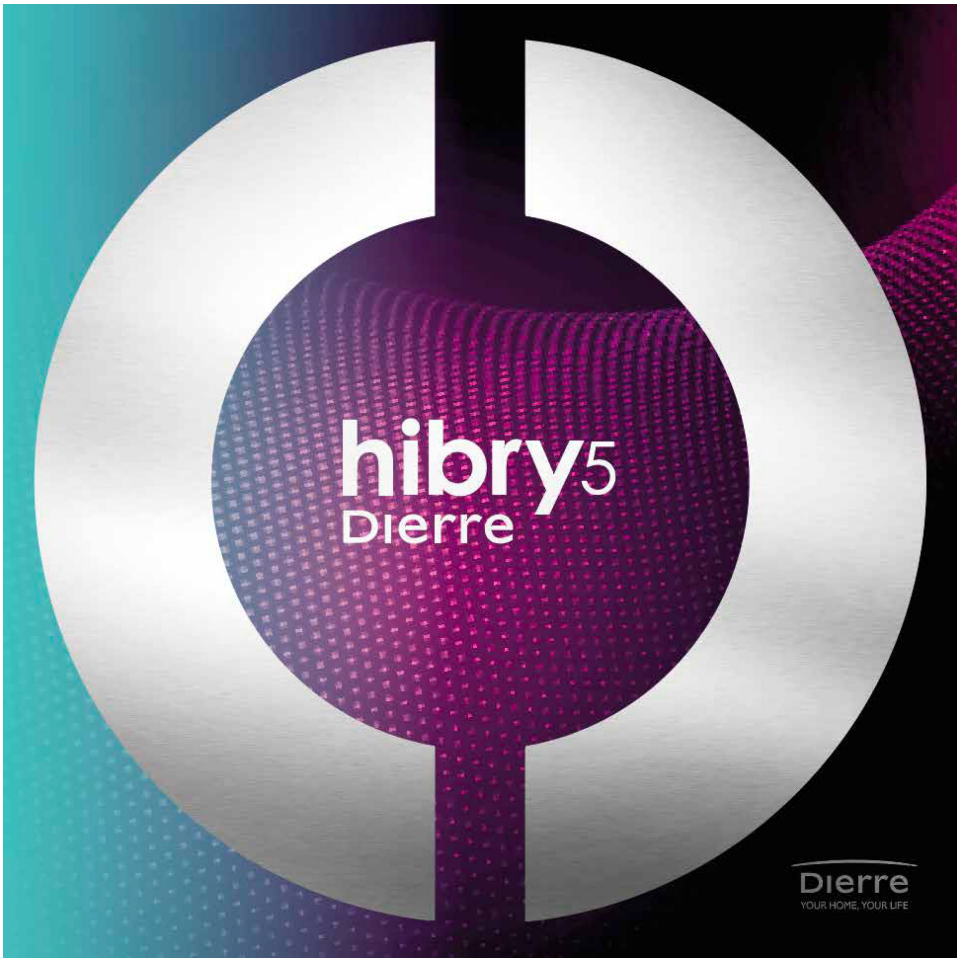
Operation and Maintenance Manual

hibry5

English version 06



Dierre

www.dierre.com

Document Information

Title: Operation and Maintenance Manual – hibry5
Version: 06
Date: 14/04/2026
Author: Dierre S.p.A. / Technical Department

Revision History:

Version	Date [DD/MM/YYYY]	Description
01	18/02/2025	First release
02	01/07/2025	Added section on the rotary selector, updated FAQs
03	01/08/2025	FAQ update and troubleshooting
04	21/10/2025	Added D-igit reader and D-igma numeric keypad
05	10/02/2026	Layout review
06	14/04/2026	Technical data update and LED indication

Contents

1. Premises and References

1.1 Purpose of the manual and relevance for product safety

This manual describes the functions of the hibry5 product for proper use. It includes descriptions of potential issues that may occur during normal use of the product, along with some suggestions for resolving critical situations immediately.

Warning: all installation, configuration, maintenance, and troubleshooting operations on the electronic lock must be carried out exclusively by qualified and authorized personnel. Interventions performed by unqualified personnel may compromise safety, proper system operation, and warranty validity.

1.2 Intended users and definitions of intended use

This manual is primarily intended for installers and users of the hibry5 motorized door by Dierre S.p.A..

1.3 Applicable standards and essential definitions

The product hibry5 is a short-range radio device (Short Range Device – SRD) operating with NFC (Near Field Communication) technology of type MIFARE®, and complies with the essential requirements of the following European Union Directives:

- Directive 2014/53/EU (RED – Radio Equipment)
- Directive 2011/65/EU (RoHS II), as amended by Delegated Directive (EU) 2015/863 (RoHS III)

Compliance with Directive 2014/53/EU (RED)

Compliance with the essential requirements set out in Article 3 of Directive 2014/53/EU is demonstrated by application of the following harmonized standards:

Art. 3.1(a) – Electrical Safety

- EN IEC 62368-1

Art. 3.1(b) – Electromagnetic Compatibility

- ETSI EN 301 489-1 V2.2.3
- ETSI EN 301 489-3 V2.3.2
- EN 55032:2015
- EN 61000-3-2:2019
- EN 61000-3-3:2013+A1:2019
- EN 61000-4-2:2009
- EN 61000-4-3:2006+A1+A2
- EN 61000-4-4:2012
- EN 61000-4-5:2014+A1:2017
- EN 61000-4-6:2014
- EN 61000-4-8:2010
- EN 61000-4-11:2004

Art. 3.2 – Efficient Use of the Radio Spectrum

- ETSI EN 300 330 V2.1.1 (2017-02)

Frequency Bands and Transmitted Power

The integrated NFC radio module operates with the following characteristics:

- Frequency band: 13.56 MHz
- Radio technology: NFC compliant with ISO/IEC 14443 standard (MIFARE®)

EU Declaration of Conformity

Hereby, Dierre S.p.A. declares that the product hibry5 is in compliance with Directive 2014/53/EU.

Compliance with the RoHS Directive

The product complies with Directive 2011/65/EU (RoHS II) and Delegated Directive (EU) 2015/863 (RoHS III) on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

1.4 Typographic conventions

1.4.1 Indications requiring special attention

In this manual, the symbols described below are used.

Icon with blue frame: this symbol is used to draw attention to particularly important information

Icon with yellow frame: situation in which it is recommended to contact an authorized service center

Icon with red frame: potential danger if the instructions are not followed correctly

1.4.2 Languages used in texts and messages in diagrams and images

This manual is written in the language of the country where the product is sold. Some images, for example those showing photographs of the display, are, for simplicity, always presented in Italian. In these cases, reference should be made to the written text in the document and not based solely on the image.

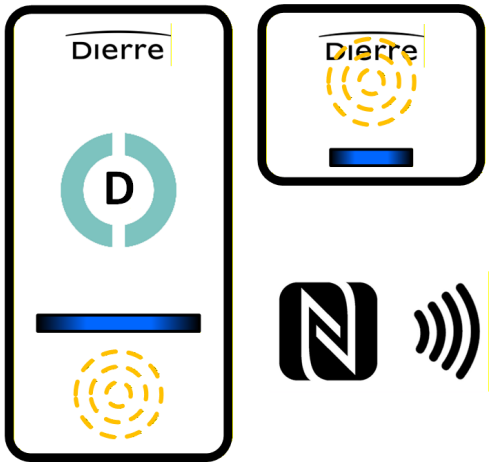
Electrical diagrams, being technical material, are always provided at least with dual nomenclature in Italian and English. In case of doubt, contact the authorized dealer, who can provide support in the desired language.

2. Product Identification

2.1 Description, critical components, and traceability

The term hibry5 refers to an electronic system for motorizing and managing the lock of Dierre S.p.A.armored doors. This system can be combined with different types of armored doors, which will consequently have various mechanical and performance characteristics.

The movement of the bolts and the rods that control the deviators is motorized and managed by an electronic control unit, operated by one or more NFC keys that use high electronic security standards. The latch can only be operated manually via the handle or knob, both on the inside and outside.



The lock is usually equipped with two electronic units / panels visible on the door surfaces: the internal unit includes the NFC reader, a status LED, and an LCD *touch screen* display that allows system configuration. The external unit includes the NFC reader and a status LED.

The electronic keys (EasyKey and Card) leave the factory without being associated with a lock. Therefore, it is necessary to associate them with the door during the system configuration. To maintain high security levels, the association process performs the following two operations:

- authentication data for the electronic key are stored inside the lock
- authentication data for the lock are stored inside the NFC electronic key

The maximum limits are as follows:

- one key can be associated with up to 25 locks
- up to 200 keys can be registered (associated) to a single lock

In case of loss or theft of a key, it is not necessary to replace any lock parts installed in the door. The key can be deleted from the lock memory with simple operations.

The system is powered by a 230 V mains voltage through a 12V AC/DC power supply provided with the door. The presence of only low voltage on the door ensures protection against electric shock.

The door can be opened and closed manually, both from the inside and outside, using a high-security cylinder equipped with specific protections. The cylinder uses EasyKey keys, which contain an NFC transceiver for motorized opening. External information on the door status is available: door open or closed, and if closed, whether it is secured (bolts extended from the lock) or not (bolts retracted into the lock). From both the inside and outside, it is possible to command opening by bringing EasyKey cards close to the relevant panel. The door can operate in automatic or semi-automatic closing mode (details in the following sections). Inside, where a secure environment

is assumed, touching the display allows opening. This function can be disabled and re-enabled through a specific procedure.

2.2 Intended use, operating conditions, and prohibited uses

hibry5 armored doors are designed for domestic residential use. They offer greater convenience compared to traditional doors while maintaining opening control ensured by the mechanical lock.

It is possible to connect a remote opening button to the electronic board mounted on the door frame, in case there is a need to operate the door remotely (e.g., to open it from rooms distant from the door). This command can be enabled or disabled through a specific option in the configuration menu.

*The door must be installed in a location **protected from weather conditions** that could compromise the functionality of the electronic components.*

Any use of the door other than what is explicitly indicated in this manual, including unapproved application areas, is considered prohibited.

3. Safety and Residual Risks

3.1 General Warnings and Reasonably Foreseeable Risks

3.1.1 Behavior in the event of a blackout

The doors in the hibry5 family, unlike other electronic doors by Dierre S.p.A., are not equipped with internal batteries.

As a result, in the event of a power outage, the lock remains usable only mechanically. For this reason, the door is always supplied with mechanical keys, which should be kept in a safe place and can be used in case of blackout.

