



KelNet Lock

USER GUIDE

Copyright

This document is the sole property of Fichet Technologies, a company in the FICHET group. Reproduction is strictly prohibited. Fichet Technologies reserves the right to make any changes or corrections without notice.

The trademarks mentioned in this document are the property of their respective owners.

Copyright © Fichet Technologies 2020

KeINet Lock – User guide

A0U571B – 100037847 – Ed. 05 - NEX – October 2020

PROTECTION OF THE ENVIRONMENT



In compliance with the 2012/19/UE directive pertaining to the Waste Electrical and Electronic equipment (WEEE), this product must be collected separately from the household refuse at the end of its useful life.

This action contributes to the protection of the environment.



The product's packaging is fully recyclable.



RoHS The product complies with the 2011/65/UE directive (RoHS).

WARRANTY



The product is guaranteed for one-year subject to it having been installed in accordance with these instructions.

In the event of the product being returned, it must be placed in packaging similar to the original packaging.

Electronic cards must be packed in antistatic packaging for protection against electrostatic discharges.

READING THE DOCUMENT



This symbol in front of a comment indicates that you must pay particular attention.

Fichet Technologies
Fichet Group
23 route de Schwobsheim
B.P. 40285 Baldenheim
67606 Sélestat Cedex – France

Visiting address:
7 rue Paul Dautier
78140 Vélizy-Villacoublay – France
www.fichetgroup.com

Contents

1	INTRODUCTION	5
2	PRODUCT DESCRIPTION	6
2.1	Input Unit.....	6
2.2	Digital display.....	6
2.3	Sound.....	7
2.4	Power supply.....	8
3	USING THE LOCK	9
3.1	User categories.....	9
3.2	Identification settings	9
3.3	Opening procedure (Class B lock).....	10
3.4	Opening procedure (Class C or D lock).....	12
3.5	Closing procedure (Class B lock).....	15
3.6	Closing procedure (Class C or D lock)	16
3.7	Emergency blocking.....	17
3.8	CIT anti-passback procedure.....	17
3.9	Wrong code blocking rules.....	17
3.10	Messages.....	18
3.11	Mandatory changing of the opening code when using the lock for the first time	19
3.12	Changing the opening code by the user himself.....	20
4	INPUT UNIT CONFIGURATION	22
4.1	Basic Input Unit configuration	22
4.2	Advanced configuration (Technician menu)	23
5	SECURE UNIT CONFIGURATION	24
5.1	Access to configuration menu.....	24
5.2	Menus list.....	26
5.3	User's parameters configuration	28
5.4	Schedules configuration.....	29
5.5	Delays configuration	30
5.6	Calendar configuration.....	31
5.7	Identification configuration	32
5.8	Secure Unit configuration.....	33
5.9	System configuration	37
5.10	Maintenance.....	38
5.11	Audit.....	39
6	CHANGING THE CONFIGURATION WITH A USB KEY	40
6.1	Introduction	40
6.2	Writing configuration with a USB key.....	40
6.3	Reading configuration and saving on a USB key	41
6.4	Writing schedules with a USB key	42
6.5	Reading schedules and saving on a USB key.....	43
7	FINGERPRINT	44
7.1	Instructions for enrolling fingerprints.....	44
7.2	Enrolment in mode “Code + Fingerprint”	44
7.3	Enrolling procedure.....	45
7.4	Opening procedure with fingerprint.....	48
7.5	Changing the fingerprint by the user himself	49
7.6	Deleting a fingerprint by the user himself	50
7.7	Deleting all fingerprints	51
8	REDUNDANT LOCK SPECIFICITIES	52
9	FACTORY SETTINGS.....	53
10	RECYCLING	54
10.1	Recycling the Secure Unit's authentication keys.....	54
10.2	Recycling the Secure Unit's address	54
10.3	Complete recycling of the Secure Unit	55
10.4	Recycling the Input Unit's authentication keys	55

- 10.5 Complete recycling of the Input Unit..... 55
- 11 MAINTENANCE..... 56
 - 11.1 Replacing an Input Unit operating in factory mode..... 56
 - 11.2 Replacing a Secure Unit operating in factory mode 57
- 12 GLOSSARY 58

1 INTRODUCTION

KelNet is a certified high-security electronic lock for securing access to valuable objects inside safes and vaults.

KelNet Components:

- **IU (Input Unit):**

The terminal used for entering codes and setting the locks.

An Input Unit manages from 1 to 16 Secure Units.



- **SU (Secure Unit):**

There are two types of SUs:

- **Standard SU (SU):**

Component used for blocking the door locking mechanism.



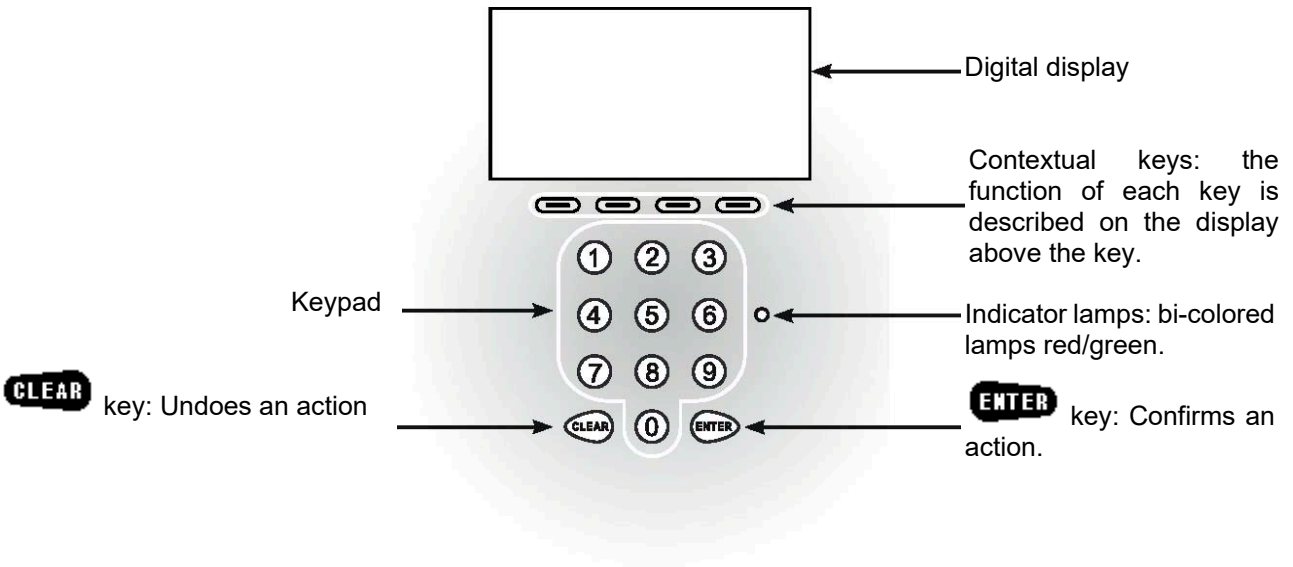
- **Redundant SU (SU-R):**

As compared with the standard SU, the SU-R provides the system with increased reliability: the electronic card, the motor and the communications bus are all duplicated.



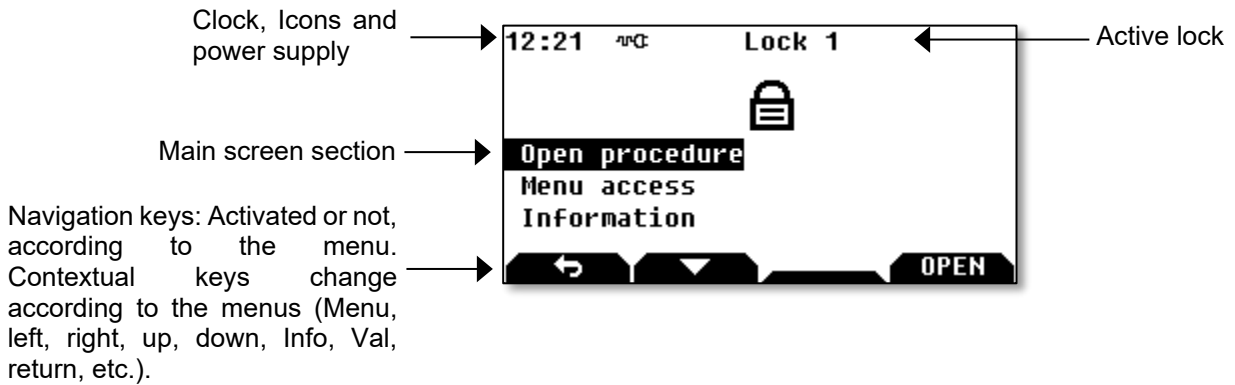
2 PRODUCT DESCRIPTION

2.1 Input Unit






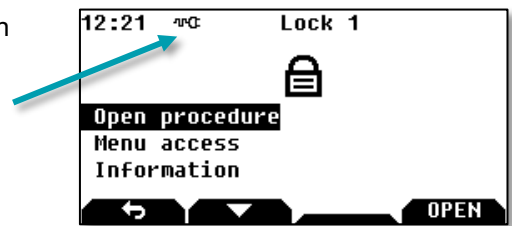
2.2 Digital display

2.2.1 Display zones










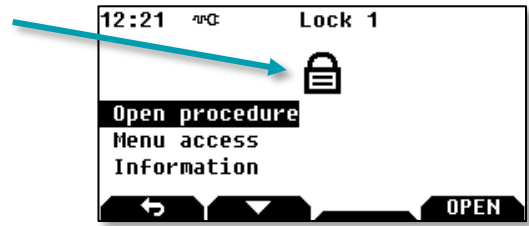
2.2.2 Status icons

-  Battery power supply and low battery indication
-  External power supply
-  Wrong code








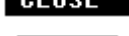









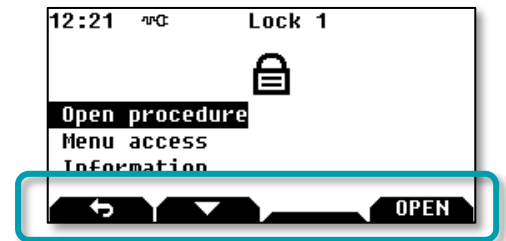
2.2.3 Menu icons

-  Locking Device closed
-  Locking Device open
-  Fingerprint
-  Single access
-  4 eyes access
-  Caution – This icon is used to display system messages.
Press **ENTER** to continue the procedure in progress.
-  Indicates that the conveyors (or any user with CIT anti-passback procedure) have passed. The icon is displayed until another code is used.



2.2.4 Contextual keys

-  Left
-  Right
-  Up
-  Down
-  Return to previous screen
-  Select or validate a modification
-  Launch the opening procedure (available in all languages)
-  Launch the closing procedure (available in all languages)
-  Decrease by one
-  Increase by one
-  Enable
-  Disable
-  To validate an action (available in all languages)
-  To discard an action (available in all languages)
-  Without function



2.3 Sound

The lock is equipped with a buzzer:

- with adjustable intensity,
- and with a time and a frequency that can be set in the list of messages.

2.4 Power supply

2.4.1 Battery and/or mains supply

The lock can be supplied with:

- Battery only.
- Battery and mains supply.
- Mains supply only.

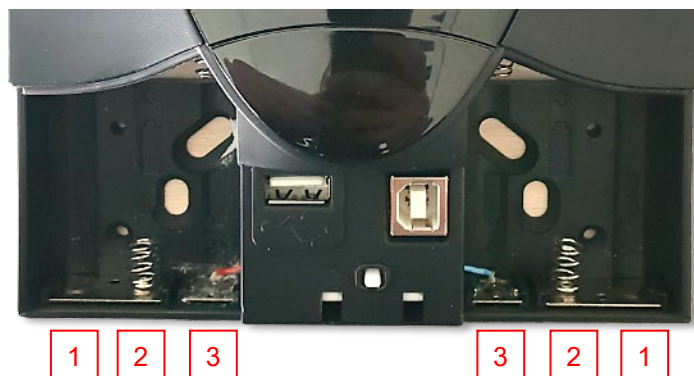
The Input Unit's batteries can be used to power it with a maximum of 2 Secure Units.



If the lock is supplied with external supply and battery:

- It is still necessary to check the battery regularly. Replace them as soon as a "low battery level" message is displayed.
- When the main supply is lost, the lock switches over automatically to the battery supply.

2.4.2 Battery installation



- Type of batteries: 6 x AAA (LR6) 1.5V.
- Respect the polarity.
- Install batteries in the following order: **1** , **2** , then **3**.

3 USING THE LOCK

3.1 User categories

The users are distributed in 3 groups:

- **Super managers:** There are 2 super managers. The Super managers have authority over the managers. Each super manager can change the user code of another super manager with the Input Unit.
- **Managers:** The managers can have authority over the operators
- **Operators:** The “standard” users of the lock.

3.2 Identification settings

A user is identified by:

- His user ID.
- His pin code from 6 to 10 figures:
 - For B class, the minimum length is 6 figures.
 - For C class, the minimum length is 7 figures.
 - For D class, the minimum length is 8 figures.



Super Managers:

- User ID: 1 or 2
- Default code: 00000000.

Different identification modes are possible:

■ Code only:

- Enter your user ID and press the **ENTER** key.
- Enter your PIN code and press the **ENTER** key.

■ Code + Fingerprint (optional):

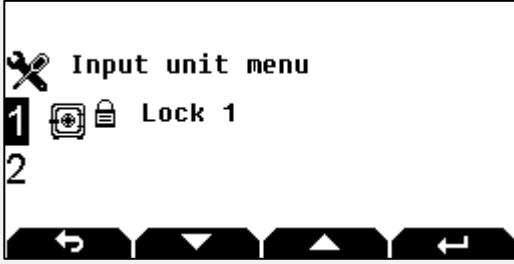


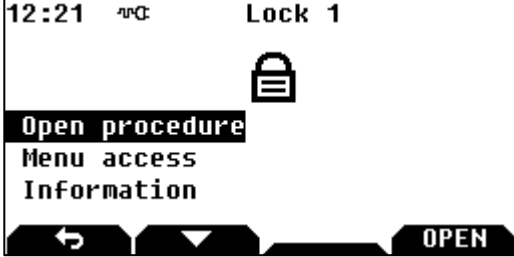
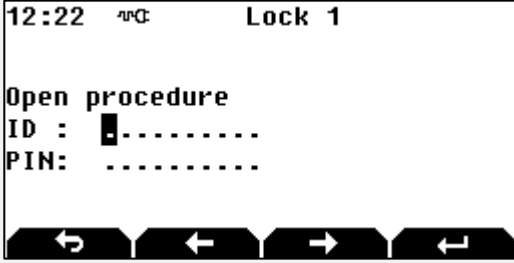
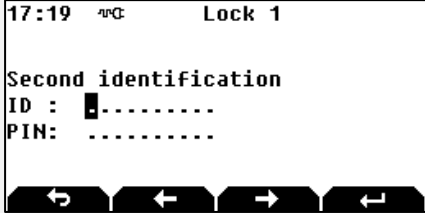
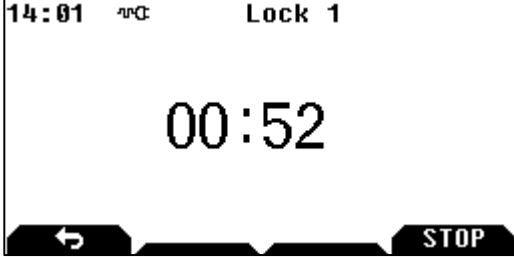
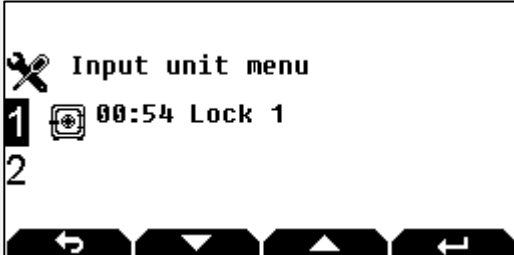
- Enter your user ID and press the **ENTER** key.
- Enter your PIN code and press the **ENTER** key.
- When the code is validated, the fingerprint is requested: scan your finger with the biometric reader.



