



EN

User Manual

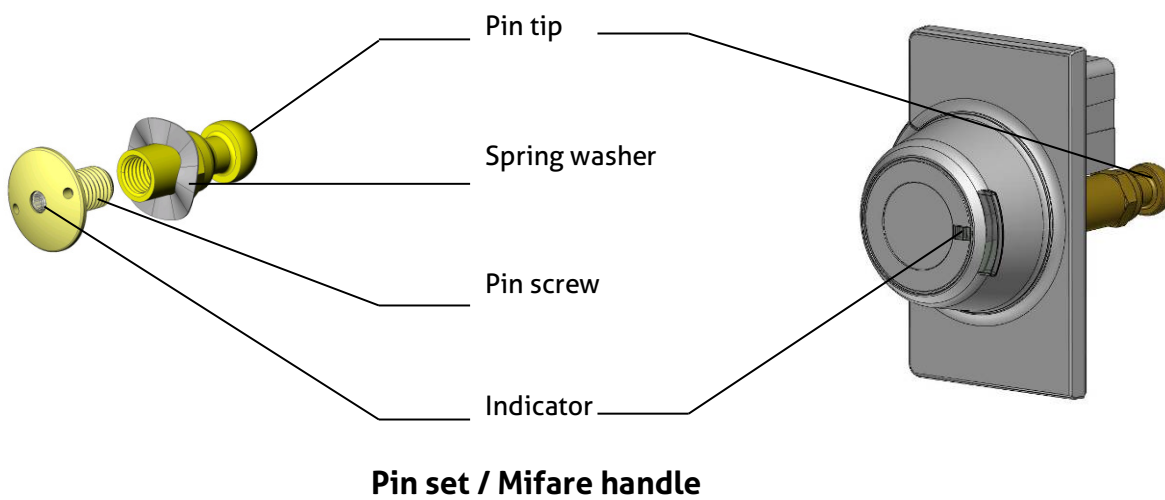
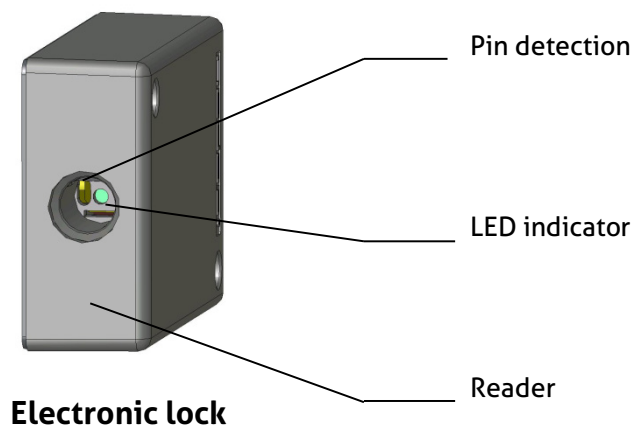
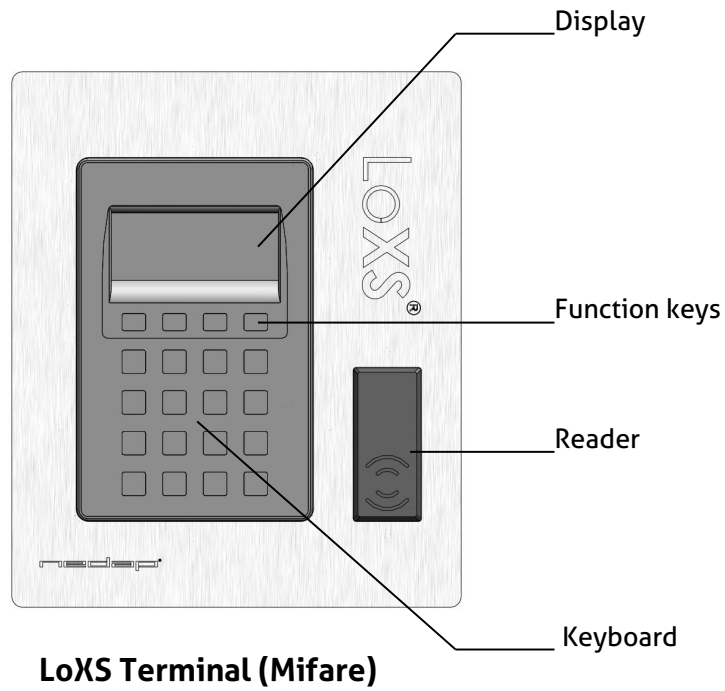
LoXS IV

Version 10

| 04-01-2022



Date	Version	Changes
04-01-2022	10	Update locker and reader firmware
15-06-2017	9	Lay-out
11-05-2016	8	
12-08-2015	7	
	...	





