00001.

⚠ **The user with ID number 00001 cannot be deleted from the module. The user's "Administrator" and "Change code" rights cannot be revoked either.**

You should change the factory code before you start using the access control module (see: "Changing the code").

3.4 User rights

Administrator – the user can:
– display the module identifier in the LCD keypad,
– clear the alarm memory.

Switching – the user can:
– change the door status to blocked,
– change the door status to unblocked,
– restore the door to normal operation mode.

i *The user can only change the door status by using the terminal when, according to the access schedule, the user has access to that door.*

Change code – the user can change the code by using the ACCO-KLCDR keypad.

4.   Using the ACCO-KLCDR keypad

If the ACCO-KLCDR keypad is connected to the module, the users can use the code or the proximity card.

Fig. 1. ACCO-KLCDR keypad.

4.1 Description of the keypad

4.1.1 LEDs

LED	Color	Description
🔒	yellow	**ON** – door blocked (permanently locked) **flashing slowly** – door blocked (permanently locked) after the "Alarm – block door" type of input is activated
🔓	green	**ON** – door unblocked (permanently unlocked) **flashing slowly** – door unblocked (permanently unlocked) after the "Fire – unblock door" type of input is activated **flashing rapidly** – access to door granted
🔧	green	LED not used
🔔	red	**ON** – alarm **flashing** – alarm memory

4.1.2 Display

The information presented on the display help the user communicate with the module. Date and time are displayed in the upper line. The installer can define the keypad backlight mode and the time format to be shown on the display.

4.1.3 Keys

Use the number keys to enter the code. Use the other keys to:

✳	- open the user menu (after you enter the code), - exit the user menu / function, - quit changing the code.
# / ok	- get access (after you enter the code), - run the function, - confirm new code.
◄	- exit the user menu / function, - move the cursor left when changing the code.
▲	- scroll up the list of functions, - delete digits when changing the code, - confirm that entry / exit is made on duty.
▼	- scroll down the list of functions.
►	- run the function, - move the cursor right when changing the code.

4.1.4 Built-in proximity card reader

The reader supports the Unique 125 kHz proximity cards and key fobs.

4.1.5 Audible signaling

**1 short beep** – access granted and door unlocked.

2 short beeps – door blocked, unblocked or restored to normal mode.

3 short beeps – waiting for the second identifier to be used.

1 long beep – access denied (known card or code). The user cannot unlock the door because:

 − the keypad only grants access based on the code but the card has been used,

 − the keypad only grants access based on the card but the code has been entered.

2 long beeps – access denied (card or code unknown).

3 long beeps [after you present the card / enter the code and press # / ok] – access denied (known card or code). The user cannot unlock the door because:

 − the user is not authorized to unlock the door according to the access schedule,

 − the door is blocked,

 − the user exceeded the defined limit of entries,

 − the user tries again to enter or exit – the "Anti Passback" option is enabled,

 − the module operates in the mantrap / airlock configuration and the other door is open.

3 long beeps [after you hold the card] – impossible to change the door status (block / unblock / restore to normal mode), because the door status is not controlled.

1 very long beep – access denied (the keypad is blocked by the "Anti-Scanner" function).
Long beep lasting 10 seconds – alarm.

4.2   Unlocking the door

The door will unlock when you are granted access. When the door is unlocked, you will be able to open the door. The installer should tell you how much time you have to open the door after access is granted and how much time you have to close the door. The installer should also tell you which of the following procedures to use in order to get access.

i   *If alarm memory is signaled in the keypad (the* 🔔 *LED is flashing), the alarm memory will be cleared as soon as the user with the "Administrator" right is granted access.*

4.2.1   Getting access

Getting access by using the code
1. Enter the code and press $\boxed{\# \; 🔥}$ or $\textcircled{\text{ok}}$.
2. When the 🔓 LED will start flashing, open the door.

Getting access by using the proximity card
1. Present the card on the keypad reader.
2. When the 🔓 LED will start flashing, open the door.

Getting access by using two identifiers
1. Use the first identifier.
2. When the message will be displayed that the keypad is waiting for the second identifier – use the second identifier.
3. When the 🔓 LED will start flashing, open the door.