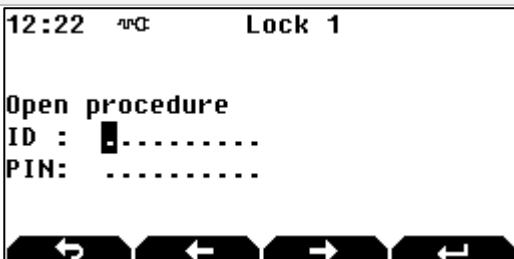
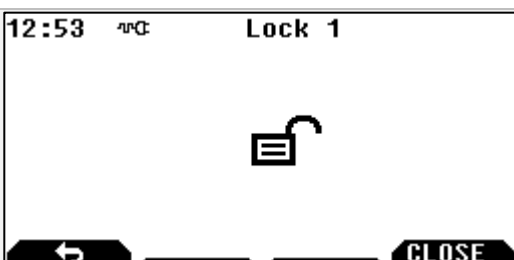
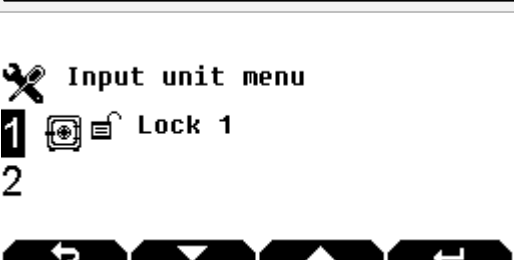
See chapter 7 “FINGERPRINT” for more details.



It is possible to configure a lock with fingerprint identification on its own (without a code). This is only authorized on a lock without certification, only available on request.

3.3 Opening procedure (Class B lock)

Step	Screen	Description
1		<p>Select the lock + ENTER</p> <p>Note: to select another lock, use arrows  and .</p>
2		<p>Press ENTER or use the open button OPEN to launch the opening procedure.</p>
3		<p>Enter your user ID + ENTER</p> <p>Enter your PIN code + ENTER</p> <p>A safe PIN code is composed of at least 6 figures for the B class (max 10 figures).</p> <p>If a fingerprint is linked with the user, it will be required (See Fingerprint chapter).</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>In accordance with the settings, a "4 eyes" procedure may be required (involving two different users being identified). In this case, a second code is requested:</p>  <p>If a fingerprint is linked with the user, it will be required (See Fingerprint chapter)</p> </div>
4		<p>Wait until the end of delay if delays are programmed and used in a schedule, otherwise go to step 9.</p>
5		<p>If the main screen is displayed, the states of all locks are available.</p>

Step	Screen	Description
6		<p>This main screen means that a second identification is necessary.</p> <p>Select the lock and press ENTER</p>
7		<p>Select Open procedure or the OPEN button to continue the opening procedure or Closing procedure to abort opening.</p>
8		<p>Enter your user ID + ENTER .</p> <p>Enter your PIN code + ENTER .</p> <p>The second user shall enter their ID and PIN code.</p>
9		<p>The lock is unlocked.</p>
10		<p>This main screen means the lock is unlocked.</p>



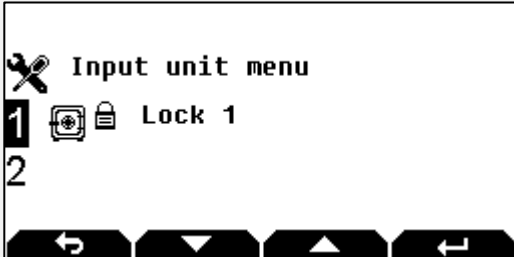


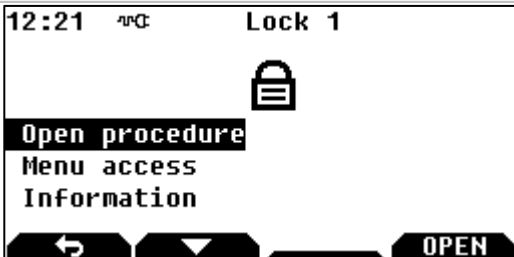
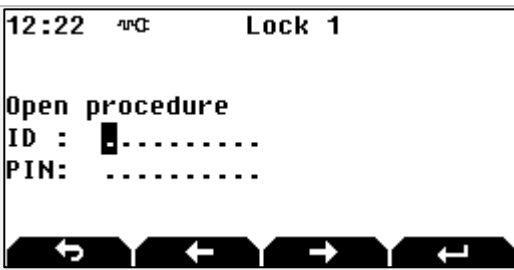
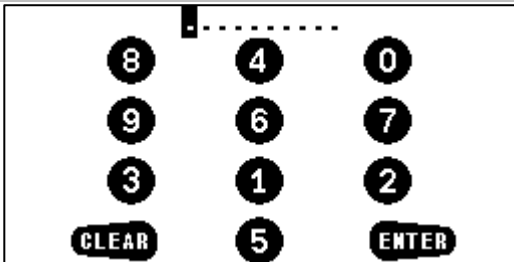
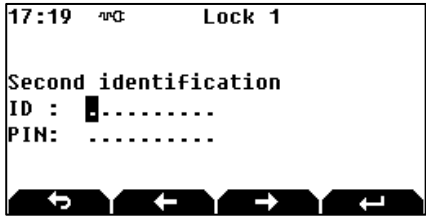
When the opening procedure is started, if no entries are made on the keypad within 20 seconds, the opening procedure is aborted, and the main screen is displayed.

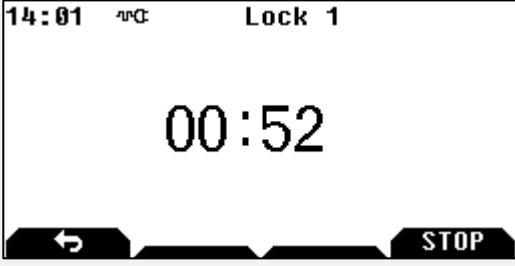
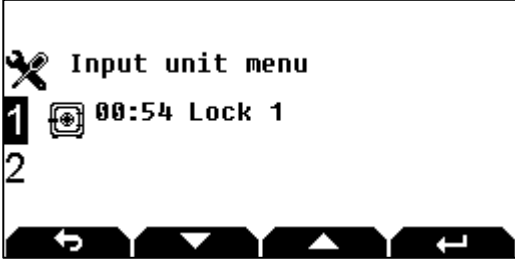

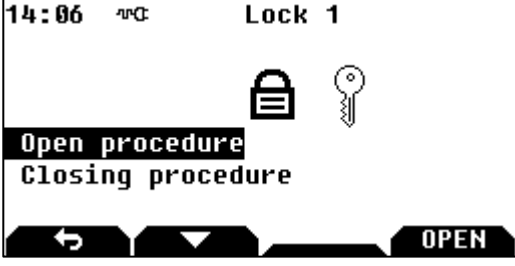
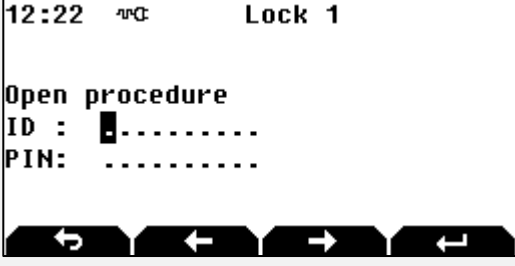
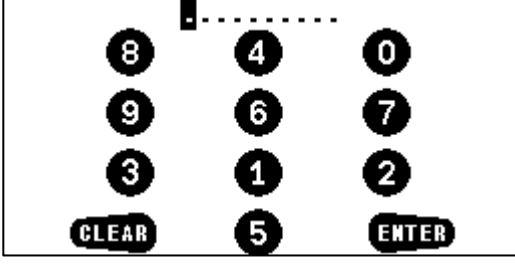
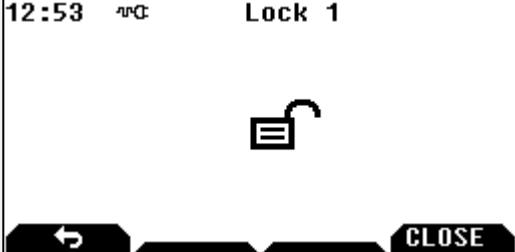


The opening code is confidential and must be entered exclusively in a safe environment.

3.4 Opening procedure (Class C or D lock)

If the lock is a **class C or D lock**, the code can only be entered in **random mode**.

Step	Screen	Description
1		<p>Select the lock + ENTER</p> <p>Note: to select another lock, use arrows  and .</p>
2		<p>Press ENTER or use the open button OPEN to launch the opening procedure.</p>
3		<p>Enter your user ID + ENTER.</p>
4		<p>Enter your PIN code with the virtual keyboard + ENTER</p> <p>In this example, key 1 corresponds to figure 8, key 2 corresponds to figure 4, etc.</p> <p>The position of virtual figures changes for each display.</p> <p>A safe PIN code is composed of at least 7 figures for the C class and 8 for the D class (max 10 figures).</p> <p>If a fingerprint is linked with the user, it will be requested (See Fingerprint chapter).</p> <div style="border: 1px solid black; border-radius: 15px; padding: 10px; margin-top: 10px;"> <p>In accordance with the settings, a "4 eyes" procedure may be required (involving two different users being identified). In this case, a second code is requested:</p>  <p>If a fingerprint is linked with the user, it will be requested (See Fingerprint chapter)</p> </div>

Step	Screen	Description
5		<p>Wait until the end of delay if delays are programmed and used in a schedule, otherwise go to step 10.</p>
6		<p>If the main screen is displayed, the states of all locks are available.</p>
7		<p>This main screen means that a second identification is necessary.</p> <p>Select the lock and press ENTER</p>
8		<p>Select Open procedure or the OPEN button to continue the opening procedure, or Closing procedure to abort opening.</p>
9		<p>Enter your user ID + ENTER</p> <p>Enter your PIN code + ENTER</p> <p>The second user shall enter their user ID + ENTER</p>
10		<p>Enter your PIN code with the virtual keyboard + ENTER</p> <p>In this example, key 1 corresponds to figure 8, key 2 corresponds to figure 4, etc.</p> <p>The position of virtual figures changes for each display.</p>
11		<p>The lock is unlocked.</p>



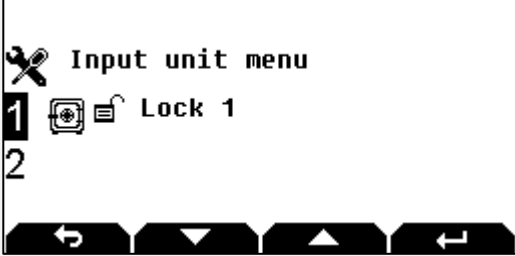


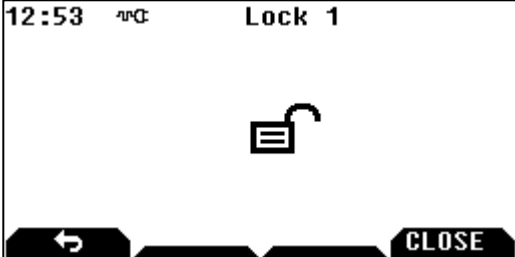
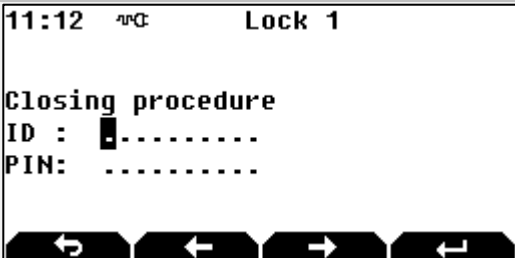
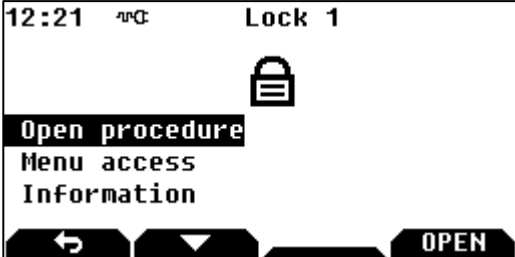
When the opening procedure is started, if no entries are made on the keypad within 20 seconds, the opening procedure is aborted, and the main screen is displayed.



The opening code is confidential and must be entered exclusively in a safe environment.

3.5 Closing procedure (Class B lock)

- **Automatic:** if the boltwork switch is connected, the lock will automatically be secured and the boltwork is locked.
- **Manual:** follow the procedure below.

Step	Screen	Description
1		<p>Select the lock + ENTER</p> <p>Note: to select another lock, use arrows  and .</p>
2		<p>Press CLOSE button to launch the closing procedure.</p>
3		<p>If identification for closing is activated:</p> <p>Enter your ID + ENTER and your PIN code + ENTER, otherwise go to step 4.</p> <p>If a fingerprint is linked with the user, it will not be requested for the closing procedure.</p>
4		<p>The lock is locked.</p>

3.6 Closing procedure (Class C or D lock)

- **Automatic:** if the boltwork switch is connected, the lock will automatically be secured and the boltwork is locked.
- **Manual:** follow the procedure below.

Step	Screen	Description
1		<p>Select the lock + ENTER</p> <p>Note: to select another lock, use arrows and .</p>
2		<p>Press CLOSE button to launch the closing procedure.</p>
3		<p>If identification for closing is activated:</p> <p>Enter your ID + ENTER , otherwise go to step 5.</p>
4		<p>Enter your PIN code with the virtual keyboard + ENTER</p> <p>In this example, key 1 corresponds to figure 8, key 2 corresponds to figure 4, etc.</p> <p>The position of virtual figures changes for each display. If a fingerprint is linked with the user, it will not be requested for the closing procedure.</p>
5		<p>The lock is locked.</p>

3.7 Emergency blocking

In emergency, press keys **7** + **9** to secure the door and to prevent any opening procedure for 30 mins (settable from 1 to 99 mins).



It is not possible to change the emergency blocking keys.

3.8 CIT anti-passback procedure

This procedure can be used to limit the period of time within which a code may be used and the number of consecutive openings.


If the anti-passback function is activated in "CIT" mode:


- The first time the code is entered, the door is opened, and the time delay defined in the Configuration Tool is started.
- The same code may then be used several times up to the maximum number defined in the Configuration Tool.
- Once the code has been entered the maximum number of times or once the time delay has ended, the code may no longer be used.

The code can be reactivated by a user from another rights group logging on.

As soon as the CIT anti-passback time delay has started, all other opening requests and attempts to access the menu are prohibited until it has ended.

If a code is entered during this period, the message "**Anti-passback active**" is displayed.

Once the code has been entered the maximum number of times or once the time delay has ended, the  icon is displayed to indicate that the anti-passback code may no longer be used, but that all other codes may once again be used.

The  icon disappears once a user from another rights group has logged on.

Until the CIT anti-passback code has been rearmed (by a user code), the message "**Invalid code**" is displayed if the code is entered.

3.9 Wrong code blocking rules

There are 2 rules that define the blocking time after entering several wrong codes:

- Increasing blocking time:
 - After 4 wrong codes = 10' blocking
 - Then, if the next code is wrong = 20' blocking
 - Then, for each wrong code entered = 30' blocking.
- Fixed blocking time; Blocking time value is 3 to 99 minutes for class B or C and 8 to 99 minutes for class D.

Entering the correct code will reset the wrong code counter.