Contents

PREFACE	7
INTRODUCTION	8
1. THE SYSTEM	8
1.1. HARDWARE OUTLINE	8
1.2. THE LOXS TERMINAL	9
1.3. THE ELECTRONIC LOCK	9
1.4. ELECTRONIC KEYS	10
2. OPERATION WITH ELECTRONIC KEY	11
2.1. PRINCIPLE	11
2.2. TERMINAL ALLOCATES LOCKER – STANDARD MODE	11
2.3. SELECT THE LOCKER YOURSELF - TOGGLE MODE	12
2.4. OPERATING THE LOCKER UNIT SMART WITH ELECTRONIC KEYS	13
3. OPERATION WITH PIN CODE	14
3.1. PRINCIPLE	14
3.2. TERMINAL ALLOCATES LOCKER	14
3.3. SELECT THE LOCKER YOURSELF (PIN-TOGGLE MODE)	16
3.4. COIN ACCEPTOR (THIRD PARTY)	17
4. OPERATION WITH THIRD-PARTY KEYS	19
4.1. PRINCIPLE	19
4.2. TERMINAL ALLOCATES LOCKER	19
4.3. SELECT A LOCKER YOURSELF	20
ADMINISTRATOR SECTION	21
5. THE ADMINISTRATOR MENU	21
5.1. LOCKER MANAGEMENT	21
5.2. KEY MANAGEMENT	22
5.3. RELEASE ALL LOCKERS	23
6. FREQUENTLY ASKED QUESTIONS	25
ENGINEER SECTION	26
7. INSTALLATION MENU	26
7.1. BASIC SETUP	26
7.1.1 DEFAULT LANGUAGE	26
7.1.2 OPERATING MODE	27
7.1.3 STATUS FREE LOCKER	27
7.1.4 PIN CODE	27
7.1.5 USE OF COINS	27



7.1.5.1	COINS TIME BASED	27
7.1.6	COINS RENT	27
7.1.7	COINS DEPOSIT	28
7.1.8	HOPPER PRESENT	28
7.1.9	AUTOMATIC RELEASE	28
7.1.10	SAVE CHANGES	28
7.2.	HARDWARE CONFIGURATION	29
7.2.1	LOCKER UNIT	29
7.2.2	INFO READER	30
7.2.3	IN READER	30
7.2.4	OUT READER	30
7.2.5	UNLOCK READER	31
7.2.6	DUMMY READER	31
7.3.	ADVANCED SET-UP	32
7.3.1	SECOND LANGUAGE	33
7.3.2	THIRD LANGUAGE	33
7.3.3	UNLOCK TIME (LONG)	33
7.3.4	UNLOCK TIME (SHORT)	33
7.3.5	ALARM TIMEOUT	33
7.3.6	DELAYED DEASSIGN	33
7.3.7	ENABLE WHITE LIST	33
7.3.7.1	AFTER RELEASE ALL	34
7.3.8	AEOS COMPATIBLE	34
7.3.9	ASSIGN UPON 'HAVE'	34
7.3.10	LOCKER RELEASE MENU	34
7.3.11	ENABLE IN USE LED	34
7.3.12	LED INTENSITY	34
7.3.13	SETUP NEDAP CONFIG	34
7.3.13.1	ENABLE NEDAP	35
7.3.13.2	ENABLE EM4102	35
7.3.13.3	ENABLE RW80	35
7.3.13.4	LF FIELDSTRENGTH	35
7.3.13.5	LED STYLE	35
7.3.14	THIRD PARTY READER	35
7.3.15	SETUP MIFARE CONFIG	37
7.3.15.1	CFG: <NAME>	37
7.3.15.2	CSN	37
7.3.16	CONTRAST	37
7.3.17	SAVE CHANGES	37
7.4.	UPDATE LOCKER AND READER FIRMWARE	38
7.4.1	FORCE DOWNLOAD	39
7.5.	ASSIGN SYSTEM ADDRESSES TO LOCKERS	40
7.6.	NETWORK SETUP	40
7.6.1	IP-ADDRESS	40
7.6.2	NETMASK	41
7.6.3	GATEWAY	41
7.6.4	MAC-ADDRESS	41
7.6.5	SAVE CHANGES	41
7.7.	RESET MENU	42
7.7.1	NOTHING (RESTART)	42
7.7.2	TERMINAL SETUP	42
7.7.3	LOCKERS CONFIG	42
7.7.4	RESET LOCKER SMART ADDRESSES	42
7.7.5	KEYS DATABASE	42