4.2.2   On duty

After you are granted access, when the message "On duty" is displayed (Fig. 2), you can press ▲ to register the entry / exit as made for official purposes. Ignore the message if your entry / exit is not connected with your official duties.
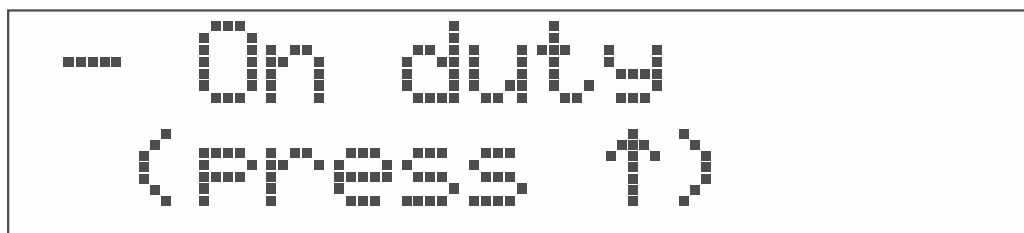
```
    ─ On duty
    (Press ↑)
```

Fig. 2. Message on the possibility to register entry / exit as made for official purposes.

4.2.3   Access denied

The door will remain locked if:
- the identifier is unknown,
- the user cannot get access because:
  - the keypad only grants access based on the card, but the code has been entered,
  - the keypad only grants access based on the code, but the card has been used,

– the user is not authorized to unlock the door according to the access schedule,

– the door is blocked,

– the user exceeded the defined limit of entries,

– the user tries again to enter or exit – the "Anti Passback" option is enabled,

– the module operates in the mantrap / airlock configuration and the other door is open,

– the keypad is blocked by the "Anti-Scanner" function.

4.3 Other functions available when the code is used

4.3.1 User menu

Enter the code and press ✱▢ to get access to the user menu. The list of functions will be displayed. These are the functions that you will be able to run. Which functions are available to you depends on your rights and on the door status.

To scroll through the list, use the ▲ or ▼ key. Point the cursor ✛ to the function you want to run. Press the ▶, # ✋ or ⓞⓚ key to run the function. Below, only the # ✋ key is used to describe how to run a function, however, you can use any of these three keys.

List of functions

Unblock door – use to unblock the door. This function is available to the user with the "Switching" right.

Block door – use to block the door. This function is available to the user with the "Switching" right.

Normal mode – use to switch the door to normal operation mode. This function is available to the user with the "Switching" right.

Change code – use to change your user code. This function is available to the user with the "Change code" right.

Module data: Module ID – use to display the module identifier set in the ACCO-SOFT-LT program. This function is available to the user with the "Administrator" right.

4.3.2 Blocking the door

1. Enter the code and press ✱▢.
2. Use the ▼ or ▲ key to find the "Block door" function.
3. Press # ✋. The door will be blocked. The 🔒 LED will turn ON in the keypad.

4.3.3 Unblocking the door

1. Enter the code and press ✱▢.
2. Use the ▼ or ▲ key to find the "Unblock door" function.
3. Press # ✋. The door will be unblocked. The 🔓 LED will turn ON in the keypad.

4.3.4 Restoring the door to normal operation mode

1. Enter the code and press ✱▢.
2. Use the ▼ or ▲ key to find the "Normal mode" function.
3. Press # ✋. The door will be restored to normal operation mode. The LED will turn OFF.

4.3.5 Changing the code

1. Enter the code and press ✻.
2. Use the ▼ or ▲ key to find the "Change code" function. Press # ♠.
3. Enter the new code.
4. Press # ♠ to save the new code.

4.3.6 Module data

1. Enter the code and press ✻.
2. Use the ▼ or ▲ key to find the "Module data" function.
3. Press # ♠. The "Module ID" function will be displayed.
4. Press # ♠. The module ID will be displayed.
5. Press ✻ to exit the function.

4.4 Other functions available when the proximity card is used

i | *The following functions are available when the door status is controlled.*

4.4.1 Blocking the door

1. If no LED is turned ON (the door operates in the normal mode), make sure that the door is closed.
2. Present the card on the keypad reader and hold for about 3 seconds. The door will be blocked. The 🔒 LED will turn ON in the keypad.

4.4.2 Unblocking the door

1. If no LED is turned ON (the door operates in the normal mode), get access and open the door (see p. 8).
2. Present the card on the keypad reader and hold for about 3 seconds. The door will be unblocked. The 🔓 LED will turn ON in the keypad.