To mitigate this risk, the user may independently equip themselves with a domestic UPS system.

4. Assembly

4.1 Operating Sequence

The door must be installed on a masonry support in which the appropriate passages for electrical wiring have been prepared. The correct sequence for installing the hibry5 door is as follows:

1. Check that the passages for the wiring needed to supply power to the electronic board located in the door frame, on the lock side, have been properly prepared, as described in the following paragraphs. The same passages can be used for the control signal cables of the lock.
2. Route the necessary cables and place the power supply unit in the external box. **DO NOT CONNECT THE POWER SUPPLY TO THE MAINS**.
3. Install the door structurally, mounting the subframe (if provided), then the frame, and finally the leaf (both leaves in the case of double-leaf doors).
4. Connect the cables to the frame board.
5. Connect the power supply to the mains.
6. Carry out the checks described in chapter 5 and, if successful, proceed with the system configuration for operational use as described in chapter 6.

4.2 Electronic Board Installation (Critical Points)

4.2.1 Preparation for Installation

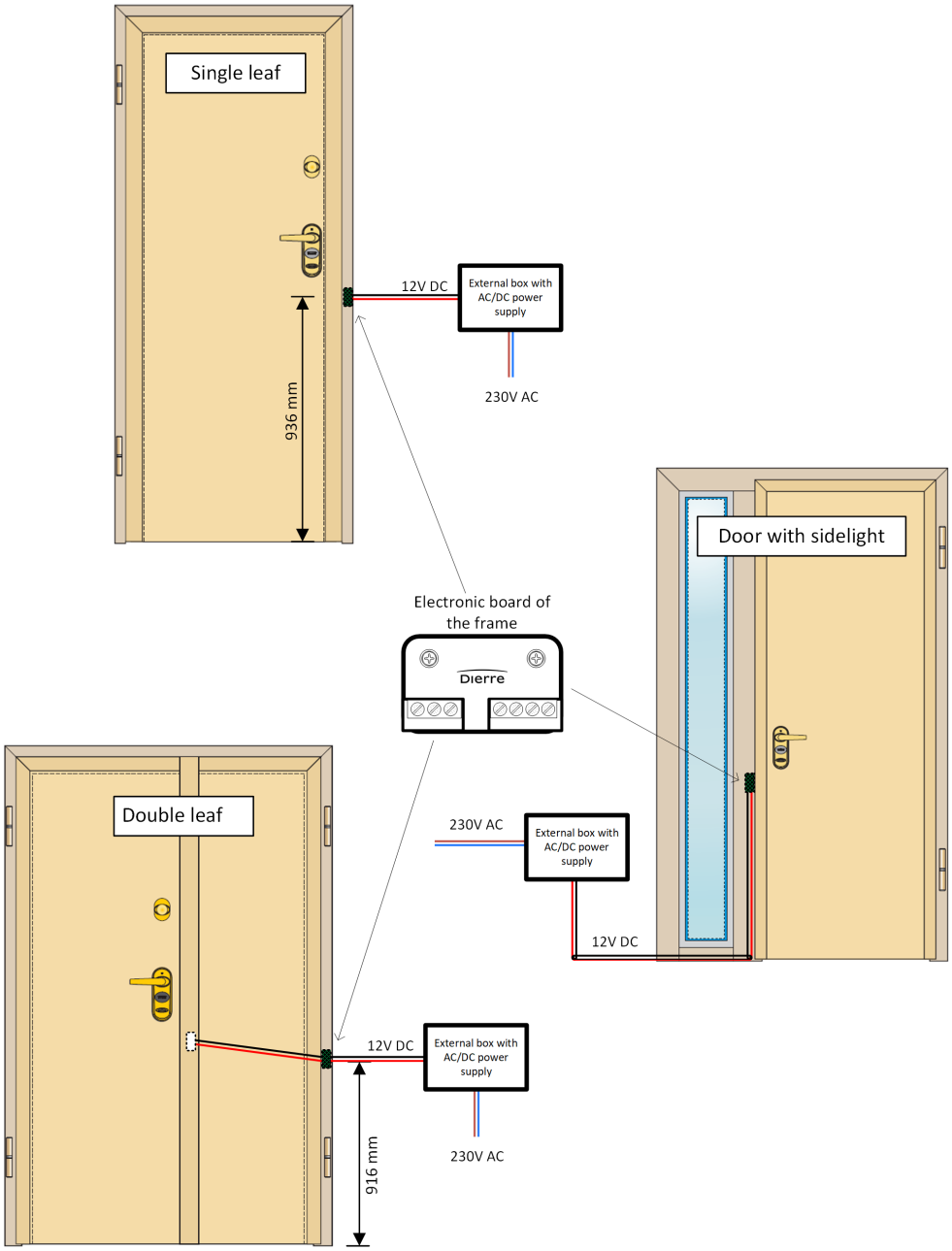
To ensure the safety and correct functioning of the system, the installation must be carried out properly, in accordance with current regulations. It is recommended to entrust the installation to qualified and authorized personnel, possessing the technical-professional requirements set out by Ministerial Decree 37/08.

The installer must follow the following directives:

1. **Compliance with Technical Standards:** All work must comply with industry technical regulations, including those issued by the Italian Electrotechnical Committee (CEI).
2. **Quality Materials:** Use only materials and components that meet recognized safety and quality standards.
3. **Compliance Documentation:** At the end of the work, the installer must issue the Declaration of Conformity, certifying that the system has been built according to current regulations.
4. **Testing and Inspections:** Perform all necessary tests and inspections to ensure the correct operation of the system.

Relying on qualified professionals ensures not only system safety but also compliance with legal provisions, avoiding potential penalties and liability in case of accidents. The preparation of the system for door installation requires the placement of a corrugated conduit to bring the low-voltage power supply wires near the frame, at the height and side of the lock.

For safety reasons, the power supply must not be installed inside the door frame.



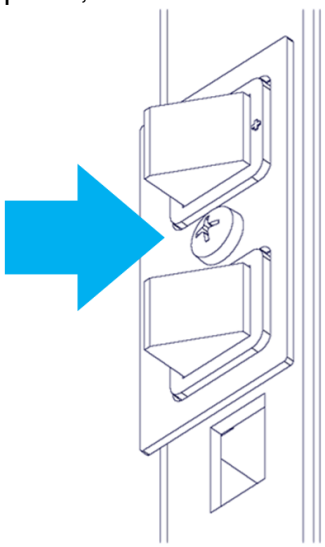
Some examples of wiring and frame board positioning.

First, proceed with the installation of the door and its mechanical alignment via the

cylinder.

For optimal system functionality, the cables connecting the power supply from the door to the transformer must have an adequate cross-section. For distances up to 50 m, use cables with 1 mm^2 cross-section; up to 100 m, use 1.5 mm^2; up to 200 m, use 2 mm^2.

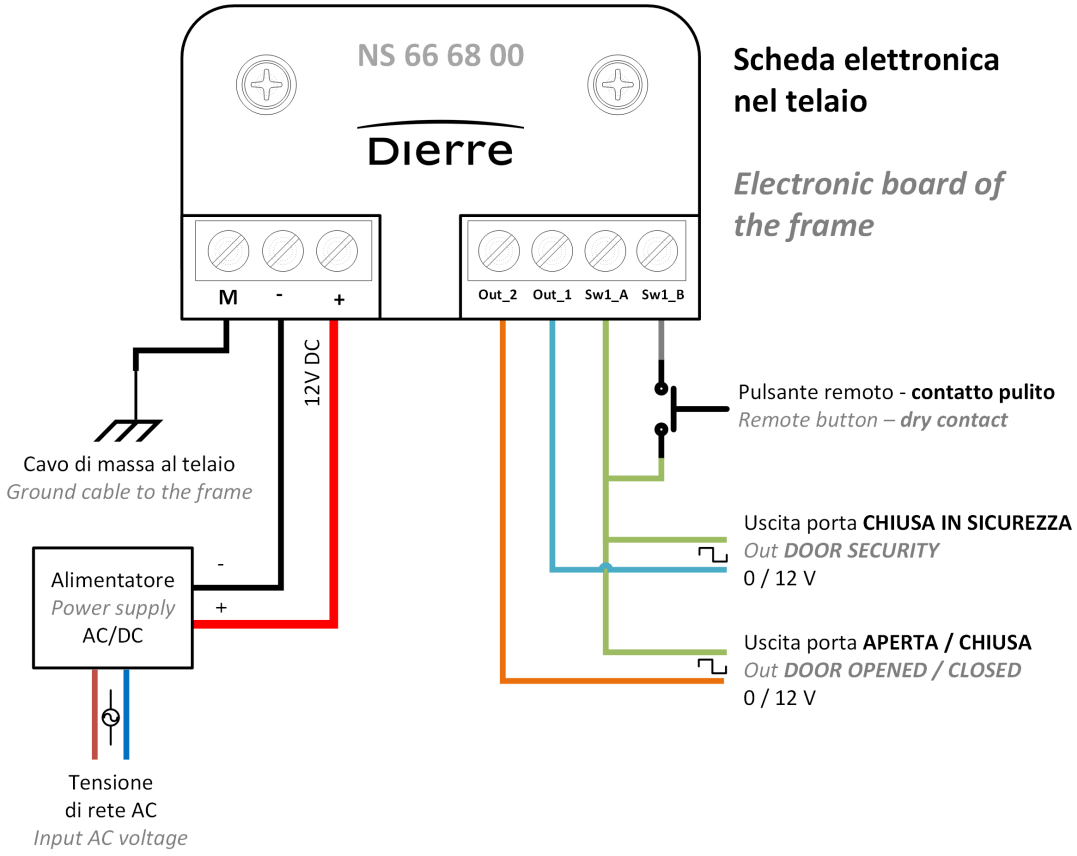
After connecting the wires, install the contact group on the frame by screwing it in place, then close the door.



During manual adjustment, pay attention to the **latch alignment**, because if the latch does not fully extend when the door is closed, the green LED will blink continuously and lock actuation will be disabled. Check that the **door leaf contacts touch the frame contacts**; if not, adjust using the screw located between the two leaf contacts.

4.2.2 Electrical Connections – Frame Board

The power connection always requires the use of 3 wires: positive and negative from the power supply and the ground connected to the frame.



Failure to connect the ground wire to the frame will compromise the door's operation.

Connect the optional remote button. This allows the door to be opened remotely via a clean contact (clean contact definition: contact without any voltage). The opening command through the clean contact can come from any external electronic device: telephone dialer, fingerprint reader, etc.