7.7.6	NEDAP ID FILTER	43
7.7.7	THIRD PARTY ID FILTER	43
7.7.8	MIFARE CONFIG	43
7.7.9	ALL (FACTORY DFLT)	43
7.7.10	RESTART NOW?	43
7.8.	SET TIME	44
7.9.	THIRD PARTY ID FILTER	45
APPENDIX 1	TERMINAL CONNECTIONS	46
APPENDIX 2	INSTALLATION SCHEMATIC	47
APPENDIX 3	LOCKERBUS	48
APPENDIX 4	CABLE TESTING	49
APPENDIX 5	ADDRESSING LOCKER UNITS	50
APPENDIX 6	ASSEMBLY RULES FOR THE LOXS TERMINAL	52
APPENDIX 7	DIMENSIONAL SKETCHES	52
APPENDIX 8	ELECTRONIC KEYS	52
APPENDIX 9	TECHNICAL SPECIFICATIONS	53
APPENDIX 10	CONFIGURATION SHEET	56



Preface

Nedap LoXS is an electronic system for managing lockers, mail boxes and various other lockable compartments. For these systems Nedap supplies locks with built-in transponders. After installing these locks, lockers can be opened and closed by holding an electronic key from Nedap or Mifare closely to their locks. These electronic keys can come in the form of cards, wristbands and key rings. Additionally Nedap supplies the LoXS Terminal which keeps track of locks and keys and which makes it possible, if necessary in conjunction with special card readers, to also use (a.o.) PIN codes, bar codes, magnetic cards, Technogym keys. Moreover, the LoXS Terminal opens up a range of management and installation possibilities for the system. Multiple LoXS Terminals can be managed with the LoXS Webserver application. Nedap LoXSs can also operate with locks that do not have an integrated reader, the locker unit Smart. Although this entails a number of restrictions (such as not being able to operate locker doors at the locks) it can serve as a significant cost reduction.

The entire system was developed by Nedap and is also produced by Nedap.

At the moment of purchase and when the LoXS system is being installed a number of choices regarding the operation of the system will have to be made. You can choose to make use of wristbands, or perhaps you have already chosen barcode cards and a third party serial card reader. Also you have already had to indicate the language the system should work with, whether the lockers should be always closed or always open when not in use; whether users must come up with their own PIN code to gain access to their locker; et cetera. These settings will have been configured for you by the engineer installing the system.

However, the Nedap LoXS system is so designed that its settings can very easily be adjusted when, for example, daily use makes clear that not all choices were the most practical. Some changes to the system require the intervention of a technician, but practical changes in everyday use can be made by the administrator. This manual is therefore divided into three parts: a general explanation of the user options; a set of instructions for the administrator; and engineer section.

Firstly the system is introduced (paragraph 1). Next all functionalities of the system for users are presented (paragraphs 2, 3 & 4). Thus this first section also serves as a practical reference guide for the explanation of the system to users. Secondly there is the Administrator section (paragraphs 5 and 6) where options for changing settings and features without the intervention of an engineer can be found, as well as the FAQ. The third and last section contains all the information an engineer needs to install and configure the system exactly as desired by the administrator (paragraph 7 and Appendices). Smart locks are handled differently by users as well as at installation of the system. This is described separately in the appropriate paragraphs and appendices.

By setting up the manual in this manner, the system administrator can keep the Nedap LoXS system running smoothly and perfectly adjusted to the daily practice at all times.