4.4.3 Restoring the door to normal operation mode

If the 🔒 LED (door blocked) or the 🔓 LED (door unblocked) is turned ON, present the card on the keypad reader and hold for about 3 seconds. The door will be restored to normal operation mode. The LED will turn OFF.

5.   Using the ACCO-SCR keypad

If the ACCO-SCR keypad is connected to the module, the users can use the code or the proximity card.

Fig. 3. ACCO-SCR keypad.

5.1 Description of the keypad

5.1.1 LEDs

LED	Color	Description
	yellow	**ON** – door blocked (permanently locked) **flashing slowly** – door blocked (permanently locked) after the "Alarm – block door" type of input is activated
	green	**ON** – door unblocked (permanently unlocked) **flashing slowly** – door unblocked (permanently unlocked) after the "Fire – unblock door" type of input is activated **flashing rapidly** – access to door granted
	red	**ON** – alarm **flashing** – alarm memory

5.1.2 Keys
Use the number keys to enter the code for user authorization. Use the other keys to:

✱	- block the door (after you enter the code), - unblock the door (after you enter the code), - restore the door to normal mode (after you enter the code).
#	- get access (after you enter the code).
🔔	- control the keypad's OC type output (output is active when the key is pressed).

5.1.3 Built-in proximity card reader
The reader supports the Unique 125 kHz proximity cards and key fobs.

5.1.4   Audible signaling

1 short beep – access granted and door unlocked.

2 short beeps – door blocked, unblocked or restored to normal mode.

3 short beeps – waiting for the second identifier to be used.

1 long beep – access denied (known card or code). The user cannot unlock the door because:

– the keypad only grants access based on the code, but the card has been used,

– the keypad only grants access based on the card, but the code has been entered.

2 long beeps – access denied (card or code unknown).

3 long beeps [after you present the card / enter the code and press $#$] – access denied (known card or code). The user cannot unlock the door because:

– the user is not authorized to unlock the door according to the access schedule,

– the door is blocked,

– the user exceeded the defined limit of entries,

– the user tries again to enter or exit – the "Anti Passback" option is enabled,

– the module operates in the mantrap / airlock configuration and the other door is open.

3 long beeps [after you hold the card / enter the code and press $*$] – impossible to change the door status (block / unblock / restore to normal mode), because the door status is not controlled.

1 very long beep – access denied (the keypad is blocked by the "Anti-Scanner" function).

Long beep lasting 10 seconds – alarm.

5.2   Unlocking the door

The door will unlock when you are granted access. When the door is unlocked, you will be able to open the door. The installer should tell you how much time you have to open the door after access is granted and how much time you have to close the door. The installer should also tell you which of the following procedures to use in order to get access.

i | *If alarm memory is signaled in the keypad (the 🔔 LED is flashing), the alarm memory will be cleared as soon as the user with the "Administrator" right is granted access.*

5.2.1   Getting access

Getting access by using the code

1. Enter the code and press $#$.

2. When the 🔓 LED will start flashing, open the door.

Getting access by using the proximity card

1. Present the card on the keypad reader.

2. When the 🔓 LED will start flashing, open the door.

Getting access by using two identifiers

1. Use the first identifier.

2. When 3 short beeps signal that the keypad is waiting for the second identifier – use the second identifier.

3. When the 🔓 LED will start flashing, open the door.

5.2.2   Access denied

The door will remain locked if:

- the identifier is unknown,
- the user cannot get access because:
  - the keypad only grants access based on the card, but the code has been entered,
  - the keypad only grants access based on the code, but the card has been used,
  - the user is not authorized to unlock the door according to the access schedule,
  - the door is blocked,
  - the user exceeded the defined limit of entries,
  - the user tries again to enter or exit – the "Anti Passback" option is enabled,
  - the module operates in the mantrap / airlock configuration and the other door is open,
  - the keypad is blocked by the "Anti-Scanner" function.

5.3 Other functions available when the code is used

i | *The following functions are available when the door status is controlled.*

5.3.1   Blocking the door

1. If no LED is turned ON (the door operates in the normal mode), make sure that the door is closed.
2. Enter the code and press ✳. The door will be blocked. The 🔒 LED will turn ON in the keypad.

5.3.2   Unblocking the door

1. If no LED is turned ON (the door operates in the normal mode), get access and open the door (see p. 12).
2. Enter the code and press ✳. The door will be unblocked. The 🔓 LED will turn ON in the keypad.