The frame control board also provides system status output, with the following details:

- indication of door fully closed (deadbolts engaged);
- indication of door open or closed;

via the **Out_1** and **Out_2** outputs respectively.

The status of these outputs changes based on the lock status. The deadbolt status signal changes value instantly, while the door open/closed indication may have a delay of up to 9 seconds.

These outputs are to be considered as status signals and cannot directly drive external electrical loads. For this purpose, an external relay must be used, as described below.

The output voltage of the status signals can be configured, depending on the DIP switch settings, in two modes: driving a “low” voltage of about 0V or a “high” voltage of about 12V.

It is important to remember that the lock has no internal battery. In case of power surges or outages, the status signals may give incorrect values compared to the actual state of the lock.

4.2.3 Output Signal Behavior

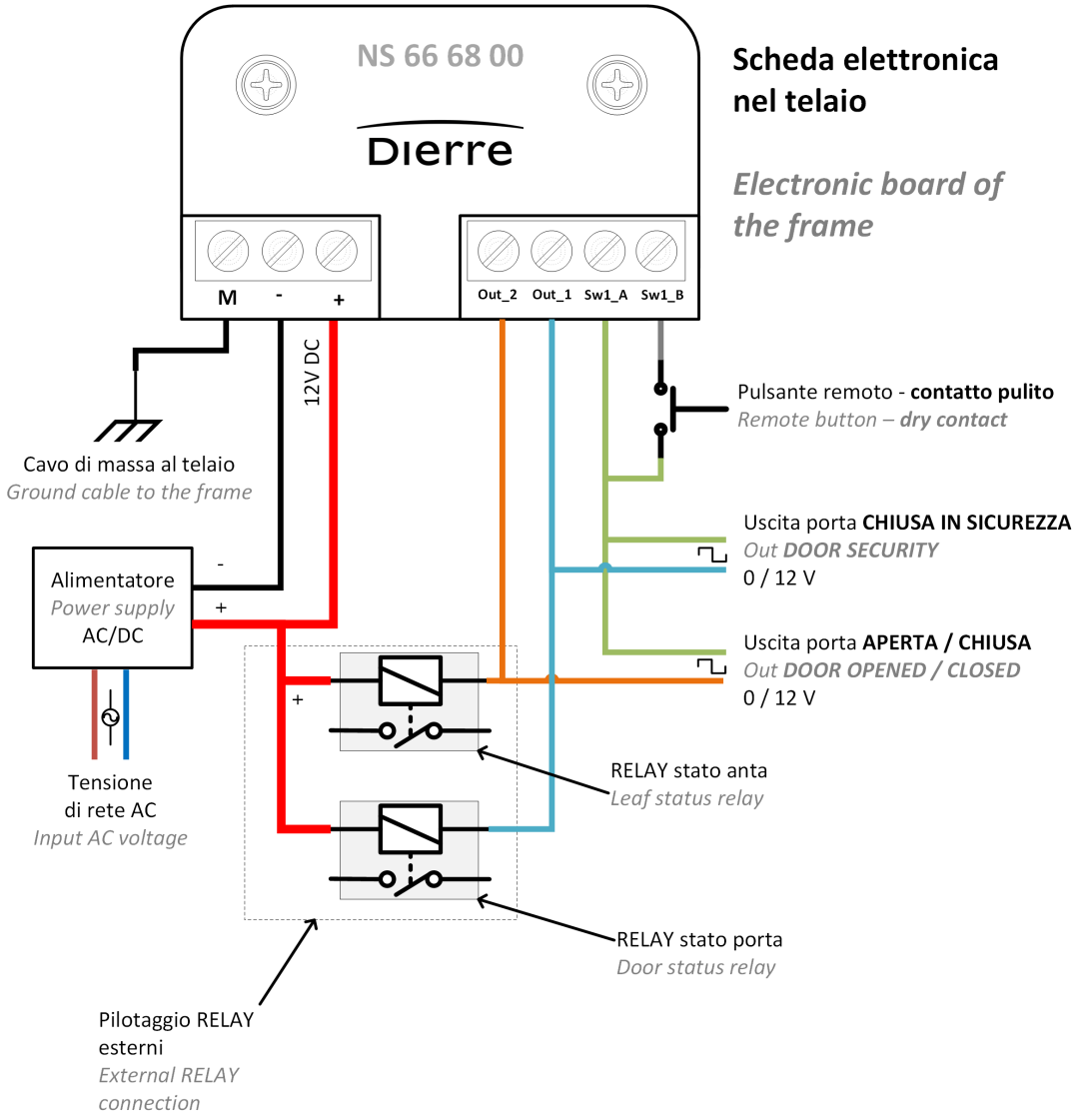
The **Out_1** and **Out_2** signals provide information about the door’s safety status (fully closed) and the door leaf status (open or closed), respectively. These are 12V signals and their polarity (active high or active low) can be set via the lock’s DIP switches.

For more information, refer to the “Use of DIP switches” section.

It is not recommended to use these signals for the control of alarm or anti-theft systems, as they may return false positives in case of power loss.

4.2.4 External Relay Connection

To drive external electrical loads with the status signals, a relay must be connected for each output to be used. In this case, the relay input should be connected between the 12V power supply and the signal that will control the switching.



- coil actuation voltage 12V DC;
- actuation current less than 30 mA.

Use relays that include a flyback diode internally, or add a diode externally.

5. Inspections and Testing

5.1 Pre-Use Checks

After completing all the connections, with the door powered but still unconfigured (factory state), the following checks can be carried out to ensure you can proceed with the next configuration steps.

- ✓ When the door leaf is brought close to the frame, the internal display should turn on with a yellow light and begin functioning. If this does not happen, refer to section 10.1.1.
- ✓ The lock should automatically engage and secure the door. If this does not happen, refer to section 10.1.6.
- ✓ When the door is closed and the yellow light is steady, simply present any electronic key to the reading area of the units to open the door. If this does not happen, refer to section 10.1.4.

5.2 Mandatory Warnings for the User

Carefully follow the operating instructions, and in case of doubts, contact the authorized dealer who supplied the product.

6. Operation

6.1 Initial Start-Up and Configuration

When the door is purchased, the system is in factory state. **In this condition, the door is not secure because any electronic key can open the lock or access the menu: therefore, it is necessary to register the final keys as soon as possible in order to secure the entrance.**

6.1.1 Door in factory state and new NFC TAGs

In this condition, both the door and the NFC TAGs have “empty” internal memory, as shown in Figure 6.1.

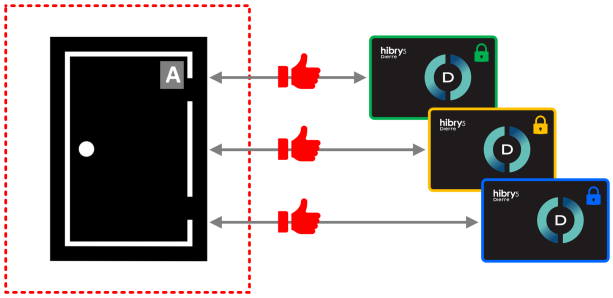


Figure 6.1: All NFC cards open door A because it is not yet configured

Since the system is in factory state, it is possible to open the door and access the menu with any NFC TAG.

6.1.2 Registration of the first master key

With this step, the door switches from factory state to operational state, accepting only the registered key. Cryptographic data is exchanged and saved in both the door and the TAG, as shown in Figure 6.2. To proceed with the registration of the first key, access the USER MANAGEMENT menu →USER LIST. Register the first user and make sure the user type is MASTER. Then proceed with the key insertion via the menu USER MANAGEMENT →USER LIST →USER →KEYS.

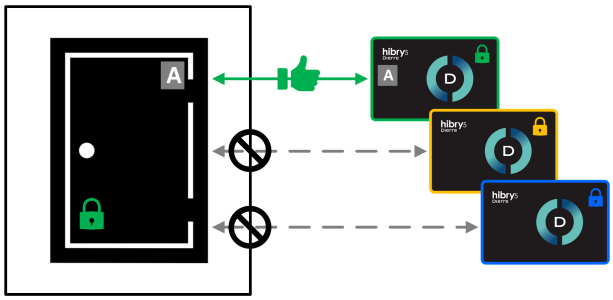


Figure 6.2: Door A saves the NFC card data and the NFC card saves the data of door A

6.1.3 Registration of additional NFC electronic keys

The door can register multiple NFC keys that can be assigned to different users, and a user can have multiple keys assigned, as shown in Figure 6.3. To register additional keys, access the USER MANAGEMENT →USER LIST menu, select the desired user (or create a new one), and proceed with inserting the key via the menu USER MANAGEMENT →USER LIST →USER →KEYS.

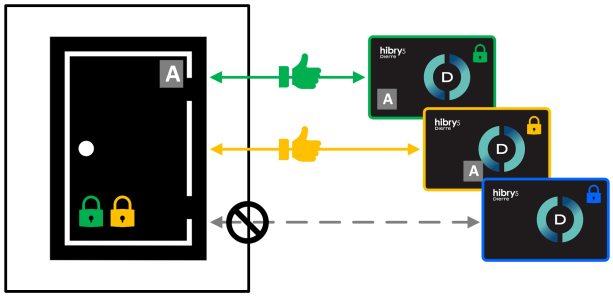


Figure 6.3: Door A also saves the data of the second NFC card

6.1.4 Managing different NFC keys on multiple doors

NFC keys can be registered to multiple doors simultaneously, allowing for the creation of complex access plans, as shown in Figure 6.4.

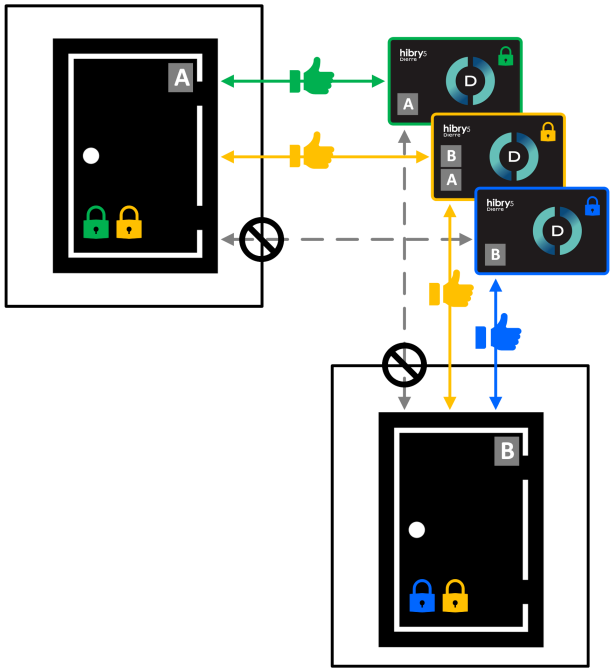


Figure 6.4: The yellow key can open both doors A and B, while the green key only opens door A and the blue key only opens door B

6.2 Normal Operation

6.2.1 Opening and closing modes

Door opening

The door can be opened in the following ways:

- from inside or outside using the NFC keys by bringing them close to the reader areas on the lower part of the escutcheons;
- from the internal display, if enabled, by pressing the unlock button;
- using the clean contact command on the frame board, if enabled.