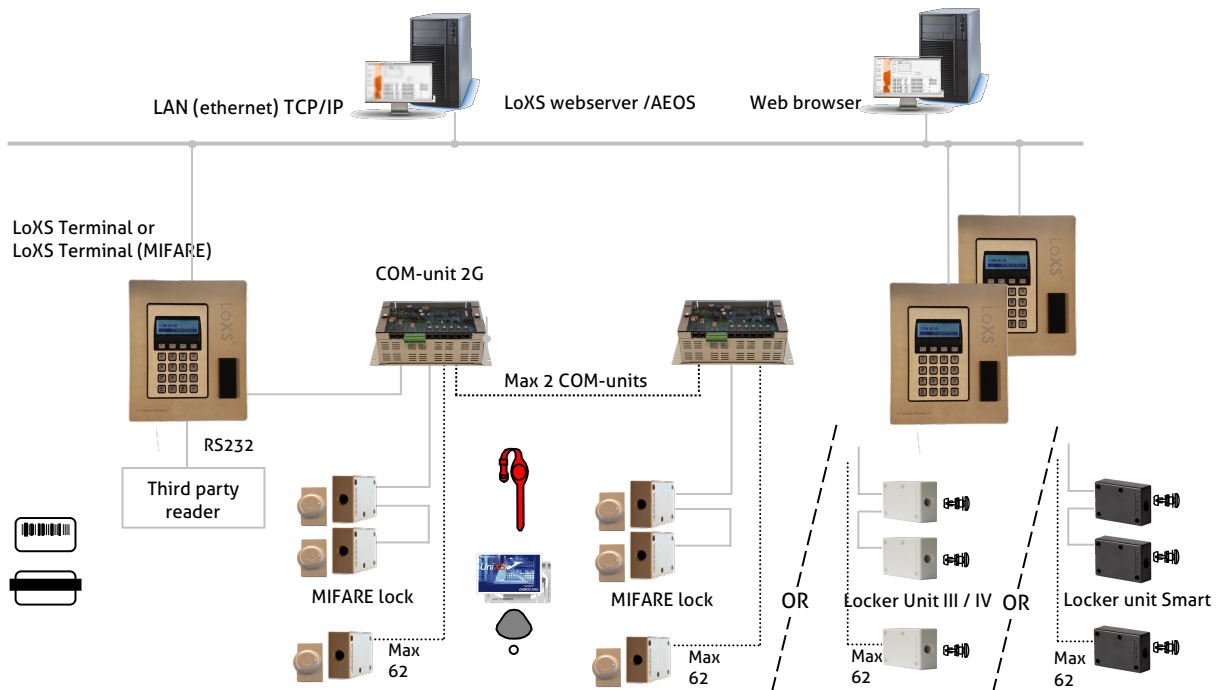
Introduction

1. The system

In this paragraph the entire Nedap LoXS system is briefly outlined, before we move to describe its separate basic elements. With the launch of LoXS software version 3.16 and LoXS Locker Unit IV (summer 2010) the Nedap LoXS system can operate on Nedap locks as well as Mifare locks. In addition to the Nedap locker and the locker unit Mifare, there is also a lock available without a reader: the locker unit Smart. In practice the functionalities of both Nedap and Mifare locks are virtually identical, they are described together in this paragraph.

1.1. Hardware outline

The hardware that is part of the Nedap LoXS system can best be presented in a wiring diagram.



The diagram contains all four basic elements of the system as well as possible electronic keys:

- LoXS Terminal can operate, at most, 124 lockers.
- COM-unit power supply can supply electricity to, at most, 62 locks.
- Electronic lock with reader for sending/receiving data, or without (Smart).
- Pin set is screwed into the locker door and hooks on to the lock.

Also, the following elements are optional:

- Serial card readers for barcode, magnetic strip card, Technogym or Mifare.
- LoXS server application to administer multiple LoXS terminals on a network.

The terminal, electronic locks and the pin sets are only parts of the system visible to users. Administrators and engineers have access to all components.



1.2. The LoXS terminal

The figure at page 2 of this manual shows the most important components of the terminal: the display, the keyboard, the reader and the function keys.

The display provides information to users (i.e. clients, guests) and administrators alike.

The terminal provides various menus, the different steps of which are shown on the display.

The keyboard is used to insert data. For instance users enter their locker number and PIN code with it, while the administrator can alter the configuration with it. The keyboard can be disabled when Nedap or other electronic keys are used.

The reader reads Nedap- or Mifare electronic keys. For instance, users can ask for their locker number in case they forgot. Additionally, the reader is used to read the administrator's master key.

The functions of the function keys, which can be found right underneath the display, are shown in the display after a master key has been scanned by the reader. When the system is configured to use PIN codes, users can also use the functional keys to go through the PIN menu which will also be shown in the display.

The most important functions of the terminal are:

- Managing the status of the lockers (open/closed, available/in use);
- Managing the status of the electronic keys (cards, PIN codes, etc.);
- Opening lockers, in case locker unit Smart is used.

In case someone requests the use of a (new) locker, the terminal will:

- Check whether there are lockers available;
- Check whether the presented key (or PIN code) is authorised;
- In case of paid lockers; check whether a correct amount of coins is inserted;
- Link the locker and the key together, which gives this particular locker the status 'in use';
- Open the locker, in case locker unit Smart is used.