5.3.3   Restoring the door to normal operation mode

If the 🔒 LED (door blocked) or the 🔓 LED (door unblocked) is turned ON, enter the code and press ✳. The door will be restored to normal operation mode. The LED will turn OFF.

5.4 Other functions available when the proximity card is used

i | *The following functions are available when the door status is controlled.*

5.4.1   Blocking the door

1. If no LED is turned ON (the door operates in the normal mode), make sure that the door is closed.
2. Present the card on the keypad reader and hold for about 3 seconds. The door will be blocked. The 🔒 LED will turn ON in the keypad.

5.4.2   Unblocking the door

1. If no LED is turned ON (the door operates in the normal mode), get access and open the door (see p. 12).
2. Present the card on the keypad reader and hold for about 3 seconds. The door will be unblocked. The 🔓 LED will turn ON in the keypad.

5.4.3 Restoring the door to normal operation mode

If the 🔒 LED (door blocked) or the 🔓 LED (door unblocked) is turned ON, present the card on the keypad reader and hold for about 3 seconds. The door will be restored to normal operation mode. The LED will turn OFF.

6. Using the proximity card readers

If the CZ-EMM / CZ-EMM2 / CZ-EMM3 / CZ-EMM4 proximity card reader is connected to the module, the users can use the proximity card. The reader supports the Unique 125 kHz proximity cards and key fobs.

6.1 Description of the CZ-EMM and CZ-EMM2 readers

Fig. 4. CZ-EMM and CZ-EMM2 readers.

6.1.1 Bicolor LED

Color	Description
green	**ON** – normal operation of the reader **flashing rapidly** – access to door granted **flashing slowly** – door unblocked (permanently unlocked)
red	**ON** – reader blocked because keypad has been connected **flashing slowly** – door blocked (permanently locked) **ON but periodically dimmed down** – reader blocked by the "Anti-Scanner" function

6.2 Description of the CZ-EMM3 and CZ-EMM4 readers

Fig. 5. CZ-EMM3 and CZ-EMM4 readers.

6.2.1 LEDs

Color	Description
green	**ON** – normal operation of the reader **flashing rapidly** – access to door granted **flashing slowly** – door unblocked (permanently unlocked)
red	**ON** – reader blocked because keypad has been connected **flashing slowly** – door blocked (permanently locked) **ON but periodically dimmed down** – reader blocked by the "Anti-Scanner" function

6.2.2 Bell key

The CZ-EMM4 reader has the 🔔 key. Ask the installer what function is started by the key.

6.3 Audible signaling

1 short beep – access granted and door unlocked.

2 short beeps – door blocked, unblocked or restored to normal mode.

3 short beeps – waiting for the second identifier to be used.

2 long beeps – access denied – card unknown.

3 long beeps [after you present the card] – access denied (known card). The user cannot unlock the door because:

– the user is not authorized to unlock the door according to the access schedule,

– the door is blocked,

– the user exceeded the defined limit of entries,

– the user tries again to enter or exit – the "Anti Passback" option is enabled,

– the module operates in the mantrap / airlock configuration and the other door is open.

3 long beeps [after you hold the card] – impossible to change the door status (block / unblock / restore to normal mode), because the door status is not controlled.

1 very long beep – access denied (the reader is blocked by the "Anti-Scanner" function).

Long beep lasting 10 seconds – alarm.

6.4 Unlocking the door

The door will unlock when you are granted access. When the door is unlocked, you will be able to open the door. The installer should tell you how much time you have to open the door after access is granted and how much time you have to close the door.

6.4.1 Getting access

1. Present the card on the reader.
2. When the LED starts flashing rapidly in green, open the door.

6.4.2 Access denied

The door will remain locked if:

- the identifier is unknown,
- the user cannot get access because:
  - the user is not authorized to unlock the door according to the access schedule,
  - the door is blocked,
  - the user exceeded the defined limit of entries,
  - the user tries again to enter or exit – the "Anti Passback" option is enabled,
  - the module operates in the mantrap / airlock configuration and the other door is open,
  - the reader is blocked by the "Anti-Scanner" function.

6.5 Other functions

i | *The following functions are available when the door status is controlled.*

6.5.1 Blocking the door

1. If the LED is turned OFF (the door operates in the normal mode), make sure that the door is closed.
2. Present the card on the reader and hold for about 3 seconds. The door will be blocked. The red LED in the reader will start flashing slowly.