Only operate the handle when the deadbolts are fully retracted (purple LED on).

It is always possible to open the door with the supplied mechanical key. Insert the key into the cylinder, from the outside or inside, and turn it to perform three full turns. Then push down the handle/knob to open the door.

Door closing

The door can be closed in AUTOMATIC or SEMI-AUTOMATIC mode.

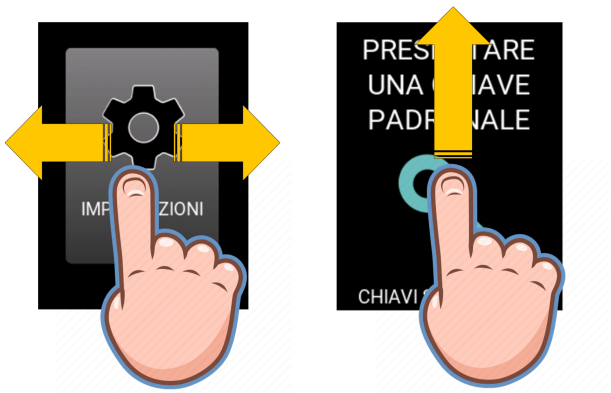
In automatic mode, once the door is closed, the three motorized deadbolts will engage automatically. In semi-automatic mode, closing the door will engage only the latch. To lock the deadbolts:

- bring the NFC key close to the internal or external escutcheon;
- if the function is enabled, tap the display;
- send a command from an external device.

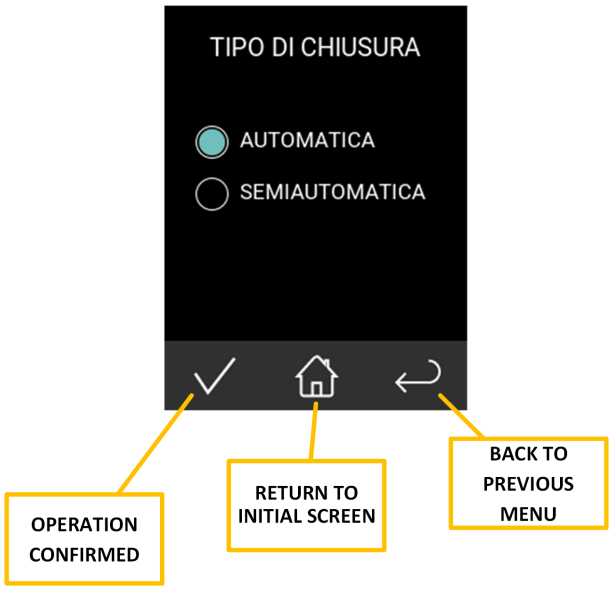
If the system is set to AUTOMATIC mode, the lock will automatically secure after about 30 seconds under any condition.

It is always possible to close the door with the supplied mechanical key.

6.2.2 System configuration menu



Menu navigation is intuitive, and the main screens are accessible with a swipe gesture **(swipe up to exit)**. Once inside a specific function, buttons at the bottom of the screen can be used.



The menu can only be used if the internal display escutcheon is present. If escutcheons are not installed, no keys can be stored, and the only setting available will be between automatic and semi-automatic locking. This setting must be configured using the DIP switches located on the side of the door.

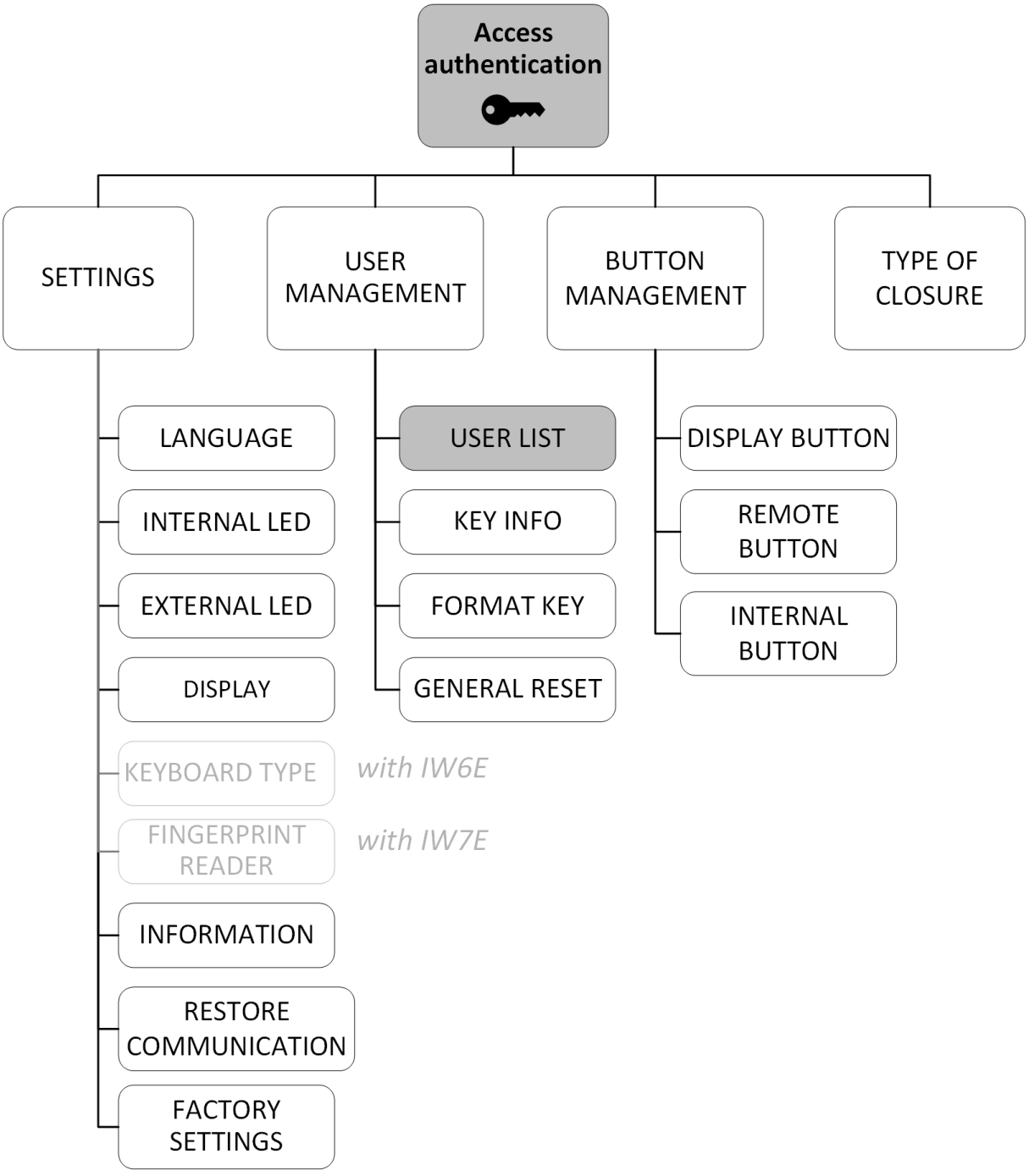


Figure 6.5: The system menu structure

It is possible to access the configuration mode of the door using the internal touch-screen display, with the door closed. During the entire configuration session, the blue LED on both the internal and external escutcheons will blink. If no interaction occurs for more than 3 minutes, the display turns off and the system automatically returns to operational mode.

To enter the configuration menu, press and hold the display until the following message appears:

- “PRESENT A KEY” if the door is in factory state
- “PRESENT A MASTER KEY” if at least one key is already stored

Presenting any key (if door is unconfigured) or a master key (if one exists) grants access to the menu. If the key is recognized, the door enters configuration menu mode. Otherwise, access is denied and a red LED blinks to indicate an error.

By pressing and holding the “SERVICE KEYS” dot for at least 1 second, all service keys can be temporarily disabled (RED dot). To re-enable the service keys, press the dot again to turn it GREEN.

The following sections describe each part of the configuration menu (figure 6.5).

Settings

Language

Allows selection of the menu language from the following options:

- English "UK"
- Italian "IT"
- French "FR"
- German "DE"
- Spanish "ES"
- Portuguese "PT"
- Polish "PL"

Internal LED

Management of the internal LED with the following options:

- Permanent, always on
- Timed, turns off after 1 minute of inactivity
- On with fade effect

Brightness can also be set. To turn off the LED completely, set the brightness to ZERO.

External LED

Management of the external LED with the following options:

- Permanent, always on
- Timed, turns off after 1 minute of inactivity
- On with fade effect

Brightness can also be set. To turn off the LED completely, set the brightness to ZERO.

Display

Backlight brightness adjustment for the display. Increasing brightness may help in brightly lit environments.

Information

This screen shows system version information for each electronic component:

- **VER.D** indicates the internal escutcheon version (Display).
- **VER.S** indicates the lock board version.
- **VER.T** indicates the frame board version.
- **OPENINGS** shows the number of electronic openings performed.
- **CLOSINGS** shows the number of electronic closings performed.
- **ERRORS** shows the number of overcurrent errors, indicating failed opening/closing operations.

The OPENINGS, CLOSINGS, and ERRORS values update after each operation. Additional information displayed may refer to optional accessories, such as the numeric keypad.

Communication reset

This is the reset procedure for restoring communication between the door's electronic boards. It must be carried out whenever one or more of the lock, frame, or display boards are replaced.

To complete successfully, the door must be fully closed with only the latch engaged. For convenience, it's recommended to set the locking mode to SEMI-AUTOMATIC during this procedure.

For further details, see *"Restoring communication between the door's electronic boards"*.

Factory settings

This function restores system configurations to factory defaults, without deleting stored user data.