3.10 Messages

Messages below can be displayed when the lock is waked-up.

Message	Cause	Action
Battery lid is open	The lib of battery access is open.	Close the battery lid.
Anti-tear switch is open	The Input Unit anti-tear switch is activated.	Check if there is no fraudulent removal of the Input Unit. Replace the Input Unit on its support.
Anti-tear switch was open!	The Input Unit anti-tear switch was activated.	Check if there was no fraudulent removal of the Input Unit.

3.11 Mandatory changing of the opening code when using the lock for the first time



The system makes it compulsory to perform this code change only for users with codes that begin with ID 4 and upwards. However, when using the device, the factory code should not be left for the users of ID 1 to 3.

Step	Screen	Description
1		Select the lock + ENTER Note: to select another lock, use arrows and .
2		Use arrows and to select Open procedure or Menu access + ENTER
3		Enter your ID + ENTER Enter the PIN code 00000000 + ENTER
4		The Expired code message appears. Enter your new PIN code + ENTER Confirm your PIN code + ENTER A safe PIN code is made with at least 6 figures for the B class, 7 for the C class and 8 for the D class.



The opening code must be kept safe and entered exclusively in a safe environment. If it is suspected or known that the code is known to another person, then it is to be replaced immediately with a new code.

Do not use:

- Personal details (e.g. date of birth) or other data that can be easily linked to the user should not be used.
- Trivial codes should not be used. Trivial codes include descending and ascending series of digits (e.g. < 5-6-7-8-9-0-1-2 > or < 3-2-1-0-9-8-7-6 >) as well as digits that are all the same (e.g. < 4-4-4-4-4-4-4 >).

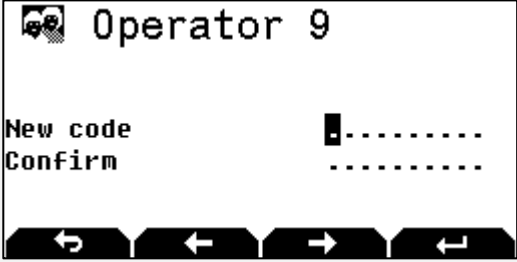
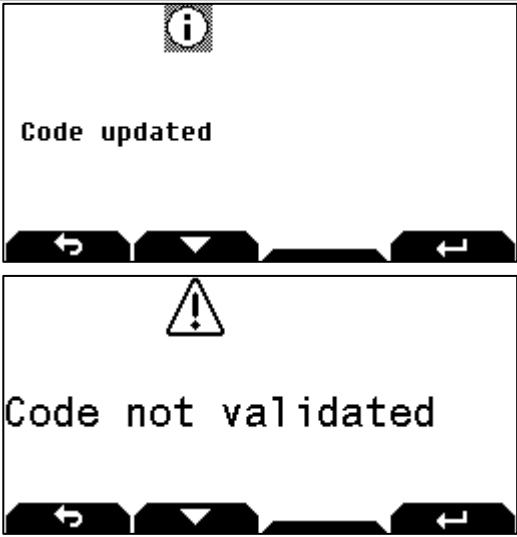
Security relevant parts of the KelNet should not be accessible to unauthorized persons when the door of the secure storage unit to which it is fitted is open.



After a code change, the lock must be tried several times, with the door in the open position.

3.12 Changing the opening code by the user himself

Step	Screen	Description
1		<p>Select the lock + ENTER</p> <p>Note: to select another lock, use arrows and .</p>
2		<p>Use arrow to select Menu Access + ENTER</p>
3		<p>Enter your ID + ENTER</p> <p>Enter your PIN code + ENTER</p> <p>If a fingerprint is linked with the user, it will be requested (See Fingerprint chapter).</p>
4		<p>Press ENTER</p> <p>For a user without fingerprint identification go to step 5 otherwise go to step 6.</p>
5		<p>Press ENTER and go to step 7.</p>
6		<p>Select My code and press ENTER.</p>

Step	Screen	Description
7		<p>Enter and confirm your new PIN code and press ENTER.</p>
8		<p>If the Code updated message is displayed, the code has been changed; else, if Code not validated is displayed, you shall restart with the step 4.</p>



The opening code must be kept safe and entered exclusively in a safe environment. If it is suspected or known that the code is known to another person, then it is to be replaced immediately with a new code.

Do not use:

- Personal details (e.g. date of birth) or other data that can be easily linked to the user should not be used.
- Trivial codes should not be used. Trivial codes include descending and ascending series of digits (e.g. < 5-6-7-8-9-0-1-2 > or < 3-2-1-0-9-8-7-6 >) as well as digits that are all the same (e.g. < 4-4-4-4-4-4-4-4 >).

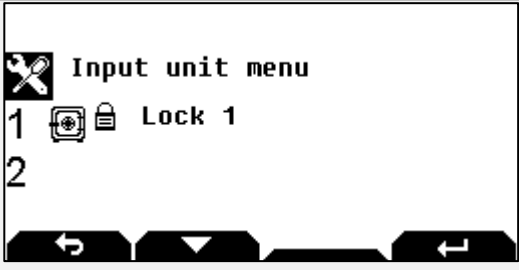

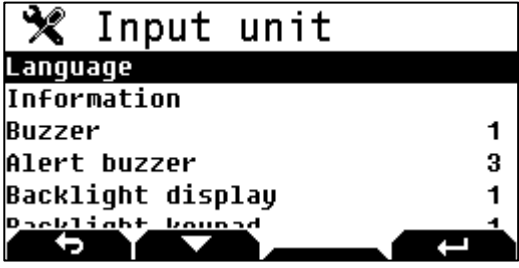
Security relevant parts of the KelNet should not be accessible to unauthorized persons when the door of the secure storage unit to which it is fitted is open.




After a code change, the lock must be tried several times, with the door in the open position.

4 INPUT UNIT CONFIGURATION

4.1 Basic Input Unit configuration

Step	Screen	Description
1		Select the Input Unit menu with  + ENTER
2		Available configuration in the Input Unit menu .



To return to the previous screen, press .

Function	Sub-function	Description
Input Unit	Language	To change the display language
	Information	To display input unit information
	Buzzer	To manage the level of the buzzer when a key is hit.
	Alert buzzer	To manage the level of the buzzer during an alert.
	Backlight display	To select the backlight level for the screen.
	Backlight keyboard	To select the backlight level for the keyboard.

4.2 Advanced configuration (Technician menu)



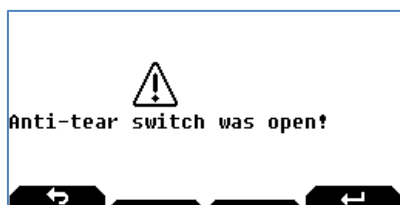
The Technician menu is only visible if the Input Unit anti-tear switch is open.

Step	Screen	Description
1		Select the Technician menu + ENTER .
2		Configuring the Input Unit's address from 17 to 20. Address 17 is for the 1st Input Unit.
3		The SU bus menu is for choosing the communications bus with the locks: <ul style="list-style-type: none"> • Either MF2 (by default) • Or RS485 The RS485 bus cannot operate by battery only.
4		The SU validation menu is for validating the locks which are managed by the Input Unit. Switch the "valid locks" to ON .
5		The Delete Fingerprints menu is for deleting all the fingerprints in the fingerprint sensor mounted on the Input Unit.



As long as the anti-tear switch is open, the "**Anti-tear open**" message is displayed and only access to the Input Unit's menu is authorised.

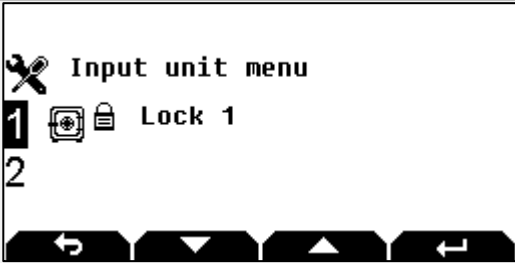


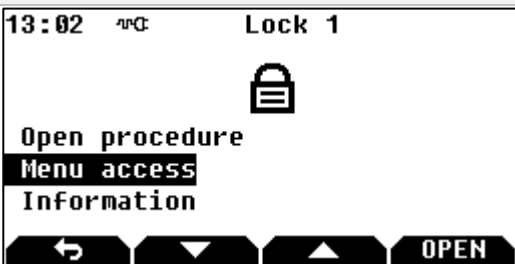

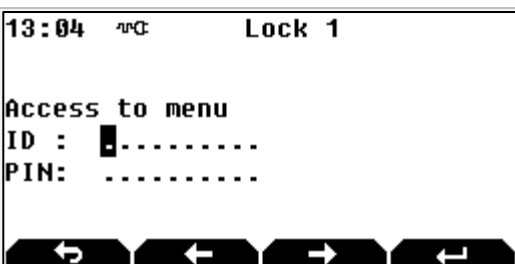
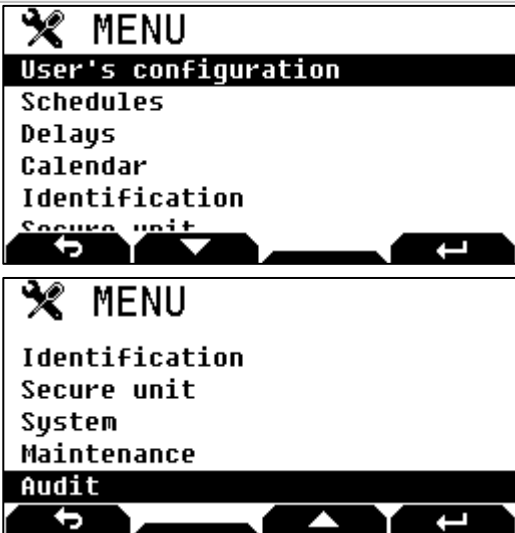
Otherwise, the following message is displayed:

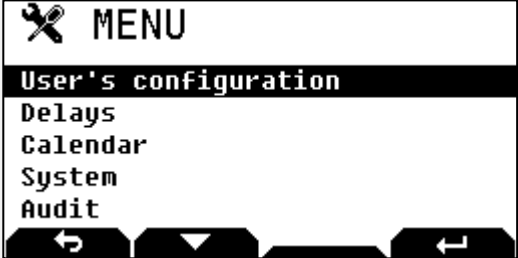
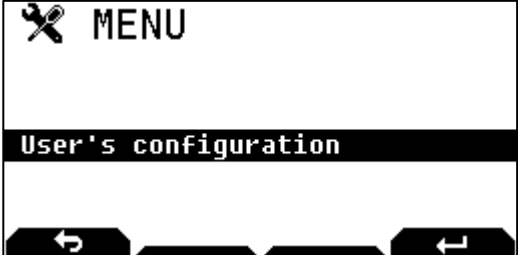




This message is displayed until there is a valid identification, but it does not prevent the lock from being used.

5 SECURE UNIT CONFIGURATION

5.1 Access to configuration menu

Step	Screen	Description
1	 <p>The screen displays 'Input unit menu' with a wrench icon. Below it, 'Lock 1' is highlighted with a '1' in a box. There are navigation arrows at the bottom.</p>	<p>Select the lock + ENTER</p> <p>Note: to select another lock, use arrows  and .</p>
2	 <p>The screen shows '13:02' and 'Lock 1' at the top. A padlock icon is in the center. Below it, the menu options are 'Open procedure', 'Menu access' (highlighted), and 'Information'. There are navigation arrows and an 'OPEN' button at the bottom.</p>	<p>Use arrow  to select Menu access + ENTER</p>
3	 <p>The screen shows '13:04' and 'Lock 1' at the top. Below it, the text 'Access to menu' is displayed. There are two input fields: 'ID : ' and 'PIN: ' with a cursor in the first field. There are navigation arrows at the bottom.</p>	<p>Enter your user ID + ENTER</p> <p>Enter your PIN code + ENTER</p> <p>If a fingerprint is linked with the user, it will be requested (See Fingerprint chapter).</p> <p>In accordance with the settings, a "4 eyes" procedure may be required (involving two different users being identified). In this case, a second code is requested.</p> <p>Available menus are displayed in accordance with user rights:</p> <ul style="list-style-type: none"> • Super-Manager: step 4 • Manager: step 5 • User: step 6
4	 <p>The top screenshot shows a 'MENU' screen with 'User's configuration' highlighted. Below it are 'Schedules', 'Delays', 'Calendar', 'Identification', and 'Secure unit'. There are navigation arrows at the bottom.</p> <p>The bottom screenshot shows a 'MENU' screen with 'Identification' highlighted. Below it are 'Secure unit', 'System', 'Maintenance', and 'Audit'. There are navigation arrows at the bottom.</p>	<p>Available menus for a Super-Manager</p>

Step	Screen	Description
5		<p>Available menus for a Manager</p>
6		<p>Available menu for a User.</p>

 To return to the previous screen, press .

The content of the menu is different according to the user rights.
 Each user only sees functions which he has the right to use.

5.2 Menus list

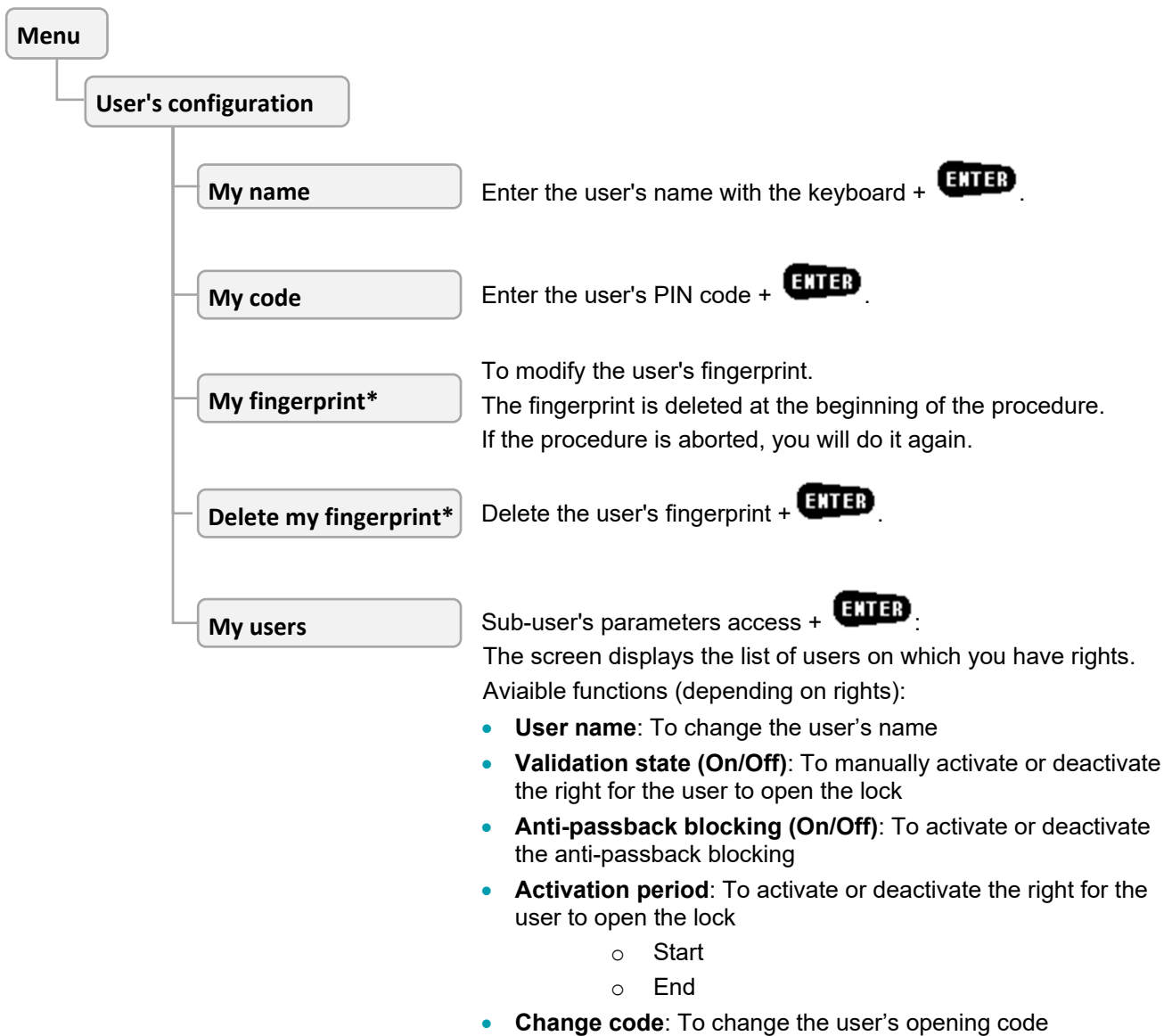
The main menu list, depending on the user's profile, contains part or the totality of the following functions: (SM: Super Manager; M: Manager; U: User):