6.5.2 Unblocking the door

1. If the LED is turned OFF (the door operates in the normal mode), get access and open the door (see p. 16).
2. Present the card on the reader and hold for about 3 seconds. The door will be unblocked. The green LED in the reader will start flashing slowly.
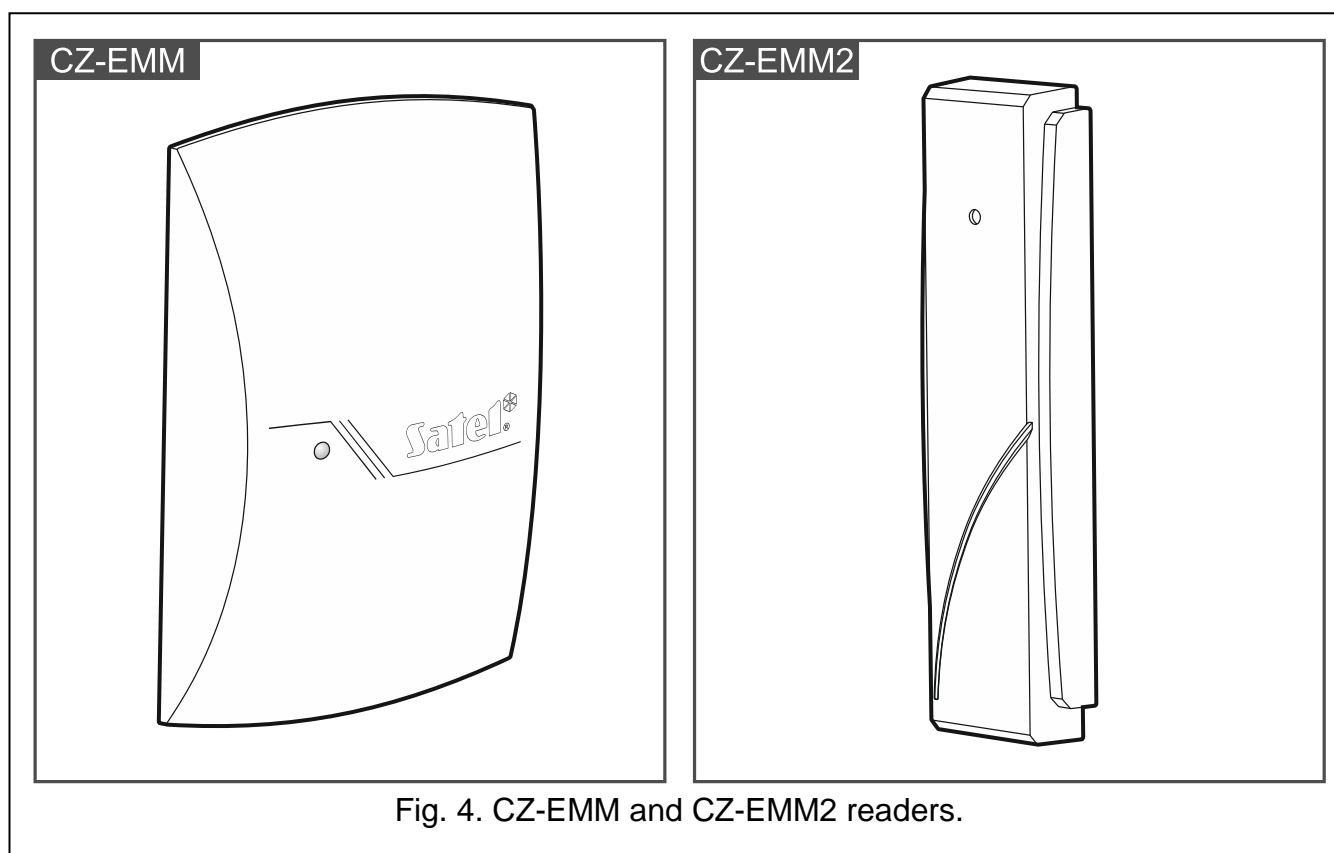
6.5.3 Restoring the door to normal operation mode

If the red LED (door blocked) or the green LED (door unblocked) is flashing slowly, present the card on the reader and hold for about 3 seconds. The door will be restored to normal operation mode. The LED will turn OFF.