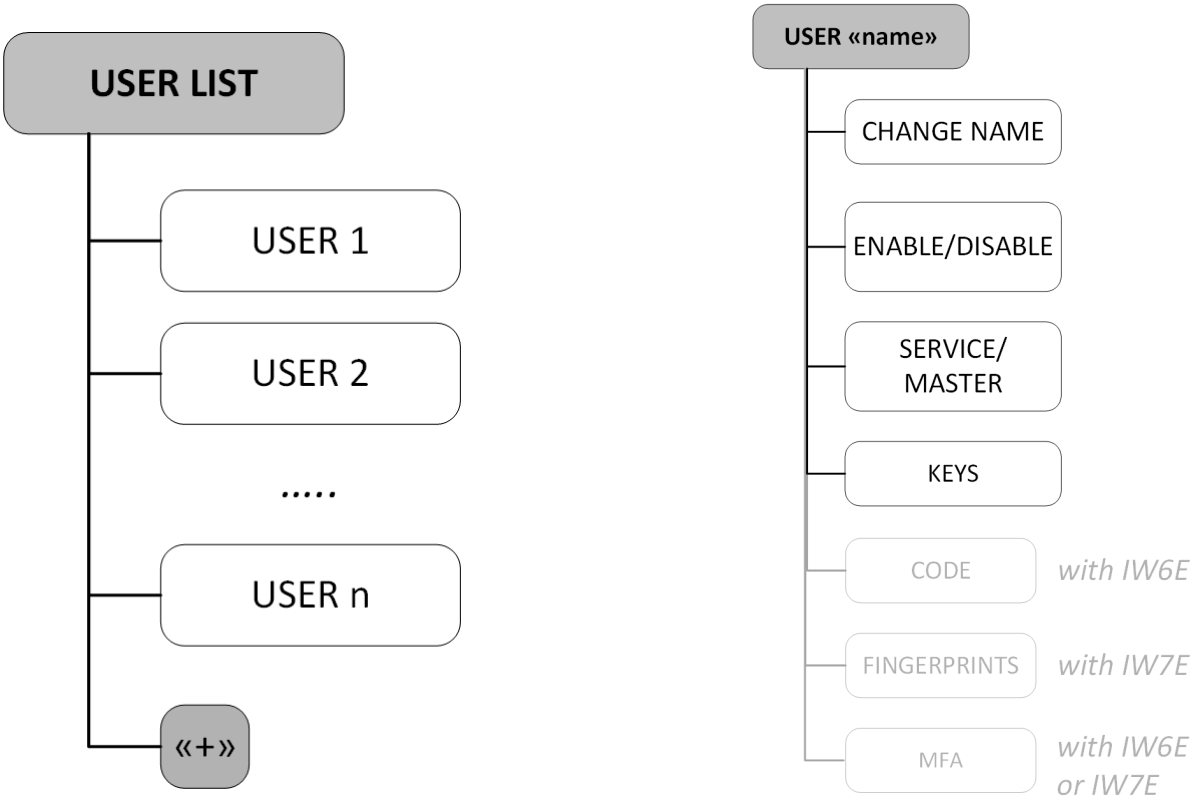
User management

User list

This section allows you to view the list of users and perform management operations.
On the user detail screen, you can:

- Change the name
- Enable or disable the user
- Set the user type as SERVICE or MASTER
- Manage the list of associated NFC electronic keys

*Users with **MASTER** NFC keys can access the system menu, change lock settings, and manage users. Users with **SERVICE** keys can only open and close the door, if enabled by a MASTER user.*



Key info

This screen allows identification of which user an electronic key is associated with. Simply enter this menu and place the key near the reader.

When the key data is displayed, the bottom of the screen shows the number of available slots on the key. These slots are used to associate the key with multiple doors.

Format key

This section allows formatting of any electronic key. All internal data will be erased, and the key will no longer be able to open doors until re-registered.

General reset

This action deletes all users and their associated electronic keys.

Button management

By pressing the BUTTON MANAGEMENT button, you can access the submenu. Three types of buttons are listed: display button, remote button, and internal button.

- The display button allows door opening/closing by tapping the internal escutcheon.
- The remote button allows remote door opening/closing using the clean contact input on the frame board.
- The internal button is used if a fingerprint reader or other on-board accessories are present.

For new (unconfigured) doors, the remote and internal buttons are enabled by default. The display button is disabled. The remote and internal buttons are disabled automatically when a key is stored.

Display button

For the display button, you can choose from 3 options:

- DISABLE means pressing the display does nothing;
- SINGLE CONSENT means pressing the display opens the door;
- DOUBLE CONSENT means pressing the display shows a green circle that must be pressed to confirm. This circle changes position each time.

If you touch the display 4 times outside the circle, the system automatically disables the display button. To re-enable it, access the configuration menu again.

Remote button

Management of the remote (clean contact) button on the frame board.

Internal button

Management of the internal opening button (clean contact) located in the lock. It must be enabled if certain on-board accessories are present (e.g., fingerprint reader or keypad).

Locking type

This screen allows you to set the door locking mode as either AUTOMATIC or SEMI-AUTOMATIC.

6.3 Usage Examples

6.3.1 Deleting an NFC key from the list

To correctly remove a key from the door's key list, it is necessary to present it to the internal escutcheon during the deletion operation. This way, both the door and the NFC key lose the association and memory space is freed on both sides, as shown in figure 6.6.

In the KEY INFO screen, you can check which user a key is associated with. From there, navigate to the key list for that specific user. By presenting the key, the system highlights in green the corresponding row. Now simply press the "trash bin" button to remove the key from the list.

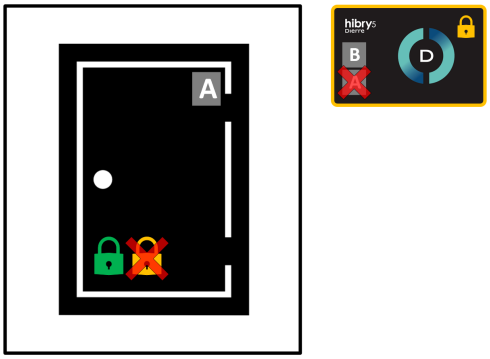


Figure 6.6: Deleting the yellow key from door A's list removes the data from both the door and the key

6.3.2 Deleting a lost NFC key

If the key cannot be presented during the deletion process (e.g., in the case of a lost NFC key), it is still possible to remove it from the list by accessing the system using any other master key. The deleted key will no longer be able to open the door, as shown in figure 6.7.

You can delete the lost key by accessing the internal display menu and going to the key list of the user who lost the key. Then simply press the “trash bin” button to remove the key from the list.

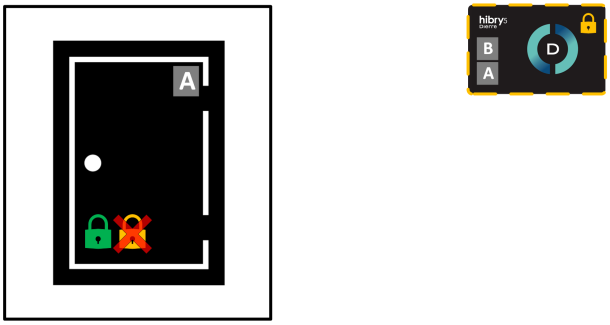


Figure 6.7: If the key is not presented during deletion, its memory space inside the NFC key will not be freed. **This does not pose any security or privacy risk**.

If the only master key in possession is lost, it will no longer be possible to access the configuration menu. A general system reset via DIP switches will then be required.

6.3.3 Clearing the memory of an NFC key

It is possible to format an NFC key, restoring it to a “new key” condition, as shown in figure 6.8.

To perform this operation, go to the USER MANAGEMENT menu →FORMAT KEY.

Figure 6.8: The purple NFC key is formatted: all internal cryptographic data is erased and the key will no longer be able to open any door. The key memory is cleaned and can once again store credentials for access to about 25 doors.

7. Special configurations and optional accessories

The manuals for the optional accessories can be downloaded via the DRcode application.

7.1 Integra fingerprint reader (code FI2E)

The fingerprint access system detects the biometric characteristics of the fingers and opens the door in case of a match.

This device is powered internally by the lock. Before using the device, it is necessary to enable the internal button from the configuration menu or via the DIP switches (depending on the configuration).

If the fingerprint reader is not yet configured, its functionality can be tested as follows: within 10 minutes from powering the system and with the door closed (bolts extended), touch the sensor for at least 3 seconds (no more than 8 seconds) to activate the relay and thus unlock the door.

7.2 D-igit fingerprint reader (code IW7E)

This configuration consists of:

- Internal unit
- External unit with display
- D-igit fingerprint reader

7.2.1 Processing of Biometric Data

Encryption and data storage - the system uses a proprietary algorithm to extract specific features from the finger, converting them into a unique digital code. All data are stored using cryptographic algorithms. It is not possible in any way to reconstruct the original fingerprint image from the stored data.

User rights and regulatory compliance - all fingerprint readers used in Dierre S.p.A.products comply with European data protection regulations. Users have the right to correct or delete their data at any time.

7.2.2 Registering a new fingerprint

To register a new fingerprint, at least one user must already be registered to associate the fingerprint with.

The procedure is as follows:

1. From the internal unit, access the menu by pressing and holding a random point on the display for at least 3 seconds and presenting a master key.
2. Enter the submenu "User management" $\rightarrow$"User list".
3. Select the user to whom you want to associate the new fingerprint.
4. Select "Fingerprints" $\rightarrow$"Fingerprint management".

5. After viewing the message *"For this function you will need to go to the other side of the door. Start the procedure?"*, confirm with the green on-screen button and wait for the lock bolts to retract (if extended).
6. Once the bolts are fully retracted, a new message will appear instructing you to go to the other side of the door. **TAKE A WORKING KEY**, open the door, go outside, and close the door.
7. At this point the procedure continues on the external unit. After viewing the message, touch the display to continue, select left or right hand by swiping horizontally, then select the desired finger by tapping on the dark gray fingertip.
8. Confirm the selected finger by tapping the "+" and wait for the procedure to start.
9. Present the finger to be registered on the reader multiple times following the on-screen instructions.
10. Once the procedure reaches 100%, wait for the message *"Fingerprint saved"* and verify that the fingerprint is recognized.
11. At this point, the registered fingertip will appear light blue instead of dark grey, indicating that a fingerprint has been associated with that finger.
12. To register a second fingerprint, repeat the procedure from step 7. To finish, continue with the following steps.
13. Swipe left or right through the pages used to select the finger and go to the page with the message *"Return to the other side of the door to end the procedure"*.
14. Open the door using the handle and return inside.
15. Close the door and press the "STOP" button on the internal unit to complete the procedure.