Function	Sub-function	Description	SM	M	U
Users	My name	To change my name.	✓	✓	
	My code	To change my code.	✓	✓	✓
	My fingerprint ⁽¹⁾	To enrol my fingerprint.	✓	✓	✓
	Delete my fingerprint ⁽¹⁾	To delete my fingerprint.	✓	✓	✓
	My users	To modify parameters of my sub-users.	✓	✓	
Schedules	Standard week	To modify the standard week schedule.	✓		
	Extended week	To modify the extended week schedule.	✓		
	Extended period	To modify the extended period schedule.	✓		
Delays	Delay 1 to delay 4	After a schedule selection, enables defining the opening delay in normal mode.	✓	✓	
	4 eyes delay	After a schedule selection, enables defining the opening delay in 4 eyes mode.	✓	✓	
Calendar	Public holiday	To enable or to disable a public holiday	✓	✓	
	Exceptional closing.	To define dates and hours of an exceptional closing.	✓	✓	
	Exceptional opening	To define dates and hours of an exceptional opening.	✓	✓	
Identification	Inactive ID	After the rights group selection, enables modifying the days' number after which the user's PIN code becomes inactive.	✓		
	Code expiry period	After the rights group selection, enables modifying the days' number after which the user's PIN code must be changed.	✓		
	Anti passback	After the rights group selection, enables changing the identification method of a user for a second identification.	✓		
	Fixed delay	After the rights group selection, enables fixing the opening delays' value in minutes. Value = 255 if delay is defined in schedules.	✓		
Secure Unit	MID	<ul style="list-style-type: none"> Displays the Module Identification number. 	✓		
	Parameters + Id after delay	Enables defining or disabling the second identification after opening delay.	✓		
	Parameters + Closing with ID	Enables defining or disabling the closing by ID.	✓		
	Parameters + Bolt inside timeout	Enables defining the delay after which the lock locks itself.	✓		
	Parameters + Delay after closing	Enables defining the delay between a closing and a new opening.	✓		
	Parameters + Access autho. time (G1)	Enables defining the delay for an access authorization (G1 procedure), value = 15 to 180 seconds. If value = 0: the "Access autho. Time (G1) » function is inactive.	✓		
	Parameters + Alarm digit	Enables defining a value added to the code to launch a duress alarm.	✓		
	Parameters + Motor speed	Enables defining the motor speed.	✓		

Function	Sub-function	Description	SM	M	U
	Parameters + Closing hour 1	Enables defining a closing hour. 00:00 = no closing hour	✓		
	Parameters + Closing hour 2	Enables defining a second closing hour. 00:00 = no closing hour			
	Inputs + IN 1 to IN 8, IL, PB	Enables choosing a function associated to the selected input.	✓		
	Outputs + OUT 1 to OUT 3, IL, Red, Green	Enables choosing a function associated to the selected output.	✓		
System	Clock adjustment	To adjust date and time.	✓	✓	
	Summer time	To enable or to disable time modification for summer and winter.	✓		
	Parallel mode	To enable or to disable the parallel mode.	✓		
	Interlocking	To choose an interlocking rule.	✓		
Maintenance	Download access	To set secure unit in download mode to send its configuration with the Configuration Tool.	✓		
	Security + Secure the IU-SU link	To start the securing of the link Input Unit with Secure Unit.			
	Security + Securing by CT authorization	To authorize the Configuration Tool to secure all devices.			
	USB memory key + Write configuration (CT -> SU)	Enables downloading a configuration file made with the Configuration Tool to the lock.	✓		
	USB memory key + Read configuration (SU -> CT)	Enables saving the configuration of the lock in the USB key to read it with the Configuration Tool.	✓		
	USB memory key + Write schedules (CT -> SU)	Enables downloading schedules made with the Configuration Tool to the lock.	✓		
	USB memory key + Read schedules (SU -> CT)	Enables saving schedules of the lock in the USB key to read it with the Configuration Tool.	✓		
	OTC mode	To choose the OTC mode wanted: None, OTC standard, OTC via IP.	✓		
	OTC key	To configure the key of the OTC mode.	✓		
	Access to menu	To select the identification type to menu access.	✓		
Audit	Display audit	To display past events of the secure unit.	✓	✓	
	Download to USB memory	To save past events in USB key.	✓	✓	
	Display program download audit	To display the software update audit.	✓	✓	

(1) Only for users with identification mode "PIN Code + Fingerprint".

5.3 User's parameters configuration



* Only for users with identification mode "PIN Code + Fingerprint"

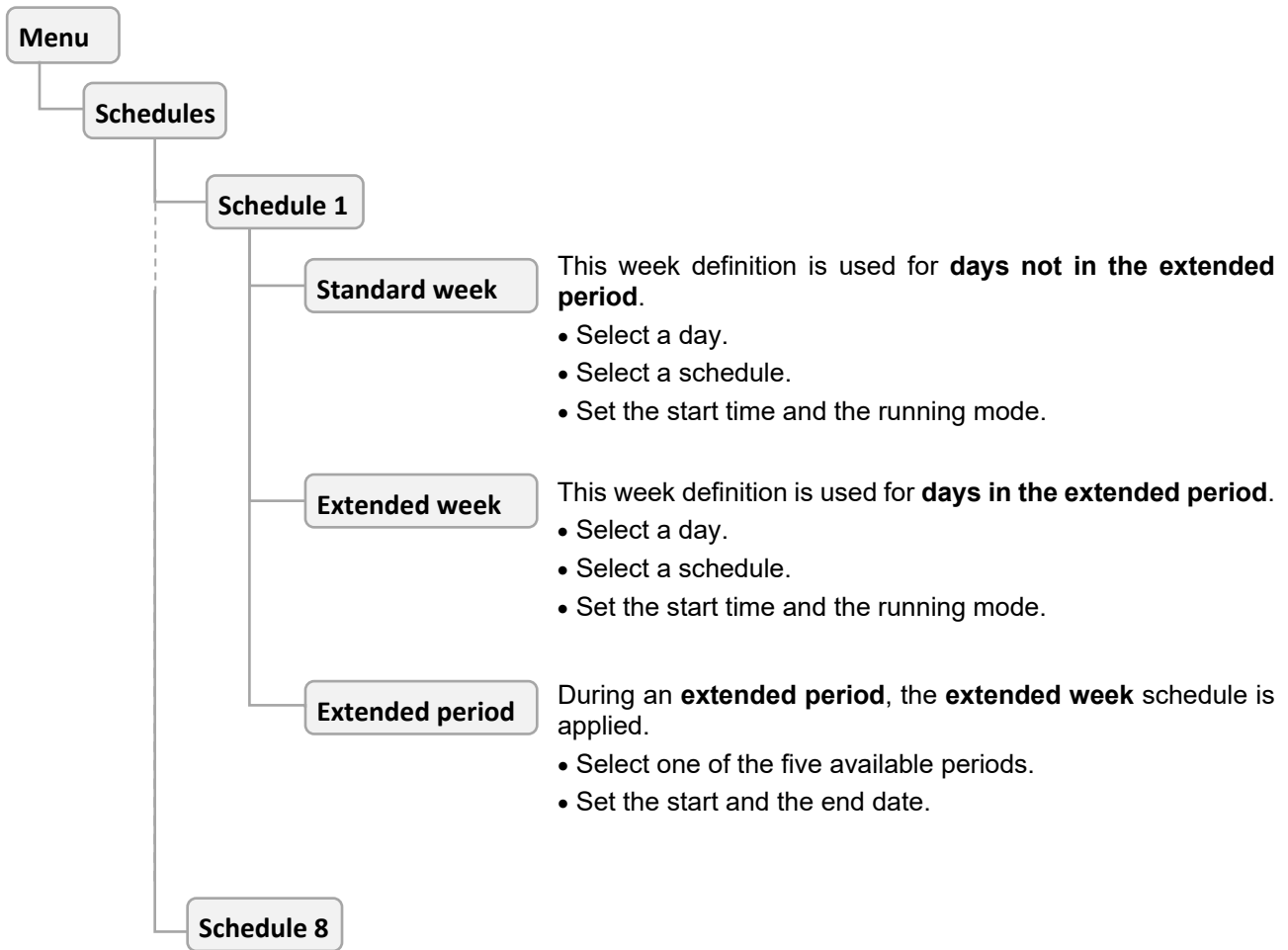


Parameters are available in accordance with the user's rights.

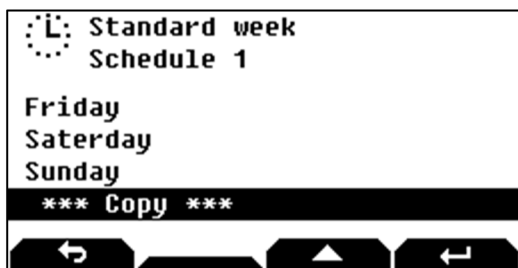


User parameters are changed only for the Secure Unit selected before entering the menu. Repeat the same operations to change the user parameters on the other Secure Units.

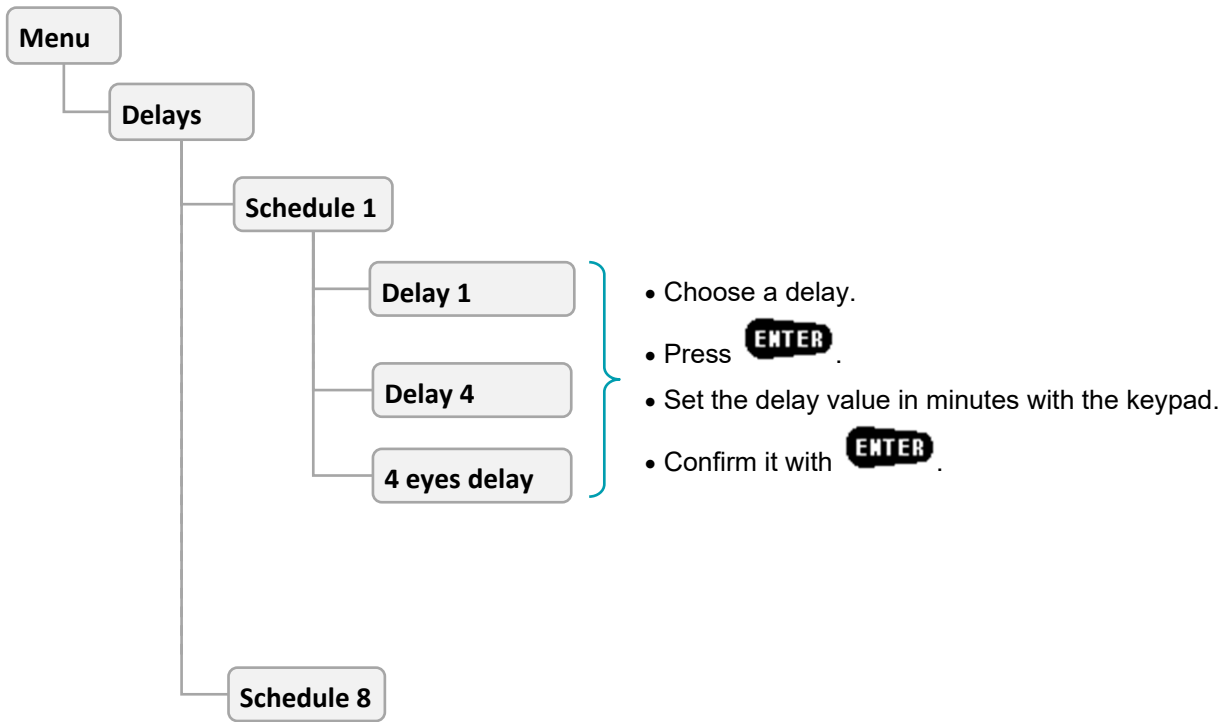
5.4 Schedules configuration




i The 8 schedules have the same parameters.
 The configuration of a day can be copied to another one with the **Copy** function at the bottom of the day list:

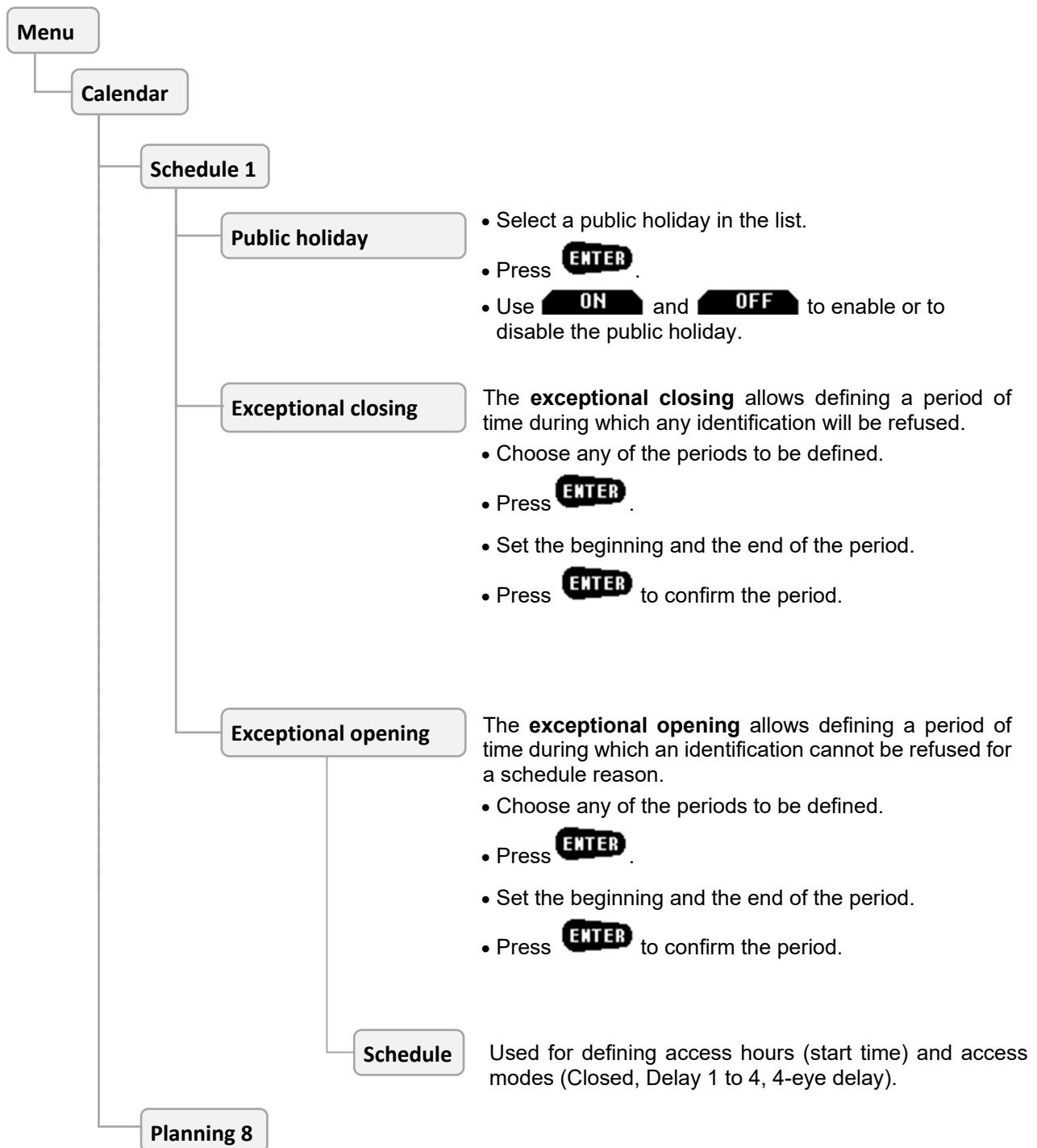


5.5 Delays configuration



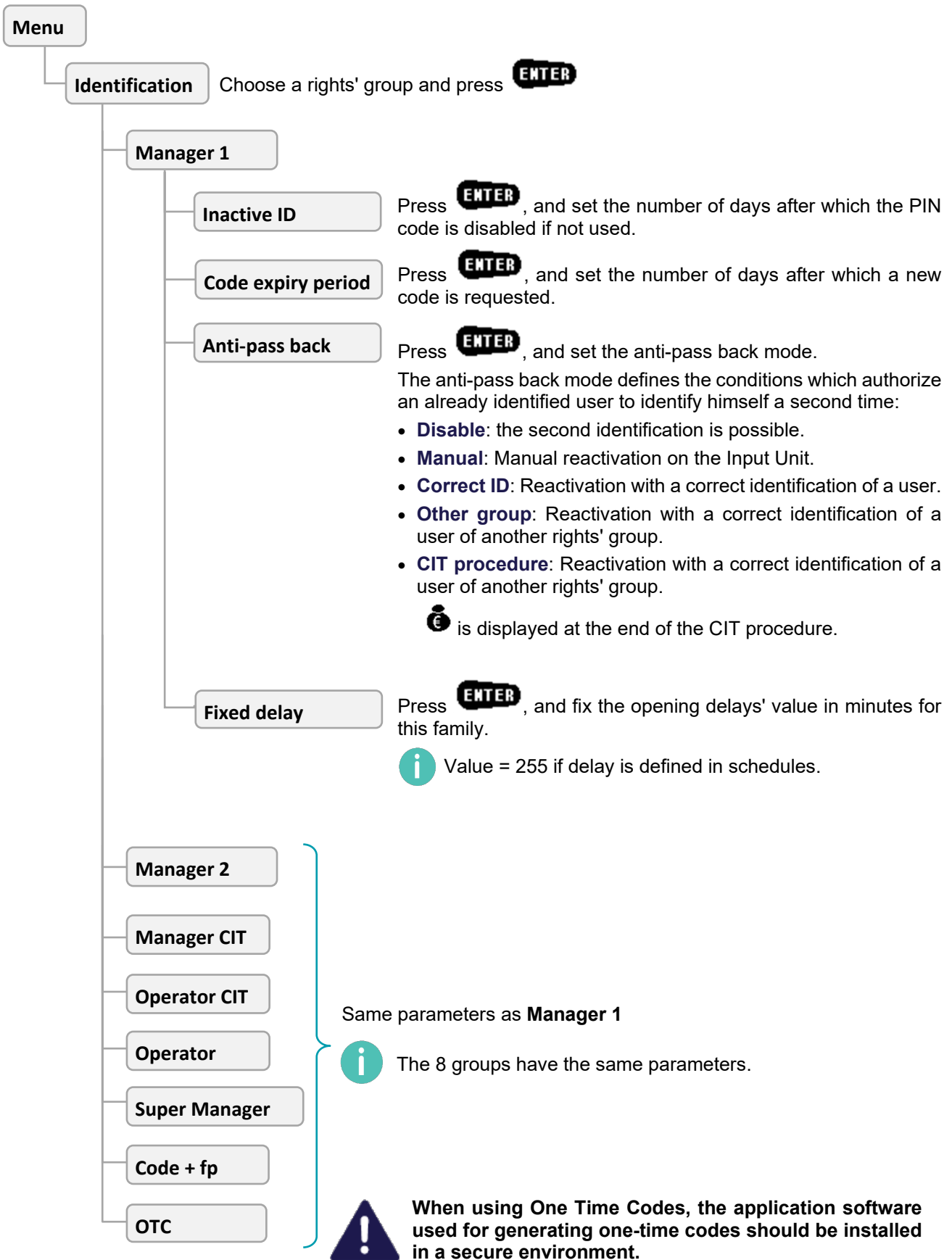
 The 8 schedules have the same parameters.

5.6 Calendar configuration

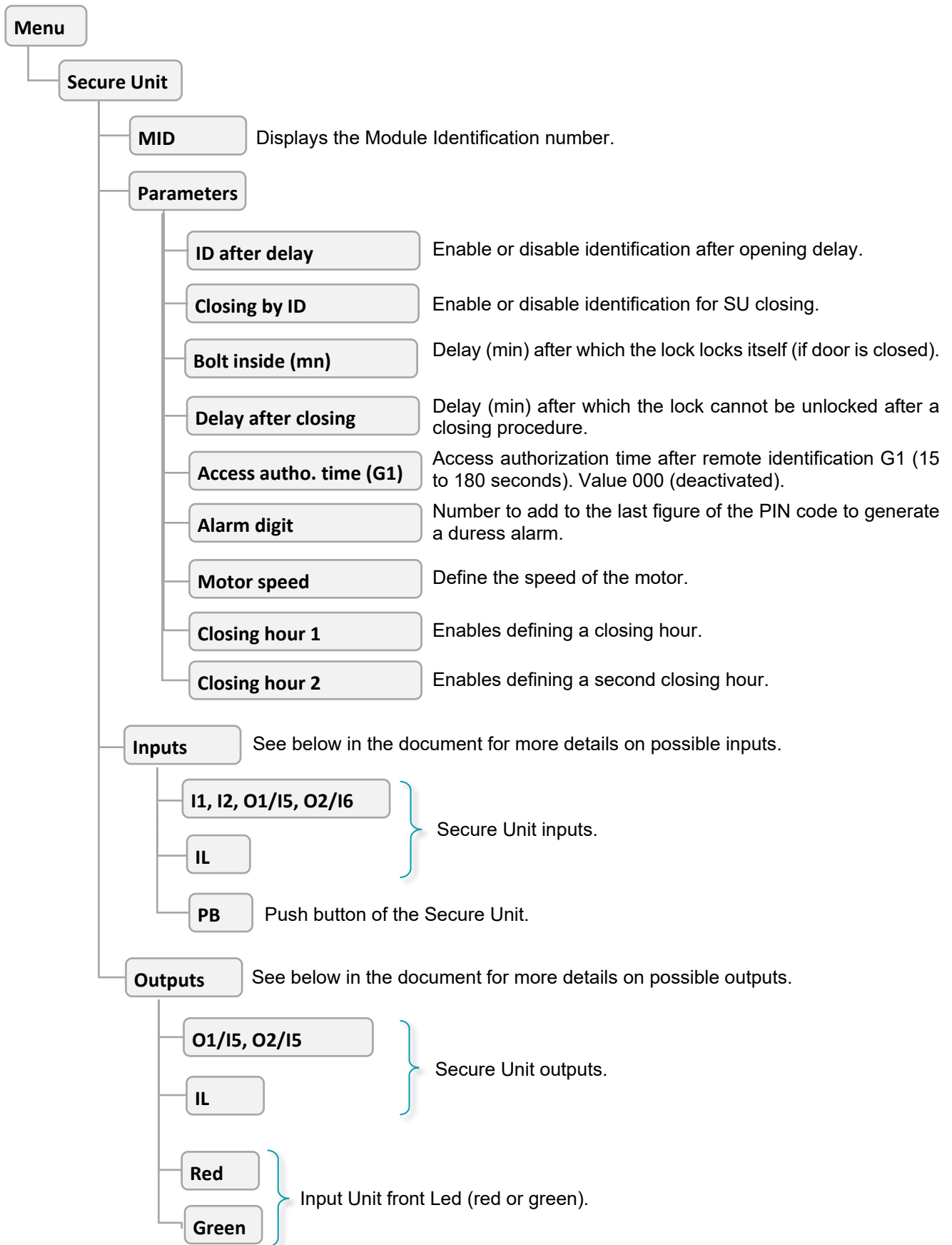


The 8 schedules have the same parameters.





5.7 Identification configuration




5.8 Secure Unit configuration



Inputs functions list

N	Function
1	<p>Opening command Launches an opening procedure (if the lock is not certified).</p>
2	<p>Boltwork switch This input is activated when the lock is locked. The Input Unit will display: .</p>
3	<p>Alarm input signal Input for an alarm signal, for example "Opening, Seismic and Thermal Detection alarm input signal".</p>
4	<p>G1-Access authorisation This function is only valid if time "Access authorization (G1) has a value between 15 and 180 seconds. When the input is deactivated, access is blocked. When the input is activated (and during 2 minutes after deactivation), access is authorized. This function is used for an opening procedure or to access to menu from the input unit.</p> <p> Be careful when using procedure G1: it can block a lock if the G1 authorization command does not work.</p>
5	<p>G2-Opening without delay When the input is activated (and during 2 minutes after deactivation), the opening procedure is done without delay.</p>
6	<p>G3-Opening cancellation When the input is activated, the current delay is cancelled and the opening is not possible.</p>
7	<p>G4-Delay substitution When the input is activated (and during 2 minutes after deactivation), the delay before opening is the substitution delay.</p>
8	<p>Duress remote button Duress alarm is activated if the remote button is not activated during the delay. More precisely, the button shall be activated:</p> <ul style="list-style-type: none"> ○ After 5 seconds after the delay starts. ○ Before 5 seconds before the end of the delay.
9	<p>Opening suspension If the input is activated, at the end of delay:</p> <ul style="list-style-type: none"> ○ The Input Unit displays for this door:  . ○ The bolt return is suspended. ○ The second identification is suspended too. <p>When the input state changes, the opening procedure can restart.</p>
10	<p>No delay – No schedule When this input is activated, the opening does not take into account schedules, and the delay before opening is null.</p>
11	<p>Interlocking input When this input is activated, the opening is forbidden.</p>

 By default, all inputs are open.

Outputs functions list

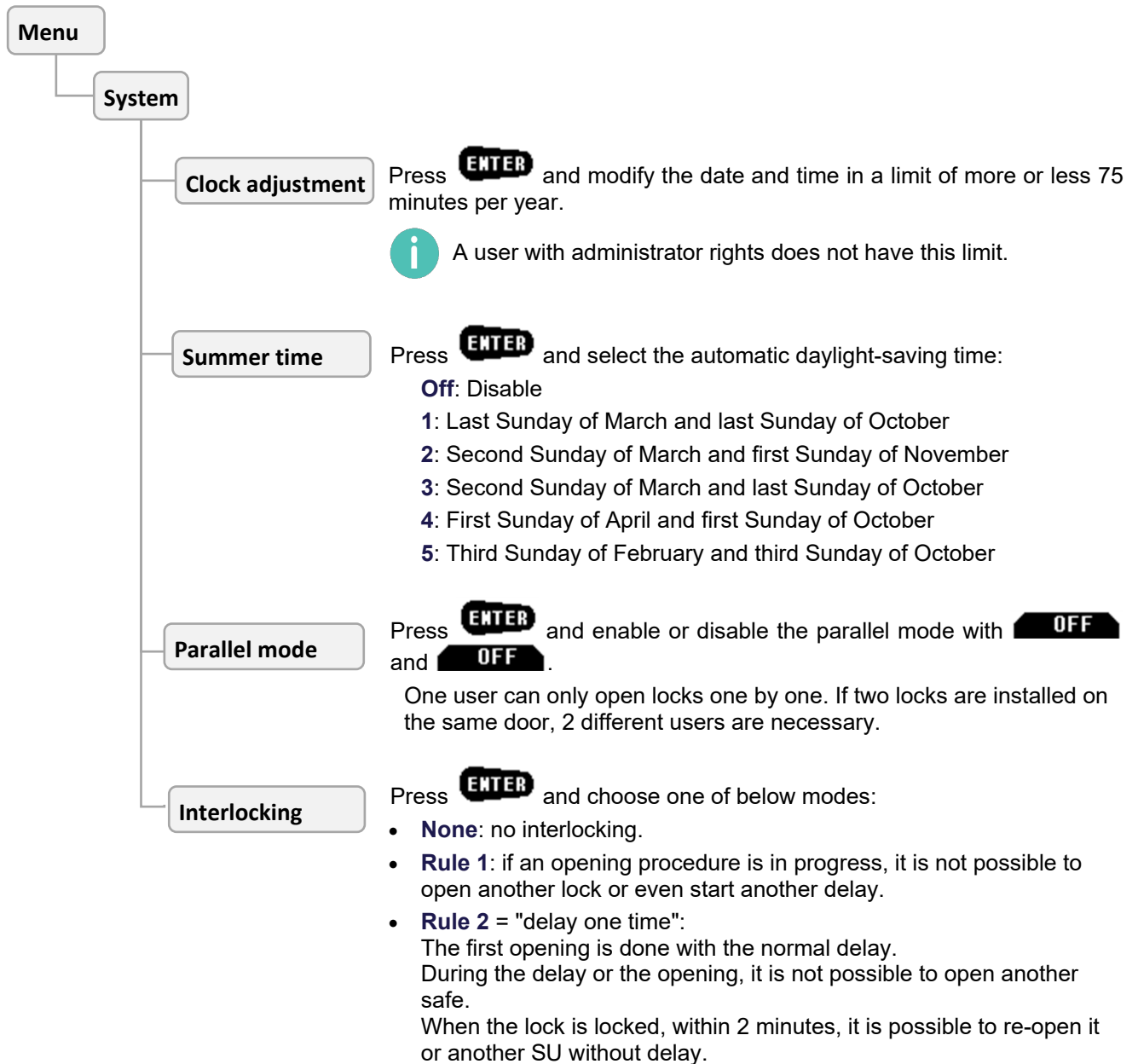
N	Functions
1	<p>Bolt fully retracted</p> <p>This output is activated when the bolt is fully retracted.</p>
2	<p>External alarm management</p> <p>This output is activated when the bolt is not locked. This output is used for example inhibit an OSTD alarm.</p>
3	<p>Good identification</p> <p>This output is activated during 3 seconds after a good identification (open procedure or menu access).</p>
4	<p>Delay in progress</p> <p>This output is activated during the delay before opening.</p>
5	<p>End of delay</p> <p>This output is activated at the end of the delay and:</p> <ul style="list-style-type: none"> • During waiting for a second code. • Or when if there is an open suspension. • Or during interlocking if this one is activated.
6	<p>Duress alarm</p> <p>This output is activated after a duress alarm and for a programmable time, by default 3 seconds.</p>
7	<p>Blocked bolt alarm</p> <p>This output is activated when there is a bolt defect during locking or during unlocking.</p>
8	<p>Door open too long</p> <p>This output is activated when the door is open for too long. This time is defined by the parameter “Door opening time” added to time “Alert after door opening time”.</p>
9	<p>Alarm output signal</p> <p>This output follows the “Alarm input signal” state except when the bolt moves and when the door is unlocked. The output is kept activated during 20 seconds after the “Alarm input signal” disappears.</p>
10	<p>Wrong identification blocking</p> <p>This output is activated when there are more than 3 false identifications. The output is deactivated when there is a good identification.</p>
11	<p>Schedule blocking</p> <p>This output is activated when users are blocked (by schedules or by holidays or by exceptional closing).</p>
12	<p>Unlock command</p> <p>= Remote relay function. This output is activated when the open procedure is done by a user who has the “Right to control remote output”. The output is deactivated when the bolt is locked again.</p>
13	<p>Sound alert</p> <p>This output is activated when the door is open for too long. This time is defined by the parameter “Door opening time”. The output is deactivated when the door is closed. The maximum time of activation is defined by the parameter “Alert after door opening time”.</p>
14	<i>Reserved</i>
15	<p>Power off alarm</p> <p>This output is activated after power off. The output is deactivated after the next good identification.</p>
16	<i>Reserved</i>

N	Functions
17	<i>Reserved</i>
18	Interlocking output This output is activated when the bolt is not locked.
19	Low battery level This output is activated if the battery level is lower than 6.3V.
20	External power OK This output is activated if the power level is more than 11V.
21	Access refused (G1) This output is activated as long as there is no access authorization by the G1 procedure.