Once a user does no longer need the locker, the terminal will:

- Unlink the locker and the electronic key and give the locker the status 'available';
- In case of a deposit; return the deposit.

Here it should be noted that it is also possible for the administrator to unlock (all) lockers. Information on how this works can be found in paragraphs (5.3 en 7.1.9).



- The system is numeric and uses three digit locker numbers (000 – 999).
- Each terminal can manage a maximum of 124 lockers.
- The terminal allocates the lockers randomly.

1.3. The electronic lock

The electronic lock is the most important part of the system. It is not only for mechanical locking, but each lock has both a memory chip and, possibly, an integrated reader to send/receive data. Locks equipped with all these features can detect and recognize Nedap and Mifare electronic keys. The locker unit Smart, without the reader, cannot do this. With these locks the option to open a locker at the lock is not available. The electronic keys operate the Smart locks via the terminal.



When a lock equipped with a reader does not open upon presentation of the electronic key it was assigned to, a masterkey can be used to open the locker anyway. This back-up function is not available with the use of the locker unit Smart, which does not recognize any electronic key, including masterkeys.

When a locker is closed its door snaps shut and the pin falls into the electronic lock, where a pin detect disk 'feels' it and immediately bolts it. This applies to all locker types. The red LED light then switches from green to red in order to indicate that the locker is occupied. With Locker Unit III the LED light is turned off when a locker is available and starts flashing in red when someone occupies it, i.e. when the lock is bolted.

1.4. Electronic keys

Nedap LoXS uses electronic keys.

We distinguish three different types of keys;

- Electronic keys (Nedap or Mifare) in wrist straps, key fobs and ISO-cards;
- PIN code;
- Other electronic key types, including barcodes and magnetic strip cards; these are the so called 'third-party' keys.

The LoXS Terminal can be used with three types of cards simultaneously: electronic keys, PIN, and one third-party key.



- The choice between Nedap-keys* or Mifare-keys is determined by the type of lock that is selected and the type of type LoXS terminal (See Appendix 8 for an extensive list of possible electronic keys).
- As of this point the explanation of both systems is equal, unless otherwise indicated.



2. Operation with electronic key

2.1. Principle

Nedap electronic keys come in different shapes and sizes, including cards, wrist straps and key fobs. Identification is based on radio frequency, which entails that an electronic key will produce a unique code when it is held in a magnetic field. This occurs when the electronic key is held closely to the reader which is integrated in each lock (with the exception of the locker unit Smart) as well as in the LoXS terminal. We distinguish two different methods of operation. With the first method, an electronic key is held close to the terminal reader; the terminal will subsequently allocate you a locker. The second method gives the visitor the opportunity to select a locker without the use of the terminal. Both methods are explained in further detail in the following paragraphs.



The option to operate lockers at the lock is not available when the locker unit Smart is used. In that case operating the locks with electronic keys is done exclusively via the terminal. (see: 2.4)

2.2. Terminal allocates locker – Standard Mode

The following procedure describes the first method, in which the terminal randomly allocates the lockers. All available lockers are locked, occupied lockers have a red LED light.

Step
01



The user holds the electronic key close to the black reader of the LoXS terminal.

Step
02



The terminal allocates a locker. The user goes to that locker, which has a red flashing LED light, and holds the electronic key close to the lock. The door unlocks and can be opened. The user stores his or her belongings in the locker and closes the door. The locker will lock with a soft 'click'.

The lockers can be opened and closed limitlessly after the terminal allocated a locker to an electronic key. The occupant simply holds the electronic key close to the lock and it opens. The terminal is no longer needed. However, in case the visitor forgets the locker number the intervention of the terminal is required again. When the electronic key is held close to the reader of the terminal, it will show the allocated locker number.

The locker remains allocated to the electronic key concerned until the administrator releases all lockers at the terminal. In practice, this often means that all lockers are released – automatically if preferred – at the end of the day. A locker will consequently be allocated to one single user per day. Please select the method described in paragraph 2.3 if you desire the lockers to be available straight after the user leaves.



2.3. Select the locker yourself - Toggle Mode

In toggle mode, lockers are only bolted when they are actually occupied. A red LED light indicates this 'locked' status. Thus it is always clear to a visitor whether a locker is allocated or not, since an 'available' locker will not be locked and have a green LED light burning.¹ Because of this, toggle mode enables the visitor to go straight to a free locker instead of having to go to the terminal first. An available locker can be allocated to a user's electronic key by holding that key close to its lock. This also bolts the locker door.