Once the fingerprint registration procedure has started, a 3-minute timer will begin. It resets with every touch on the display or fingerprint sensor for security reasons. If there are no interactions within 3 minutes, the procedure will automatically end.

7.2.3 Modifying an existing fingerprint

To modify an existing fingerprint, there must be at least one user with one or more registered fingerprints to overwrite.

The procedure is as follows:

1. From the internal unit, access the menu by pressing and holding a random point on the display for at least 3 seconds and presenting a master key.
2. Enter the submenu "User management" →"User list".
3. Select the user whose fingerprint you want to modify.
4. Select "Fingerprints" →"Fingerprint management".
5. After viewing the message "For this function you will need to go to the other side of the door. Start the procedure?", confirm with the green button on the screen and wait for the bolts to retract (if extended).
6. Once the bolts are fully retracted, a new message will appear instructing you to go to the other side of the door. *TAKE A WORKING KEY*, open the door, go outside, and close the door.
7. The procedure continues on the external unit. After viewing the message, touch the display to continue, select right or left hand by swiping horizontally, then select the finger to modify by tapping the light blue fingertip.
8. Confirm the selected finger by tapping the pencil icon "✎" and wait for the procedure to start.
9. Present the finger to be overwritten on the reader multiple times, following the on-screen instructions.
10. Once the procedure reaches 100%, wait for the "Fingerprint saved" message and verify recognition.
11. The fingertip should remain light blue, indicating the fingerprint is saved.
12. To modify another fingerprint, repeat from step 7. To end the procedure, continue with the following steps.
13. Swipe left or right to reach the page with the message "Return to the other side of the door to end the procedure".
14. Open the door using the handle and return inside.
15. Close the door and press the "STOP" button on the internal unit to complete the procedure.

Once the fingerprint modification procedure has started, a 3-minute timer will begin. It resets with each interaction on the display or fingerprint reader for safety. If there is no activity for 3 minutes, the procedure will automatically terminate.

7.2.4 Removing a single fingerprint

To remove a fingerprint, there must be at least one user with one or more registered fingerprints.

The procedure is as follows:

1. From the internal unit, access the menu by pressing and holding a random point on the display for at least 3 seconds and presenting a master key.
2. Enter the submenu "User management" →"User list".
3. Select the user from whom you want to remove a fingerprint.
4. Select "Fingerprints" →"Fingerprint management".
5. After viewing the message *"For this function you will need to go to the other side of the door. Start the procedure?"*, confirm with the green button and wait for the bolts to retract (if extended).
6. Once the bolts are fully retracted, a new message will appear instructing you to go to the other side of the door. **TAKE A WORKING KEY**, open the door, go outside, and close the door.
7. The procedure continues on the external unit. After viewing the message, touch the display to continue, select right or left hand by swiping horizontally, then select the finger to be removed by tapping the light blue fingertip.
8. Confirm the selected finger by tapping the trash icon "🗑" and confirm deletion using the green on-screen button.
9. The fingertip should now be dark grey again, indicating that no fingerprint is associated with that finger.
10. To remove another fingerprint, repeat from step 7. To complete the procedure, continue with the following steps.
11. Swipe left or right to reach the page with the message "Return to the other side of the door to end the procedure".

12. Open the door using the handle and return inside.
13. Close the door and press the "STOP" button on the internal unit to end the procedure.

Once the fingerprint deletion procedure has started, a 3-minute timer will begin. It resets with each interaction on the display or fingerprint reader for security. If there is no activity for 3 minutes, the procedure will automatically terminate.

7.2.5 Removing all fingerprints of a single user

To remove all fingerprints of a user, there must be at least one user with one or more saved fingerprints.

The procedure is as follows:

1. From the internal unit, access the menu by pressing and holding a random point on the display for at least 3 seconds and presenting a master key.
2. Enter the submenu "User management" →"User list".
3. Select the user whose fingerprints will be removed.
4. Select "Fingerprints" →"Delete all".
5. Confirm deletion using the green on-screen button.
6. Wait for the confirmation message "Fingerprints deleted".

7.2.6 Reader reset – Global fingerprint removal

The fingerprint reader reset serves two purposes.

It can be used to restore communication between the reader and the system in case of first-time installation or replacement of components, or to globally delete all fingerprints in the system, regardless of the user.

To perform this procedure:

1. Access the menu by pressing and holding a random point on the internal display for at least 3 seconds and presenting a master key.
2. Select the submenu "Settings" →"Fingerprint reader".

3. Perform the reset using the on-screen "RESET" button.
4. Confirm the reset using the on-screen confirmation button.
5. Wait for the confirmation message “Completed”.

At this point, information regarding the display should be visible, including version “Ver” and serial number “S/N”. If not, the reset failed and the reader is not communicating correctly with the system.

7.2.7 Multi-factor authentication

Multi-factor authentication (MFA) is a more advanced and secure user recognition method compared to using just the key. With this function enabled, presenting the key to the unit is no longer enough to open the door—at least one more credential will be required depending on the configuration.

The possible combinations are:

- Key + Code **2FA**
- Key + Fingerprint **2FA**
- Code + Fingerprint **2FA**
- Key + Code + Fingerprint **3FA**

This setting is user-specific, allowing for personalized configurations per user.

To enable this function, the user must have at least two types of credentials (key, code, or fingerprint) registered. Follow this procedure:

1. Press and hold a random point on the display for at least 3 seconds and enter the menu with a master key.
2. Select "User management" $\rightarrow$"User list"
3. Choose the user and go to the "Multi-factor authentication" submenu.
4. Use the switch to enable the function.
5. Select the desired combination of credentials from the list below to open the door. Using two credentials enables 2FA, while using all three enables 3FA.
6. Confirm the settings using the check mark on the lower-left corner of the screen.

It can be disabled by repeating the steps and switching the toggle in step 4 to "Disabled".

7.2.8 LED brightness adjustment

It is possible to adjust the LED brightness of the fingerprint reader. The brightness setting follows the same value as the external unit's LED, but not the "animation" effects (timed or fade-in/out).

To adjust the brightness:

1. Press and hold a random point on the display for at least 3 seconds and enter the menu with a master key.
2. Go to "Settings" →"EXTERNAL LED".
3. Adjust the brightness percentage using the slider.
4. Confirm with the check mark at the bottom-left of the screen.

7.3 Numeric keypad (code FI21E)

The keypad access system detects the entered PIN code, compares it with the stored reference codes, and opens the door in case of a match.

7.4 D-igma numeric keypad (code IW6E)

This configuration involves the use of two display panels, one on the inside and the other on the outside.

7.4.1 Adding a new code

In order to assign a new code to a user, the user must already have been added to the system and appear in the user list.

The procedure to add a new code is as follows:

1. From the internal display panel, access the menu by pressing and holding a random point on the display for at least 3 seconds and presenting a master key.
2. Go to the "User Management" →"User List" section.
3. Select the user to whom you want to assign the new code.
4. Select the entry "No code +" and then the "+" icon at the bottom left.
5. Enter the 6-digit code twice to confirm it and wait for the message "Code changed".

7.4.2 Deleting a code

The procedure to remove a code is as follows:

1. From the internal display panel, access the menu by pressing and holding a random point on the display for at least 3 seconds and presenting a master key.

2. Go to the "User Management" →"User List" section.
3. Select the user whose code you want to delete.
4. Select the entry "Code set", then the trash icon "🗑".
5. Confirm the deletion and wait for the message "Code deleted".

7.4.3 Keyboard brightness

It is possible to adjust the brightness of the external display, used as a keypad in this configuration.

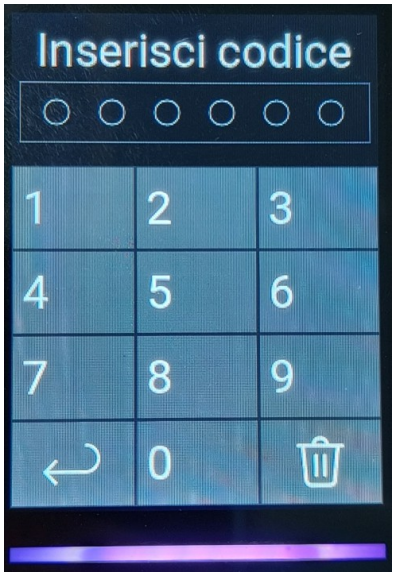
To change this setting:

1. From the internal display panel, access the menu by pressing and holding a random point on the display for at least 3 seconds and presenting a master key.
2. Go to the "Settings" →"Display" section.
3. Set the desired brightness value using the "EXTERNAL" slider and confirm with the checkmark at the bottom left.
4. Open and close the door to apply the change.

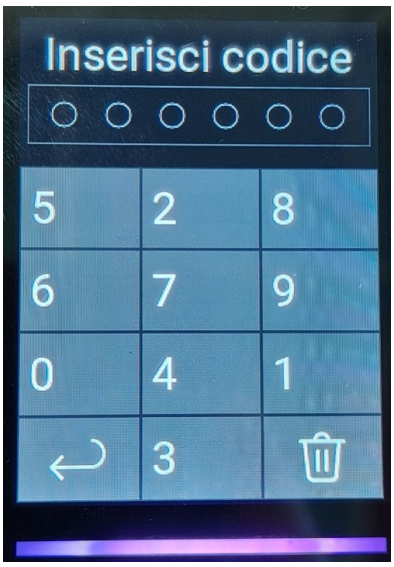
7.4.4 Standard or random keyboard

When using the external numeric keypad, you can choose between two digit layouts: standard or random.

The random layout keypad is designed to use the same numeric code without repeating a fixed sequence, since the keys are arranged in a random order different from the previous entry.



"Standard" layout



"Random" layout

To set the keyboard type:

1. From the internal display panel, access the menu by pressing and holding a random point on the display for at least 3 seconds and presenting a master key.
2. Go to the "Settings" →"Keyboard type" section.
3. Select the desired option and confirm with the checkmark at the bottom left.
4. Open and close the door to apply the change.

7.4.5 Multi-factor authentication

Multi-factor authentication is a more advanced and secure method of user recognition than the key. With this function enabled, presenting the key to the panel will no longer be sufficient to open the door; a code will also be required as a second credential. This setting is specific to each user, so you can configure it individually.