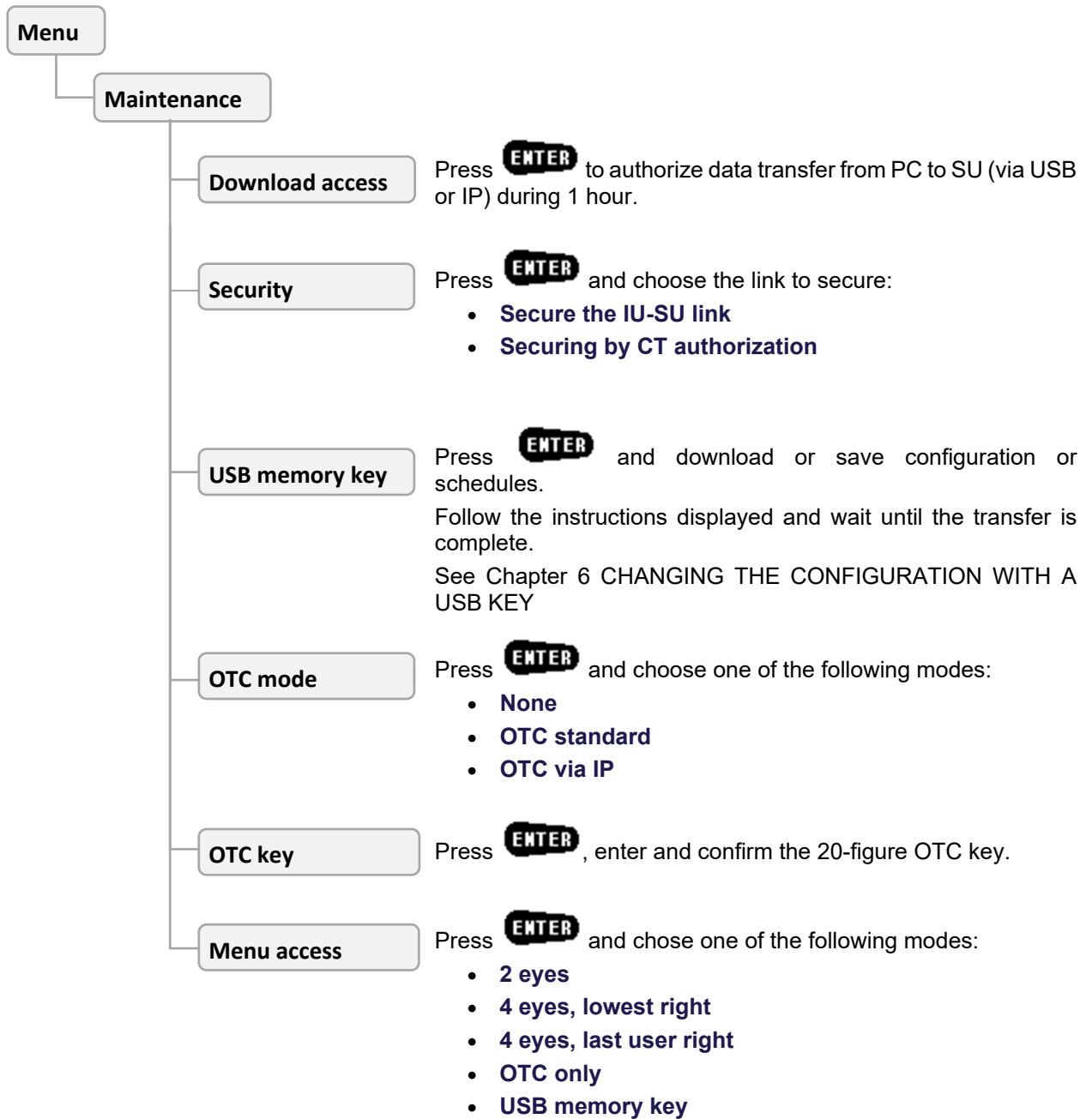


By default, the output state is disabled.

5.9 System configuration

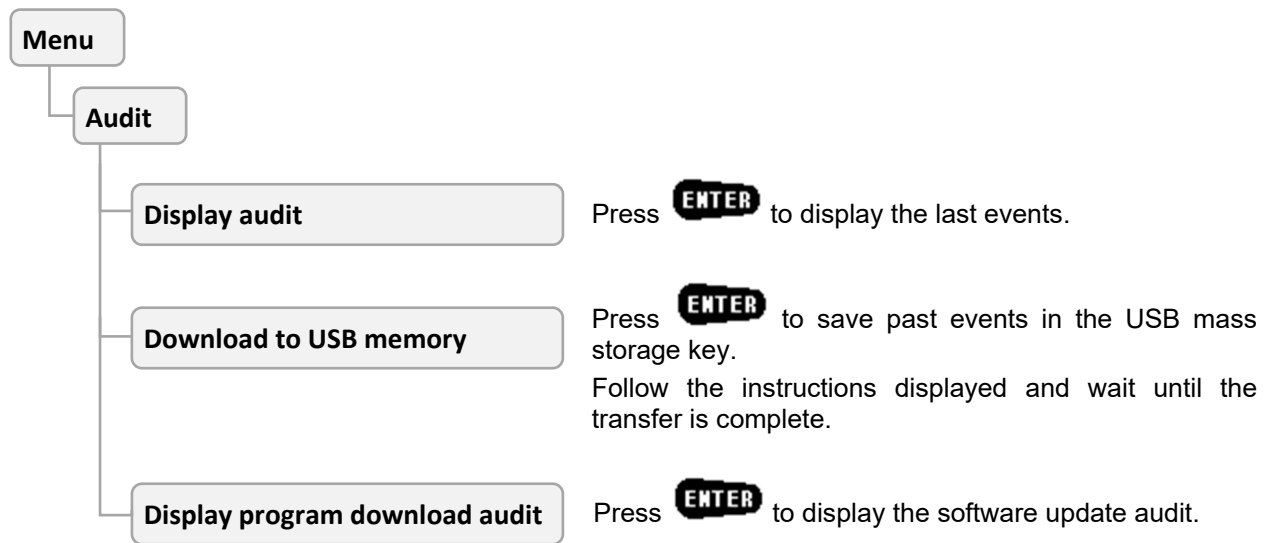


5.10 Maintenance



When using One Time Codes, the application software used for generating one time codes should be installed in a secure environment.

5.11 Audit



One USB key can be used to save several audits of different locks.



Only use USB keys with a FAT32 file system.

6 CHANGING THE CONFIGURATION WITH A USB KEY

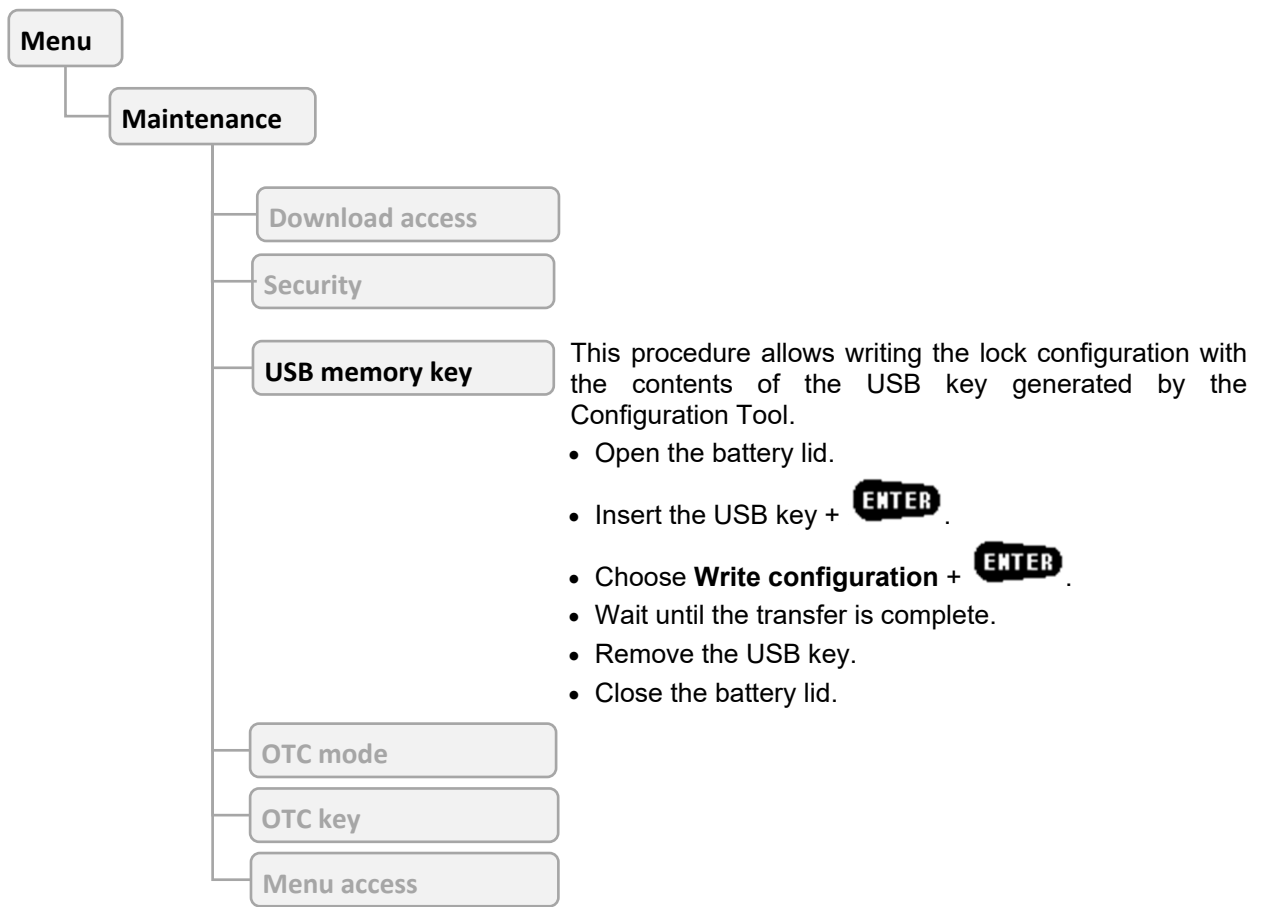
6.1 Introduction

It is possible to download a configuration to the KelNet lock with an USB key which contains a new configuration made with the Configuration Tool.

And it is possible to save the KelNet lock configuration on a USB key to manage it with the Configuration Tool.

6.2 Writing configuration with a USB key

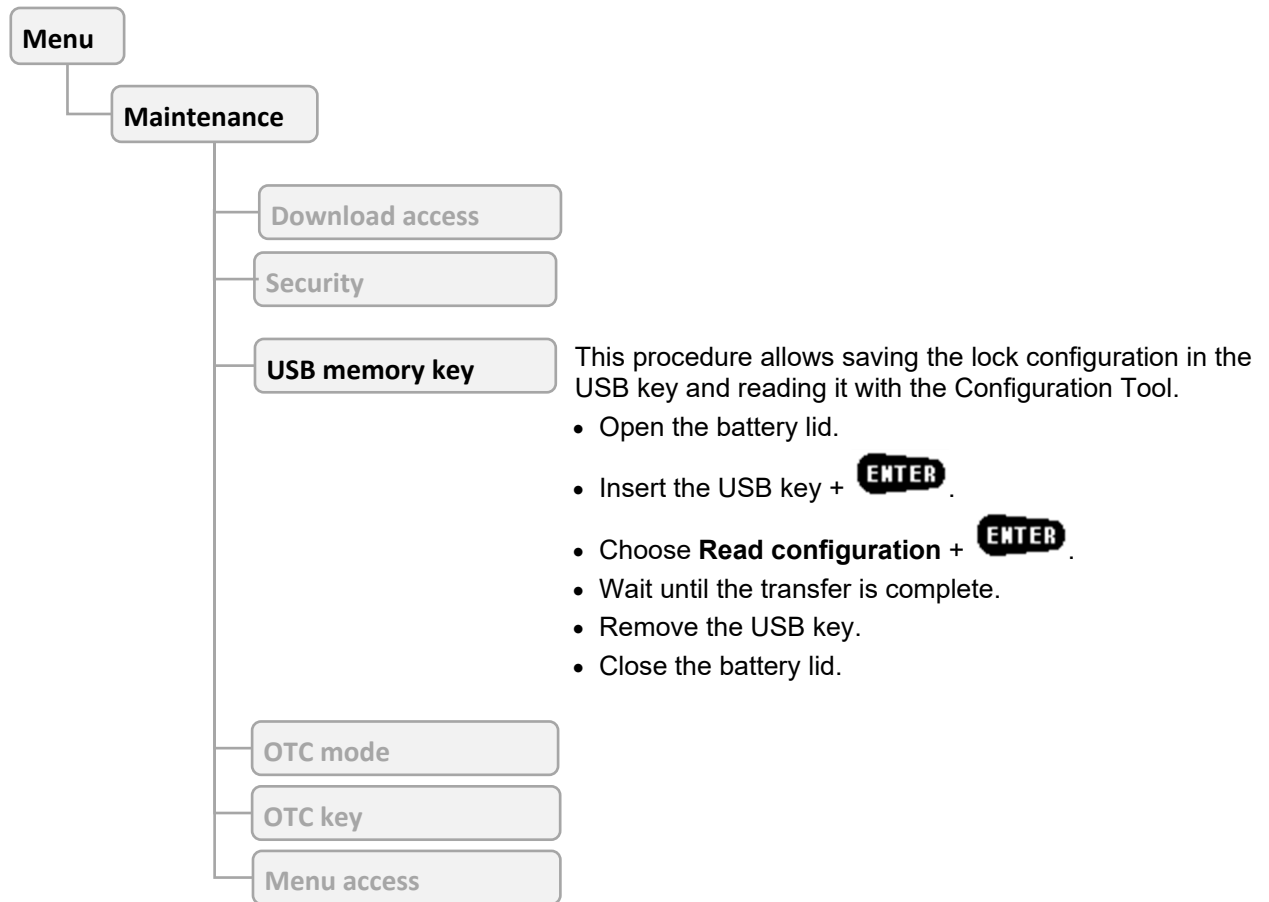
To access USB menus, the user must have rights to manage the configuration with a USB key.



The new configuration is taken into account immediately.