7. Using the CZ-DALLAS reader

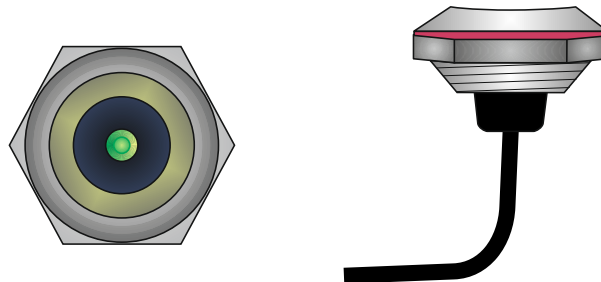If the CZ-DALLAS reader is connected to the module, the users can use the Dallas iButtons.

Fig. 6. CZ-DALLAS reader.

7.1 Description of the CZ-DALLAS reader

7.1.1 Bicolor LED

Color	Description
green	**ON** – normal operation of the reader **flashing rapidly** – access to door granted **flashing slowly** – door unblocked (permanently unlocked)
red	**ON** – reader blocked because keypad has been connected **flashing slowly** – door blocked (permanently locked) **ON but periodically dimmed down** – reader blocked by the "Anti-Scanner" function

7.2 Unlocking the door

The door will unlock when you are granted access. When the door is unlocked, you will be able to open the door. The installer should tell you how much time you have to open the door after access is granted and how much time you have to close the door.

7.2.1 Getting access

1. Tap the iButton on the reader.
2. When the LED starts flashing rapidly in green, open the door.

7.2.2 Access denied

The door will remain locked if:

- the identifier is unknown,
- the user cannot get access because:
    - the user is not authorized to unlock the door according to the access schedule,
    - the door is blocked,
    - the user exceeded the defined limit of entries,

– the user tries again to enter or exit – the "Anti Passback" option is enabled,

– the module operates in the mantrap / airlock configuration and the other door is open,

– the reader is blocked by the "Anti-Scanner" function.

7.3 Other functions

i *The following functions are available when the door status is controlled.*

7.3.1 Blocking the door

1. If the LED is ON in green (the door operates in the normal mode), make sure that the door is closed.
2. Tap the iButton on the reader and hold it for about 3 seconds. The door will be blocked. The LED will start flashing slowly in red.

7.3.2 Unblocking the door

1. If the LED is ON in green (the door operates in the normal mode), get access and open the door (see p. 17).
2. Tap the iButton on the reader and hold it for about 3 seconds. The door will be unblocked. The LED will start flashing slowly in green.

7.3.3 Restoring the door to normal operation mode

If the LED is flashing slowly in red (door blocked) or in green (door unblocked), tap the iButton on the reader and hold for about 3 seconds. The door will switch to normal operation mode. The LED will turn ON in green.

8. Unlock button

The installer can connect to the module a button or a different device (e.g. a detector) intended to unlock the door. In such case, the door is unlocked without the need to identify the user by the module. This solution can be used e.g. for leaving the premises (when the entry to the premises is controlled but the exit is not) or when access is granted by the doorman.

9. Other ways to block the door

The door can also be blocked in one of the following ways:

• after the module input programmed as "Door blocking" is activated (e.g. by using a switch),

• after the module input programmed as "Alarm – block door" is activated (e.g. by using a control panel output),

i *If the door has been blocked by means of the "Alarm – block door" type of input, the door status can only be changed by the user by means of the terminal.*

• automatically, at a specific time (it can be programmed in the module since when and until when the door is to be blocked),

• automatically, according to the access schedule (the schedule defines at what times the door is to be blocked).

10. Other ways to unblock the door

The door can also be unblocked in one of the following ways:

- after the module input programmed as "Door unblocking" is activated (e.g. by using a switch),
- after the module input programmed as "Fire – unblock door" is activated (e.g. by using a fire alarm control panel output etc.),

> *i* *If the door has been unblocked by means of the "Fire – unblock door" type of input, the door status can only be changed by the user by means of the terminal.*

- automatically, at a specific time (it can be programmed in the module since when and until when the door is to be unblocked),
- automatically, according to the access schedule (the schedule defines at what time the door is to be unblocked),
- from the ACCO-SOFT-LT program.

11. Other ways to restore the door to normal operation mode

The door can also be restored to normal operation mode in one of the following ways:

- automatically, at a specific time (when the time has passed during which the door is to be blocked / unblocked),
- automatically, according to the access schedule (when the time has passed during which the door is to be blocked / unblocked according to the schedule),
- from the ACCO-SOFT-LT program.