To enable this function, the user must have two types of credentials registered in the system (key and code), and the procedure is as follows:

1. Press and hold a random point on the display for at least 3 seconds and access the menu by presenting a master key.
2. Select the "User Management" →"User List" menu.
3. Choose the desired user and go to the "Multi-factor authentication" submenu.

4. Use the switch to enable the function. The "KEY" and "CODE" credentials will be automatically selected.
5. Confirm the settings using the checkmark on the bottom left of the display.

It can be disabled by repeating the procedure and switching the toggle mentioned in step 4 to the "Disabled" position.

7.5 Removal of the external key reader (code EQ9E)

In this configuration, the external NFC reader is not present.

7.6 Removal of the internal display and external key reader (code GD8E)

In this configuration, the two panels on the door leaf are not installed.
It is therefore possible to open and close the door electrically by operating exclusively on the frame's electronic board.

7.7 Opening via Bluetooth system (code GD9E)

In this configuration, the two panels on the door leaf are not installed, and a Bluetooth interface is integrated into the door leaf. It is therefore possible to open and close the door electrically by operating the frame's electronic board or by using the myDOOR App. This configuration has a dedicated instruction manual.

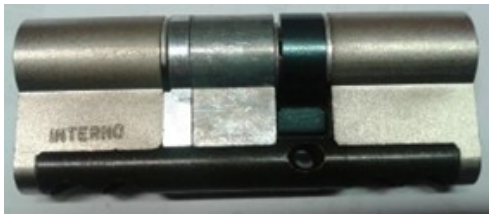
7.8 Operation with "Service Cylinder" kit (code DJ2E)

If electronic keys are used as service keys and no mechanical key is available, in the event of a power outage from the external grid there is a risk of being locked inside the house. To prevent this, Dierre offers the possibility of using a special cylinder, which can be ordered when the door is purchased or later by replacing the cylinder installed on it.

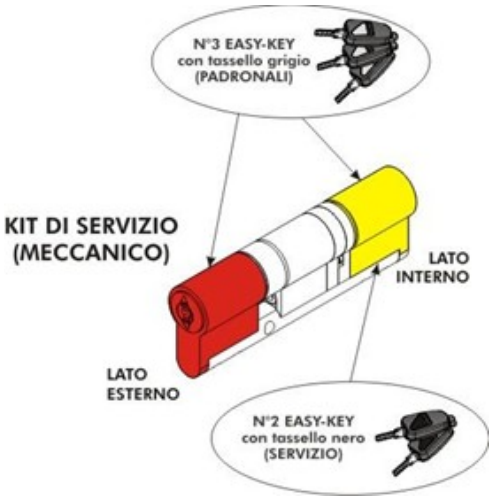
The color of the tab distinguishes the type of key (master or service).

This cylinder comes with:

- 3 easy keys with grey tab and built-in NFC transponder, with master mechanical keying (i.e. they can operate the mechanical opening and/or closing both from inside and outside the door).
- 2 easy keys with black tab and built-in NFC transponder, with service mechanical keying (i.e. they can operate the mechanical opening and/or closing from the inside but not from the outside of the door).



The cylinder indicates the mounting direction on the door (INTERIOR).



It is recommended to register the EasyKey keys with black tab as service keys, so they can be easily and quickly disabled electronically.

8. Error, Fault and Replacement Management

8.1 Basic Diagnostics

8.1.1 LED indications

LED	Colour	Meaning
	**Solid BLUE**	The lock is in the fully secure closed position.
	**Flashing BLUE**	A user is operating in the configuration menu of the internal unit.
	**Solid PURPLE**	The lock is **NOT** in the secure closed position.
	**Flashing PURPLE**	Lock movement malfunction.
	**Flashing GREEN**	Opening or closing operation in progress.
	**Solid RED**	Fault condition, follow the instructions on the display.
	**Solid YELLOW**	Indicates that the system is in **factory state**; the yellow light appears only on the internal unit.

In factory state the door is not secure, because any electronic key, even if not authorised, can open the lock and access the menu.

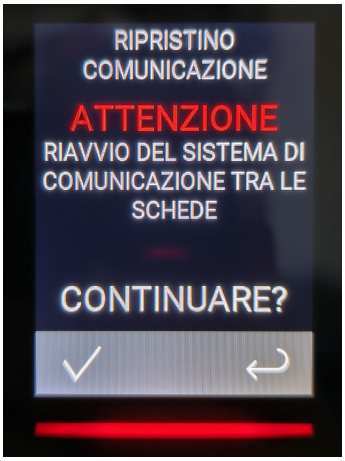
The LED behaviour can be configured from the system menu.

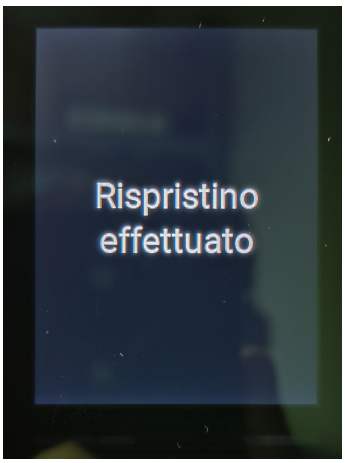
8.1.2 Resetting communication between the electronic boards of the door

Whenever one or more electronic boards of the lock, frame or internal unit must be replaced, a "Communication reset" must be performed.
When this operation is required, the internal unit shows the error message: "COMMUNICATION ERROR WITH THE LOCK".
The reset can be performed by setting DIP switches **1 and 4** to **ON**. When you then close the door, the message "Communication restored" will appear. This screen remains visible until switches 1 and 4 are returned to the desired configuration.

This operation is necessary for correct door operation and can also be performed from the door menu, with the door fully closed against the frame and held only on the latch.

The procedure is as follows:





1. If the door is configured with AUTOMATIC CLOSING, when you push it to the frame it will lock securely. Unlock the lock using the mechanical key, enter the door menu, select "SETTINGS" and then **"RESTORE COMMUNICATION"**. After reading the warning message, confirm with the check mark at the bottom left to start the procedure. The message "WAIT" will appear and then **"Communication restored"**. Open the door and close it again.
2. If the door leaf is already closed in security (bolts extended from the lock), when "RESTORE COMMUNICATION" is selected the message "WAIT" will appear and then **"FAILED"**. Open the door, close it again and repeat the procedure from step 1.
3. If the door is configured with SEMI-AUTOMATIC CLOSING, when you push it to the frame it will not lock securely. Proceed as in step 1.

8.2 Permitted/Prohibited Interventions

8.2.1 Factory reset procedure

Restores the system to the "door not configured" condition

It is possible to restore the door to the new-door state, which means it can be opened with any key.
This is an emergency procedure to be used when it is not possible to perform the key deletion described in the manual (e.g. loss of all registered master keys) or during repair and door restoration operations.

Reset from configuration menu

From the configuration menu it is possible to perform two types of reset.

Under **SETTINGS** →**FACTORY SETTINGS** it is possible to restore the door configu-

ration to factory values, without deleting users and their keys.

Under **USER MANAGEMENT** →**FULL RESET** it is possible to delete all users and therefore restore the factory condition in which any key is accepted by the system.

Reset using DIP switches

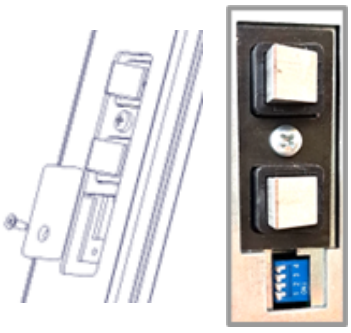
To restore the door to the new-door condition:

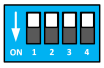
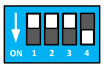
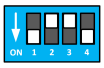
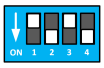
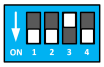
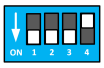
1. open the door;
2. move switches **2 and 4 to ON**;
3. close the door to power it and the display will show the screen "FULL MEMORY ERASE - press to continue";
4. press to continue and enter the code **1-2-3-4-5-6**;
5. the message "Memory erased" will appear.

At this point all keys stored in memory will be deleted and factory settings will be restored. This screen will remain visible until the switches are returned to the desired configuration position.

8.2.2 Use of DIP switches

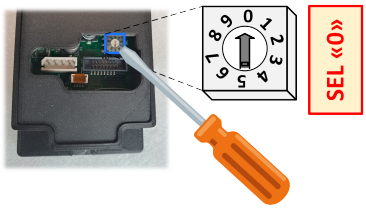
The DIP switches of the lock are located under the metal contacts of the door leaf, accessible by removing the cover, or in case of a door without display, simply by removing the cover screwed onto the lock under the movable contacts of the door leaf.