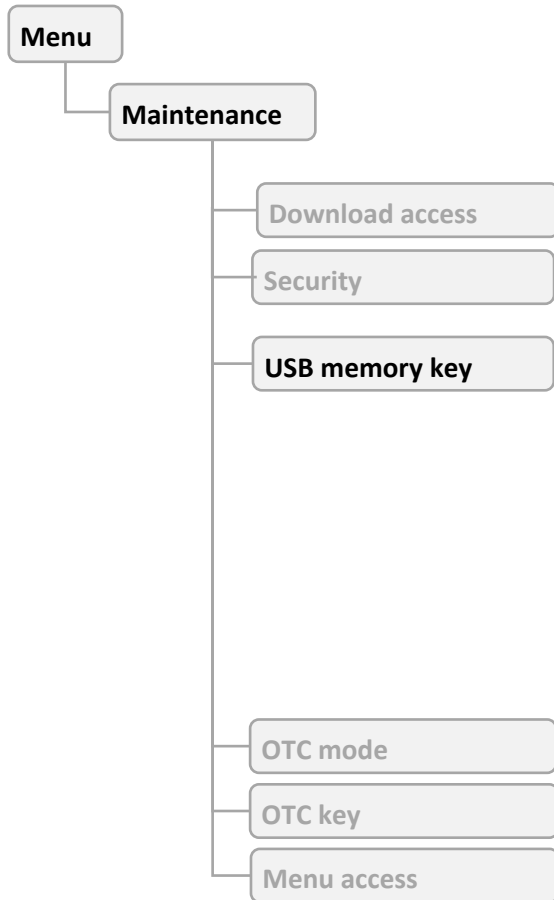
6.3 Reading configuration and saving on a USB key

To access USB menus, the user must have the rights to manage the configuration with a USB key.



6.4 Writing schedules with a USB key

To access USB menus, the user must have the rights to manage the configuration with a USB key.



This procedure allows updating schedules with the contents of the USB key generated by the Configuration Tool.

- Open the battery lid.
- Insert the USB key + **ENTER**
- Choose **Write schedules** + **ENTER**
- Wait until the transfer is complete.
- Remove the USB key.
- Close the battery lid.

6.5 Reading schedules and saving on a USB key

To access USB menus, the user must have the rights to manage the configuration with a USB key.



This procedure allows saving schedules in the USB key and reading it with the Configuration Tool.

- Open the battery lid.
- Insert the USB key + **ENTER**.
- Choose **Read schedules** + **ENTER**.
- Wait until the transfer is complete.
- Remove the USB key.
- Close the battery lid.

7 FINGERPRINT

Fingerprint identification is always linked to a PIN code.

The biometric enrolment requires two different fingers to be registered.



When installing an Input Unit, it is important to delete all fingerprints via the **Technician menu** (See §4.2). This allows initialization of biometrics.

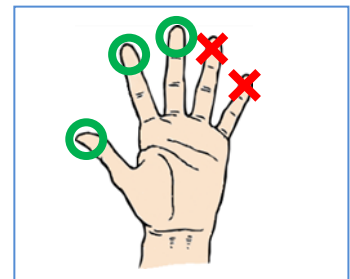


Only 25 users can be configured in fingerprint mode.



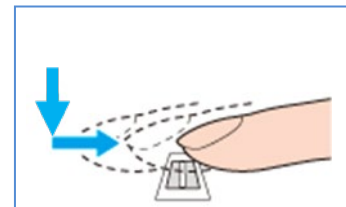
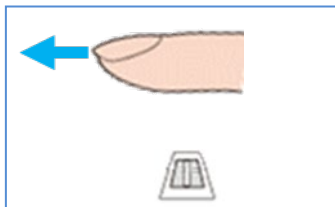
7.1 Instructions for enrolling fingerprints

- In order to get a better enrolment and read success rate, it is better to avoid using smaller fingers (ring/little fingers).
- Do not lift your finger off the biometric sensor as you move your finger over it.
- Enrolling or reading the fingerprint may fail if you move your finger too quickly or too slowly.
- Avoid twisting or rotating your finger as you move it over the sensor.
- Positioning of the finger for optimum operation:



1. Push your finger in up against the stop without touching the biometric sensor.

2. Ensure even pressure over the biometric sensor, sliding the finger towards the outside.



7.2 Enrolment in mode “Code + Fingerprint”

In this mode, the user can enrol his fingerprint himself.

This procedure is done automatically the first time the user carries out an access procedure:

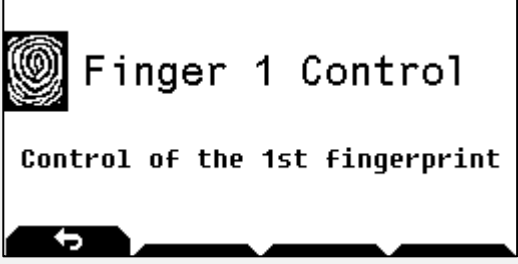
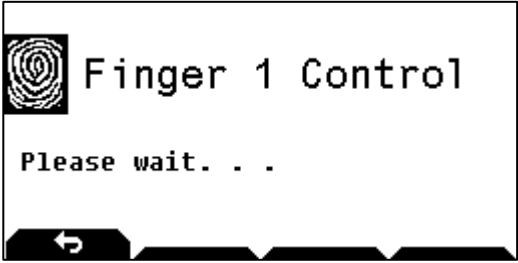

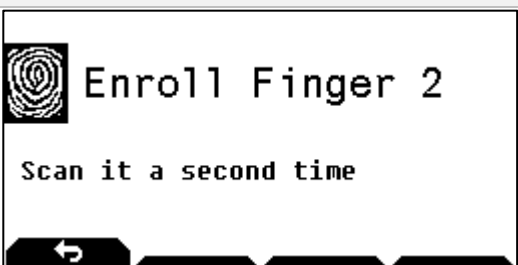
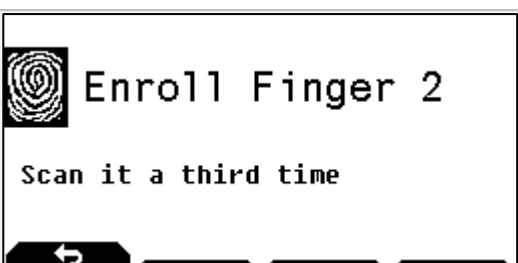
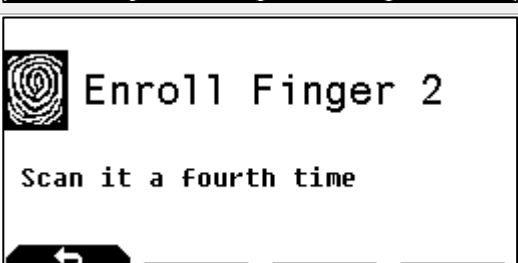
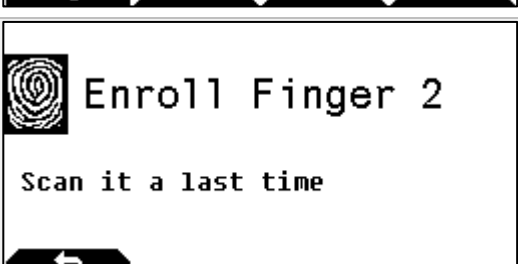
1. Select the Secure Unit + **ENTER**
2. Enter your ID + **ENTER**
3. Enter your PIN code + **ENTER**
4. Press **ENTER** key: if this code is being used for the first time, you are prompted to change it (See §3.11), then repeat the access procedure by entering your new code.
5. The enrolment procedure starts (see §7.3).

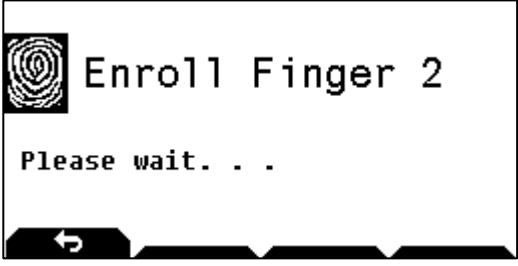
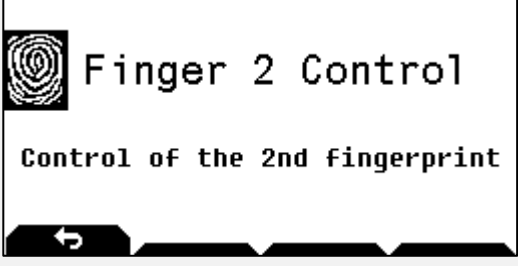
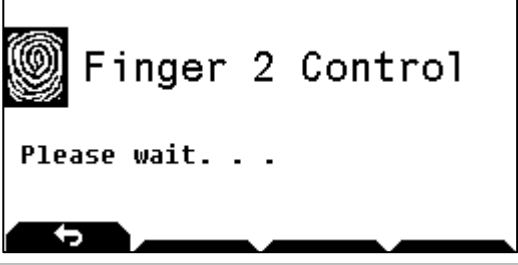
7.3 Enrolling procedure

The fingerprint enrolling is done in two steps:

1. 5 successive readings of the same fingerprint to create an image.
2. Check the image created with a fingerprint check.

Step	Screen	Description
1		Scan your first finger for the first time
2		Scan your first finger for the second time
3		Scan your first finger for the third time
4		Scan your first finger for the fourth time
5		Scan your first finger for the last time
6		Wait while the fingerprint is created and saved.

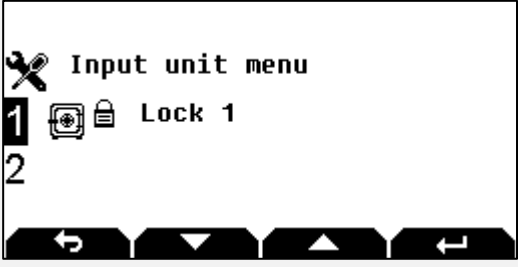


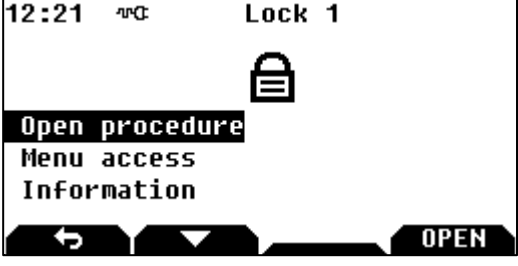
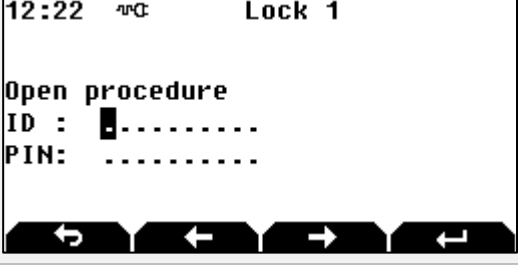
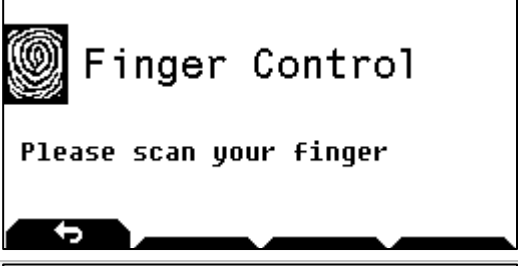
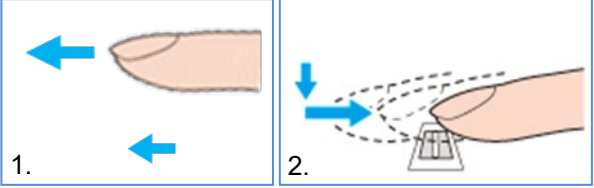
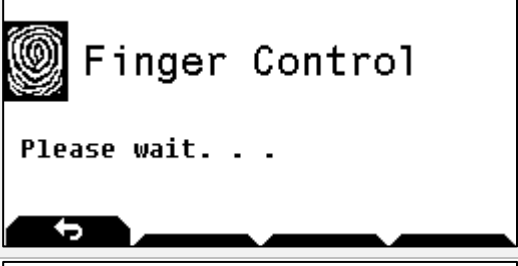
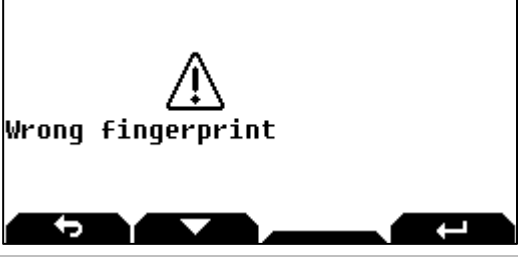
Step	Screen	Description
7	 <p>Finger 1 Control Control of the 1st fingerprint</p>	Scan your first finger to control the fingerprint creation.
8	 <p>Finger 1 Control Please wait. . . .</p>	Wait during verification.
9	 <p>Enroll Finger 2 Scan your second finger</p>	Scan your second finger for the first time
10	 <p>Enroll Finger 2 Scan it a second time</p>	Scan your second finger for the second time
11	 <p>Enroll Finger 2 Scan it a third time</p>	Scan your second finger for the third time
12	 <p>Enroll Finger 2 Scan it a fourth time</p>	Scan your second finger for the fourth time
13	 <p>Enroll Finger 2 Scan it a last time</p>	Scan your second finger for the last time

Step	Screen	Description
14		Wait while the fingerprint is created and saved.
15		Scan your second finger to control the fingerprint creation.
16		Wait during verification.



If there are several Input Units at the site, enrolment will need to be performed at each Input Unit.




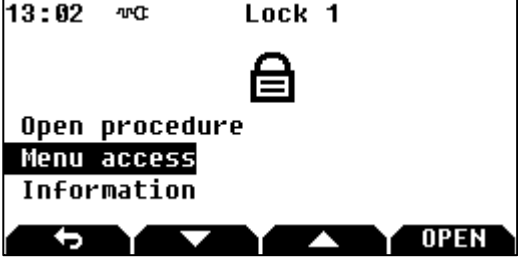


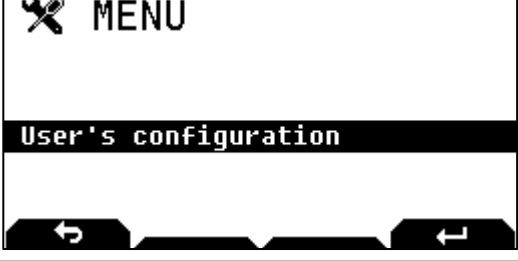
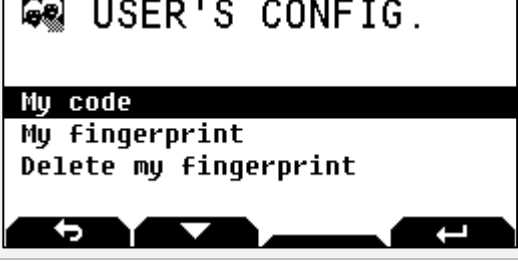

7.4 Opening procedure with fingerprint

Step	Screen	Description
1		Select the lock + ENTER Note: to select another lock, use arrows  and  .
2		Press ENTER or the OPEN button to start the Open procedure.
3		Enter your ID + ENTER Enter your PIN code + ENTER
4		Swipe your finger over the biometric sensor. 
5		Wait while the fingerprint is compared with the one recorded. If the fingerprint is correct, the opening procedure continues (bolt opening, start delay, etc.).
6		Error message if the fingerprint is not correct. The opening procedure must be restarted.



The fingerprint identification can also be used to access menus.

7.5 Changing the fingerprint by the user himself

Step	Screen	Description
1	 <p>The screen displays 'Input unit menu' with a wrench icon. Below it, 'Lock 1' is highlighted with a '1' in a box. There are navigation arrows at the bottom.</p>	<p>Select the lock + ENTER</p> <p>Note: to select another lock, use arrows  and .</p>
2	 <p>The screen shows '13:02' and 'Lock 1' at the top. A padlock icon is in the center. Below it, 'Open procedure' is shown with a list: 'Menu access' (highlighted), and 'Information'. There are navigation arrows and an 'OPEN' button at the bottom.</p>	<p>Use arrow  to select Menu Access + ENTER</p>
3	 <p>The screen shows '13:04' and 'Lock 1'. Below 'Access to menu', there are two input fields: 'ID : ' and 'PIN: ' with a cursor in the first field. There are navigation arrows at the bottom.</p>	<p>Enter your ID + ENTER</p> <p>Enter your PIN code + ENTER</p> <p>Follow the instructions for the fingerprint control.</p>
4	 <p>The screen displays 'MENU' with a wrench icon. Below it, 'User's configuration' is highlighted. There are navigation arrows at the bottom.</p>	<p>Press ENTER</p>
5	 <p>The screen shows 'USER'S CONFIG.' with a person icon. Below it, a list includes 'My code', 'My fingerprint' (highlighted), and 'Delete my fingerprint'. There are navigation arrows at the bottom.</p>	<p>With arrow  select My fingerprint + ENTER</p> <p>And follow the procedure to enrol fingerprint (See "Fingerprint" chapter).</p>



If there are several Input Units at the site, enrolment will need to be performed at each Input Unit.

7.6 Deleting a fingerprint by the user himself

Step	Screen	Description
1		<p>Select the lock + ENTER</p> <p>Note: to select another lock, use arrows and .</p>
2		<p>Use arrow to select Menu Access + ENTER</p>
3		<p>Enter your ID + ENTER</p> <p>Enter your PIN code + ENTER</p> <p>Follow the instructions for the fingerprint control.</p>
4		<p>Press ENTER</p> <p>For a user without fingerprint identification go to step 5 otherwise go to step 6.</p>
5		<p>Use arrow to select Delete my fingerprint + ENTER</p>
6		<p>Confirm deletion with YES button or abort deletion with NO button.</p>

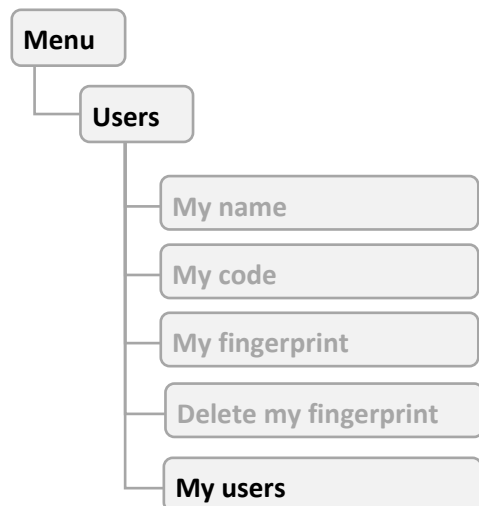


In “Code + fingerprint” mode, if the user leaves the enrolling procedure, the procedure is started automatically the first time the user carries out an opening procedure.



If there are several Input Units at the site, the fingerprint will need to be deleted from each Input Unit.

If the user does not have the right to change his PIN code, the manager (or super-manager) deletes the user fingerprint:



- Press **ENTER**, select **Delete fingerprint** with **ENTER**.
- Confirm the deletion with **YES** or **NO** to abort it.



The different parameters are available in accordance with the user's rights.

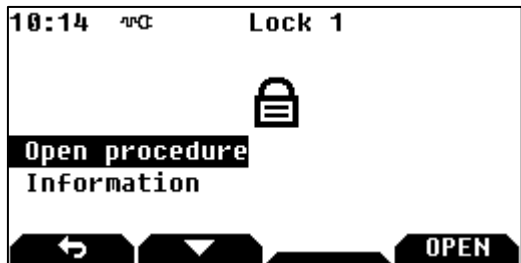
7.7 Deleting all fingerprints

See section 4.2.

8 REDUNDANT LOCK SPECIFICITIES

The redundant lock works in the same way as the standard lock.

In case of a malfunction of a part of the lock, access to the menu is no longer possible and therefore when selecting the lock, the following screen is displayed:



When the opening procedure is selected, the following error message appears:



The opening and closing procedures of the lock are always possible, depending on the programmed parameters.

9 FACTORY SETTINGS

The default factory settings are:

	Identification / code PIN		Rights	Opening right	Schedule
Super Manager 1	1 – 00000000	Enable	All	No	6
Manager 1	2 – 00000000	Enable	Change codes 3 to 19	Yes	1
Operator 01 to Operator 17	3 - 00000000 à 19 – 00000000	Disable	No	Yes	1
Manager 2	20 – 00000000	Disable	Change codes 21 to 29	Yes	2
Operator 1 Bio to Operator 9 Bio	21 – 00000000 à 29 – 00000000	Disable	No	Yes	2
CIT Manager	30 – 00000000	Disable	Change codes 31 to 39	Yes	3
CIT Operator 1 to CIT Operator 4	31 - 00000000 à 39 – 00000000	Disable	No	Yes	3
Super Manager 2	99 - 00000000	Disable	All	No	6

Schedules:

- Schedule 1: from 6:00 am to 10:00 pm all days.
- Schedule 2: from 6:00 am to 10:00 pm all days.
- Schedule 3: from 6:00 am to 10:00 pm all days.
- Schedule 6: from 0:00 am to 0:00 pm all days.

No annual schedule, no exceptional closed periods, no exceptional opening periods, and no public holidays are defined.

Delays:

- Open delay = 0 minute.
- Duress alarm procedure delay = 10 minutes.
- Emergency blocking delay = 30 minutes.
- Automatic blocking delay after closing procedure = 0.
- Time out for retracted bolt = 10 minutes.

General settings:

- Duress alarm mode = last digit + X (default value: 0, therefore disabled).
- Wrong identification blocking rule = "Increasing blocking time".
- No Interlocking rule.
- No "4 eyes mode"
- No closing procedure by identification.
- No re-identification after delay time out.
- No input / output function. Input I1 – Door boltwork switch

10 RECYCLING

The Secure Unit and the Input Unit can be recycled.

There are different levels of recycling:

1. Recycling the authentication keys (used for security).
2. Recycling the device's address.
3. Complete recycling of the operating settings of the lock.



The lock's audit is never wiped.

10.1 Recycling the Secure Unit's authentication keys

This procedure is for reverting to the factory authentication keys.

To recycle the Secure Unit's authentication keys, perform the following procedure:

1. Cut the power to the Secure Unit. If the USB cable is connected to the Input Unit, disconnect it.
2. Press the Secure Unit button: this wakes up the Secure Unit microprocessor and so discharges the power supply's capacitors, otherwise the microprocessor remains active and there is no restart.
3. Reconnect the power supply: the Secure Unit green LED starts to flash (10 seconds, maximum).
4. While it is flashing, press the Secure Unit push-button **twice**: the LED will start to flash more rapidly.
5. Wait until it stops flashing.

10.2 Recycling the Secure Unit's address

This procedure is for:

- Reverting back to the factory authentication keys.
- Wiping the Secure Unit's address (value 127).

Perform the following procedure:

1. Cut the power to the Secure Unit. If the USB cable is connected to the Input Unit, disconnect it.
2. Press the Secure Unit button: this wakes up the Secure Unit microprocessor and so discharges the power supply's capacitors, otherwise the microprocessor remains active and there is no restart.
3. Reconnect the power supply: the Secure Unit green LED starts to flash (10 seconds, maximum).
4. While it is flashing, press the Secure Unit push-button **5 times**: the LED remains lit and stops flashing.
5. Wait until the LED goes out.

10.3 Complete recycling of the Secure Unit

To completely recycle the Secure Unit, perform the following procedure:

1. Cut the power to the Secure Unit. If the USB cable is connected to the Input Unit, disconnect it.
2. Press the Secure Unit button: this wakes up the Secure Unit microprocessor and so discharges the power supply's capacitors, otherwise the microprocessor remains active and there is no restart.
3. Reconnect the power supply: the Secure Unit green LED starts to flash (10 seconds, maximum).
4. While it is flashing, press the Secure Unit push-button **10 times**: the LED will start to flash more rapidly, before stopping and remaining illuminated.
5. Wait until the LED goes out.

After recycling, all the settings are reset to their "factory" values (default value): see section 9.

10.4 Recycling the Input Unit's authentication keys

This procedure is for reverting to the factory authentication keys.

To recycle the Input Unit's authentication keys, perform the following procedure:

1. Cut the power to the Input Unit. If the USB cable is connected to the Input Unit, disconnect it.
2. Dismount the Input Unit.
3. Wait 5 seconds.
4. Reconnect the power supply: The Input Unit's red LED starts flashing (10 seconds, maximum).
5. While it is flashing, press the Secure Unit's push-button **twice**: the LED will start to flash more rapidly.
6. Wait until it stops flashing.
7. Put the Input Unit back together so that the anti-tear switch is activated.

10.5 Complete recycling of the Input Unit

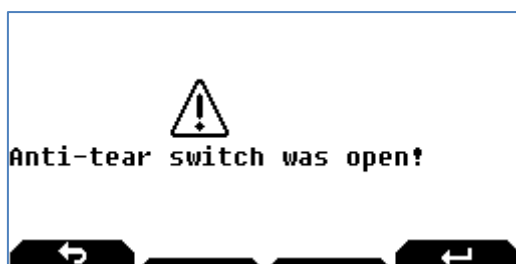
To completely recycle the Input Unit, perform the following procedure:

1. Cut the power to the Input Unit. If the USB cable is connected to the Input Unit, disconnect it.
2. Dismount the Input Unit.
3. Wait 5 seconds.
4. Reconnect the power supply: The Input Unit's red LED starts flashing (10 seconds, maximum).
5. While it is flashing, press the anti-tear switch **10 times**: the LED remains lit and stops flashing.
6. Wait until the LED goes out.
7. Put the Input Unit back together so that the anti-tear switch is activated.



As long as the anti-tear switch is open, the "**Anti-tear open**" message is displayed and only access to the Input Unit's menu is authorised.

Otherwise, the following message is displayed:



This message is displayed until there is a valid identification, but it does not prevent the Input Unit from being used.

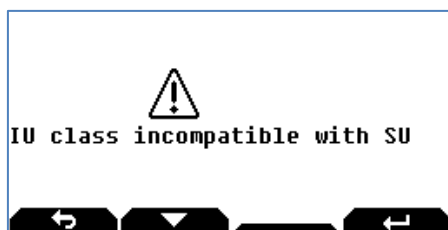
11 MAINTENANCE

11.1 Replacing an Input Unit operating in factory mode

Once the new Input Unit has been connected, perform the following procedure:


Step	Screen	Description
1		<p>Select the Technician menu + ENTER</p> <p>Note: The Technician menu is only visible if the Input Unit's anti-tear switch is open.</p>
2		<p>Configure the Input Unit's address (17 for the 1st Input Unit) and the bus type: RS485 or MF2.</p>
3		<p>Select the SU validation menu and switch the locks present to ON.</p>
4		<p>Then return to the home screen.</p> <p>The lock is once again operational.</p>

i If the Input Unit's class is A or B and the Secure Unit's class is C or D, it will not be possible to either open the lock or enter the Input Unit's configuration menu. The following message is displayed:



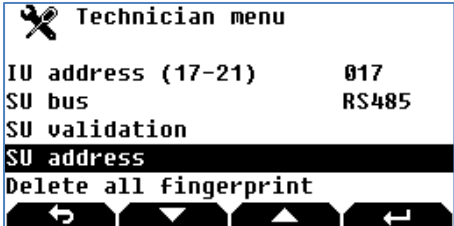


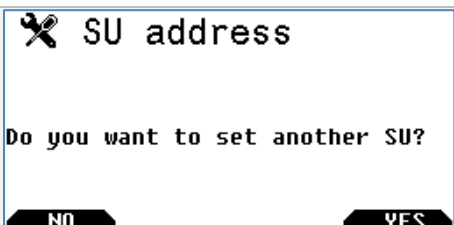


11.2 Replacing a Secure Unit operating in factory mode

If a Secure Unit has to be changed, you must first access to it.

 The new Secure Unit must have the "factory" configuration. If this is not the case, the Secure Unit will need to be recycled.

Once the new Secure Unit has been connected, perform the following procedure:

Step	Screen	Description
1		Select the Technician menu +  Note: The Technician menu is only visible if the Input Unit's anti-tear switch is open.
2		Select the SU address menu.
3		Press the Secure Unit's push-button.
4		Enter the same address as the one used for the lock that has been dismantled (from 1 to 16), then validate.
5		As there are no other SUs to change, press NO .

The Secure Unit then needs to be reconfigured and all of the user codes entered.

12 GLOSSARY

4 eyes mode

For this mode, two different users have to identify in order to validate an opening procedure or validate access to the menus.

Angular filter

Optical filter placed on the display to limit the angular view (necessary for grade C).

Approval

Certification rate of the device. Under certain conditions, the approval can be lost (identification with fingerprint only for example).

Audit

Chronological journal of events (also: "event log").

Biometric code

Code comprising human characteristics (fingerprint).

Bolt (or blocking feature)

Part of a HSL which, after inputting the correct opening code, moves, or can be moved, to either secure a door or prevent movement of boltwork.

Boltwork

Blocking feature of a door. A boltwork switch informs if the door can be opened or not.

Centre national de prévention et de protection (CNPP)

National centre for risk prevention and protection.

CIT - Cash In Transfer

The transport, delivery and receipt of valuables.

Code

Identification information required which can be entered into a HSL and which, if correct, enables the security status of the lock to be changed.

CT - Configuration Tool

Software running on PC which is used to configure all the parameters of the HSL.

Door status

The normalized status of a HSL door are:

- **Closed door:** door is within its frame ready for throwing its bolt(s).
- **Bolted door:** bolts are thrown.
- **Locked door:** boltwork cannot be withdrawn because of the HSL.
- **Secured door:** door is closed, bolted and locked with an HSL in the secured HSL condition.

Duress code

Parallel code which initiates some additional function (delay modification, alarm).

Event log

Chronological journal of events (also: audit).

G1 – Procedure G1

When a "procedure G1" is configured for an SU, identifications are not authorized. Activating this procedure authorizes Access during an adjustable time (15 to 180').

G2 – Procedure G2

When a "procedure G2" is configured for an SU and activated, the opening delay is cancelled.

G3 – Procedure G3

When a "procedure G3" is configured for an SU and activated, the current procedure is cancelled.

G4 – Procedure G4

When a "procedure G4" is configured for an SU and activated, the opening delay is replaced by a "substitution" delay.

HSL - High Security Lock

Independent assembly normally fitted to doors of secure storage units, into which codes can be entered for comparison with memorized codes (processing unit). A correct match of an opening code allows movement of a blocking feature.

ID - Identification

Method to identify a user. For KelNet, the ID is a number between from 1 to 99 for a user known by the Secure Unit. For an OTC code, the ID is defined over 4 or more digits.

Interlocking rule

Rules which define the conditions to validate an opening procedure.

IOBox - Input Output Box

Interface board used to extend the number of inputs and outputs.

IPBox

Interface device which is used to convert a serial link RS485 to Ethernet.

IU - Input Unit

Part of an HSL which communicates codes to a processing unit.

MF2

Name of the bus/protocol used between the Input Units and the Secure Units of the KelNet lock.

OSTD -Opening Seismic and Thermal Detection

Opening, seismic and thermal detection alarm input signal.

OTC - One Time Code

Code which is limited in time and in number of use.

PIN - Personal Identification Number

Password used to identify a person.

Recycling

Procedure to initialize a device with factory parameters.

Remote SU button

This button is used to fix the address of the SU.

SU - Secure Unit

Part of a HSL which evaluates whether the input code is correct and enables or prevents movement of a locking device.

SW - Switch

Interrupteur permettant par exemple de détecter une attaque sur le boîtier d'un périphérique.

USB -Universal Serial Bus

Standard serial bus to interface devices to a host computer.