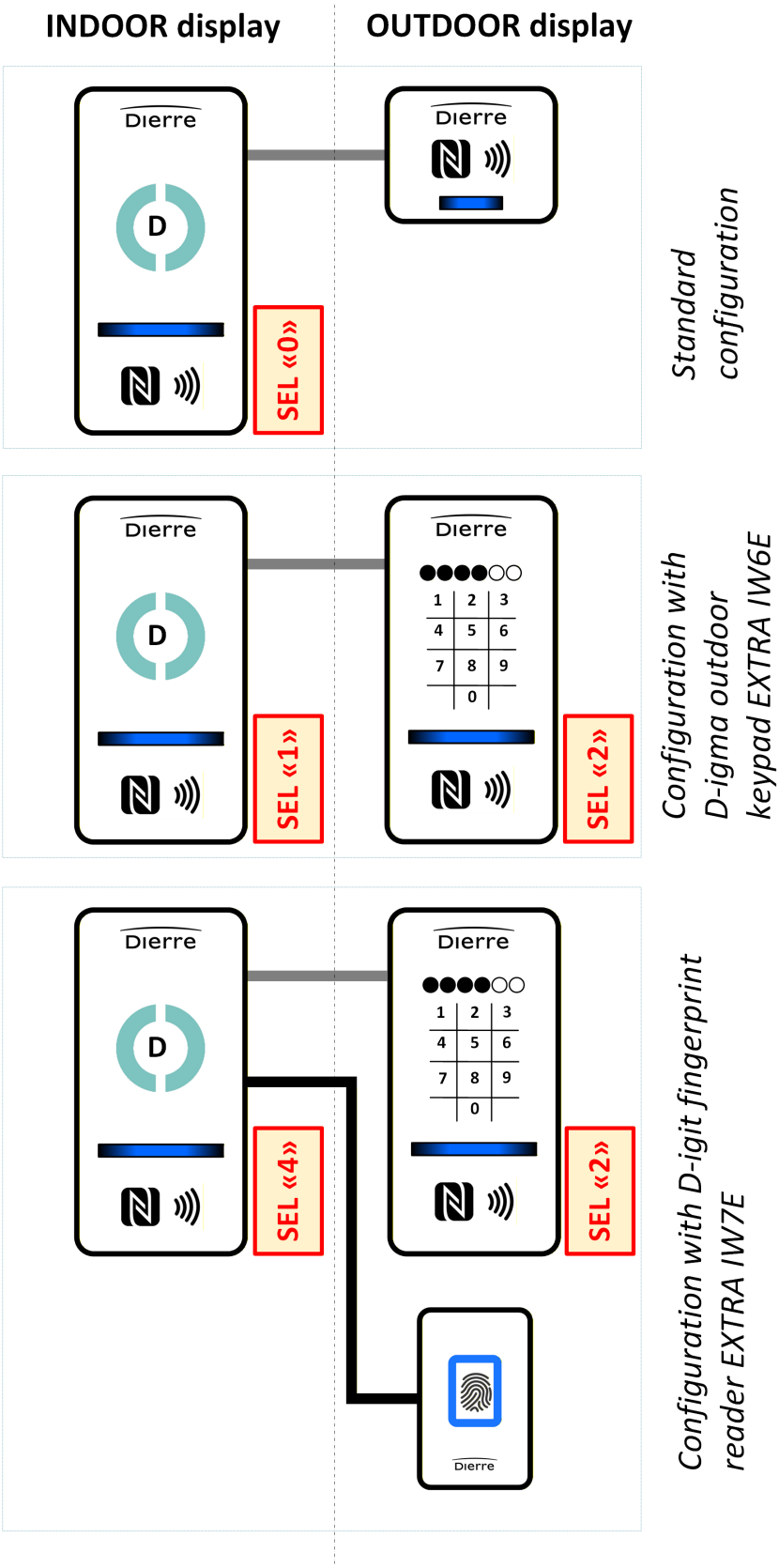


id	DIP ON	Configuration (extra)	Description	Remote button	Internal button	Frame out-puts
	-	-	Outputs active low (0V) – Factory configuration	-	-	LOW
	4	-	Outputs active high (12V)	-	-	HIGH
	1-4	-	**Communication restore function (formerly RESET CODES)**	-	-	-
	2-4	-	**Key reset and factory settings restore function**	-	-	-
	1-2-4	Use with **extra GD8**	AUTOMATIC closing mode	ON	ON	HIGH
	1-2-3		SEMI-AUTOMATIC closing mode	ON	ON	HIGH

8.2.3 Rotary selector setting

The selector is accessible from the rear of the display unit. The correct position is factory-set, but in case of problems or malfunction it should be checked.
It is possible to change the selector position without removing the unit cover, using a small flat-head screwdriver.





Available configurations

9. Disassembly and End-of-Life

9.1 Safe Disassembly

For any operation involving the removal of components from the door, it is recommended to contact an authorized Technical Service *center of Dierre S.p.A.*

For this reason, in this section we only provide instructions related to the removal of the electronic units from the door panel. This operation may be useful for functional checks or when replacing the covering panel.

To remove the internal and external units, proceed as follows:

1. insert a screwdriver into the dedicated slot located at the bottom
2. gently rotate the screwdriver until the body of the unit lifts up
3. use the screwdriver to lift the entire unit from the frame, working around the perimeter

9.2 WEEE and Battery Disposal

This product contains electronic components which must be disposed of, at the end of their life cycle, in accordance with the applicable WEEE regulations. Do not dispose of electronic components with household waste. Use authorized collection centers or follow the procedures established by your local municipality.

The door is not equipped with an internal battery. In the configuration with Extra GD9E (opening via Bluetooth system), the door is supplied with remote controls powered by CR2032 batteries. In this case, at the end of their service life, the batteries must be disposed of in accordance with applicable regulations. Do not dispose of them in the environment and do not place them in unsorted municipal waste. Use authorized collection centers only.

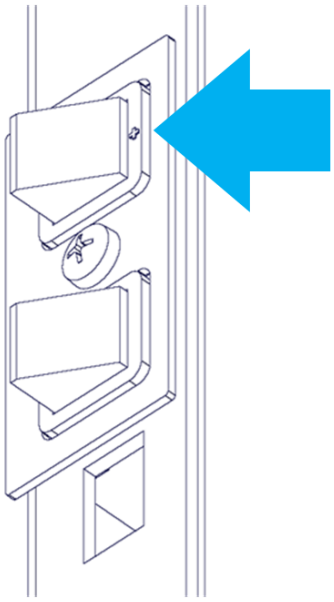
10. Troubleshooting (FAQ)

10.1 Common Issues

10.1.1 The door does not power on

In this case, check that the door is correctly powered. The measurement of the voltage supplied by the power supply is carried out by means of the contacts located on the frame. Follow the instructions below.

Using a multimeter, touch the positive frame contact with the red probe and a fixing screw of the contact holder with the black probe. The same applies to the double-leaf version. The DC voltage measurement must be approximately 12V.



Depending on the door opening direction, the positive contact may be located either on the upper or on the lower contact. To identify the positive contact, check the corresponding contacts on the door leaf where the + sign is indicated.

If the measurement is incorrect or absent, check that:

- mains power is reaching the power supply;
- the connections to the power supply are as indicated in the dedicated section.



10.1.2 The remote button does not work

The remote button allows the door to be opened/closed via a remote push-button or electronic device. Follow these instructions:

- check in the system menu that it is enabled;
- disconnect the power supply for about ten seconds and try opening again;
- perform **COMMUNICATION RESTORE** via the menu or via the DIP switches.

10.1.3 The door opens and closes continuously

If the door performs a continuous cycle of: closing and immediate reopening, then closing again after about 30 seconds, etc., it means that the remote button is short-circuited. Disconnect one of the contacts and try again.If by doing this everything returns to normal, the system that sends the opening signal must be checked. The remote system must always keep the contact open and close it only briefly to command opening.

10.1.4 The internal/external panels do not work

Check that the connector of the cable coming from the lock and the one connecting the internal panel to the external one are correctly inserted in their seats. Also check that these connecting cables are intact.

10.1.5 Service keys do not work

Enter the configuration menu by pressing and holding the display until the access screen appears. Check that the dot to the right of the wording **SERVICE KEYS** is green. **If it is red, it means that all service keys are disabled**; simply press the dot again for 1 second to enable them.

10.1.6 The door does not close with the motorized bolts

For the system to close the lock with the bolts, the latch must retract into the lock when it meets the frame, but then must fully extend once the door is fully closed. If it does not fully extend, the system will not allow motorized closing and the LED will continuously flash green. To solve this problem, adjust the latch by finding the right compromise on the gasket load.

Be careful not to leave the adjustment too loose, and make sure that the door leaf applies adequate compression to the gaskets. Insufficient gasket compression may compromise the door's thermal and acoustic insulation performance.

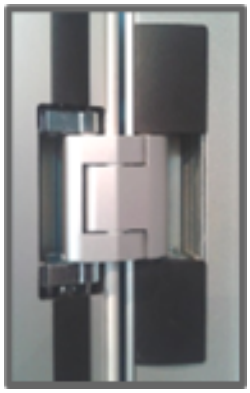
10.1.7 The door closes but immediately reopens

This may occur because the bolts or the deviators encounter an obstacle during their travel that prevents them from reaching the end position. Check that there are no obstructions in the frame along the paths of the deviators or bolts; if necessary, perform a new mechanical adjustment of the door leaf.

In these last two cases it is possible, with the door open, to simulate closing of the lock as described below. ar

For doors with visible hinges connect the positive contacts of the door and frame using an electrical wire. If, with the door open, the lock performs the closing and does not reopen, then check whether the door is too high or too low or whether there are obstacles in the frame holes (bolt and deviator passages). If instead the door continues to reopen, check that the connecting rods between the lock and the deviators are installed with the correct play.

For doors with concealed hinges (e.g. WALL SECURITY, SLEEK, D180), first connect the door leaf ground to the corresponding contact on the frame next to the hinges. On the mobile frame contact there are 2 pins, only one of which is connected to ground on the frame. Check that when the door is closed, the grounded contact touches the door leaf contact, and on the lock side connect the positive contacts of the door and frame with an electrical wire. Then perform the same checks described for doors with visible hinges.



On doors with concealed hinges it is necessary to connect the door leaf ground to the frame ground so that the electronics can operate correctly.

10.1.8 The panels show a steady RED LED or exhibit abnormal behavior

Check that the position of the rotary selector is correct, following the instructions given in the dedicated section. Also check all wiring.

10.1.9 The door shows a flashing GREEN LED but the lock does not close automatically

In this case, check the mechanical adjustment of the door, because the latch is probably not able to fully engage with the frame, and consequently the lock does not start the motorized closing cycle.

10.2 Error Messages

“LOCK COMMUNICATION ERROR”

In this case it is necessary to perform the communication restore function between the electronic boards of the door (SETTINGS →COMMUNICATION RESET); refer to the Communication restore section. If necessary, restore communication using the DIP switches of the lock.

A. Glossary

Acronym	Meaning	Explanation
LCD	*Liquid Crystal Display*	Liquid crystal display
NFC	*Near Field Communication*	Short-range radio communication
RAEE	Waste Electrical and Electronic Equipment	Waste to be disposed of through dedicated procedures
TAG	Literally "label"	Very small identification element
UPS	*Uninterruptible Power Supply*	Device that provides backup power in case of *blackout*

B. Technical Data

The following data refer to the door configuration without additional accessories. Actual current consumption, when optional accessories are installed on the door, may be slightly higher than the values shown in the table.

Specification	**Unit of measure**	**Value**
Operating temperature of electronic components	$°C$	$[-20; +70]$
Supply voltage at frame contacts	V	$12 \pm 10\%$
Nominal low-voltage current consumption at $12V$ in *standby*	A	0.2
Maximum low-voltage current consumption at $12V$ during lock operation	A	1.2
Minimum required clean contact closing time – remote button	ms	300

C. Contacts and Support

Thank you for choosing Dierre and
we wish you pleasant use of hibry5.
For any clarification, please contact your trusted Partner
from whom you purchased Dierre products.

- Contacts or Dealer search: www.dierre.com
- Support email: info@dierre.it
- Phone: +39 0141 949411