In order to use a locker a visitor first needs to find a locker that has a green LED light.² After belongings have been put in the locker the visitor closes the door and holds the electronic key close to the lock. The lock then bolts with a soft 'click' and the LED light starts to flash red. A flashing red LED light indicates that the locker is in use.



The status of lockers is also transmitted to the terminal. Thus at busy times, when searching for free locker might not convene visitors, they can always go to the terminal. After holding their electronic key close to the black reader at the terminal, it will suggest the number of a free locker. Mind you: this does not allocate the locker to the key. For that, the visitor has to go to the locker itself.

Likewise, when one has forgotten the locker number one can go to the terminal and offer the electronic key; the allocated number will then appear in the display.

Toggle mode also enables the user to render a locker free after using it, without intervention of the terminal. The locker will unlock and the electronic key will be unlinked from the locker number when the key is held close to the lock a second time. Doing so immediately releases the locker for other visitors. Note that this is only possible when the system is operating with electronic keys.

In case the visitor wants to leave the following procedure should be executed: go directly to the locker and hold the electronic key close to the lock. The locker unlocks and the door can be opened. As stated before the locker also immediately becomes available for other visitors.



When the visitor wants to open the locker but keep on using it afterwards, the door should be closed again after removing or adding items and the electronic key should be held near the lock again, in order to bolt it and reallocate the locker to that specific electronic key.

¹ With Locker Unit III a free locker's LED is off and an occupied locker's LED flashes red.

² With Locker Unit III a free locker's LED is off and an occupied locker's LED flashes red.



2.4. Operating the locker unit Smart with electronic keys

The options for operating locks as described above are not available when the locker unit Smart is used. Locks without a reader have to be operated via the terminal. The starting point may be:

1. All lockers are locked: red LEDs indicate lockers which are occupied.
2. Green LEDs indicate which lockers are available, red LEDs indicate which lockers are occupied.

In both situations the procedure is as follows:

- The key is presented at the terminal.
- The terminal assigns a locker to the key and (ad. 1) opens it - the locker's LED will start flashing, either red (ad. 1) or green (ad. 2).
- The user goes to the locker, places belongings in it and closes the door. The locker automatically locks; the LED is permanently red.

To open the locker, the key must be presented at the terminal. This can be done as often as desired.



3. Operation with PIN code

3.1. Principle

A PIN code can also serve as an electronic key. Nedap LoXS uses four digit PIN codes. The system allows visitors to choose their own PIN code for maximum convenience. With PIN code operation, visitors need to remember both their PIN code and locker number. The terminal can allocate a locker, or visitors can select the locker themselves. Both methods are discussed below. With PIN code operation visitors use the function keys and the menu that appears in the display, as was outlined in paragraph 1.2. Since this method requires that the locks are operated via the terminal, all information below also applies to the locker unit Smart.

3.2. Terminal allocates locker

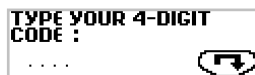
This paragraph discusses how visitors can obtain a locker. The terminal allocates lockers randomly when following this procedure.

Step
01



The visitor presses the function key below "I want a locker"

Step
02



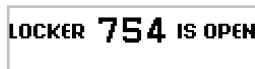
The visitor enters the preferred PIN code.

Step
03



The PIN code has to be repeated.

Step
04



The locker is now unlocked. The visitor has 20 seconds to open the door which has a red LED light flashing. Put your belongings in the locker. The lock will bolt after closing the locker door. One hears a soft 'click' and the LED light will stop flashing and burn red.³ This means that the locker is in use. Users have to remember the locker number and the PIN code themselves.

³ With Locker Unit III a free locker's LED is off and an occupied locker's LED flashes red.



The visitor may want to open the locker to leave or to take something from the locker. The procedure is as follows.

- | | | |
|--------------------|---|--|
| Step
01 |  | Press the function key below "I have a locker" |
| Step
02 |  | The visitor enters the locker number and presses the function key beneath "OK". |
| Step
03 |  | The visitor enters the PIN code. |
| Step
04 |  | Now the visitor can select either "just open" or "I will leave". The first option enables the visitor to remove or add items. The second option makes the locker available for other visitors. |

To open a locker one gently presses the locker door; this unbolts the lock.



In most circumstances the system will be configured so that available lockers are permanently unlocked. As an advantage for visitors, the door will not automatically bolt if visitors accidentally close their locker door when collecting their belongings.



Only lockers that are in use have a red LED light burning. As a result, visitors can easily select a locker they prefer. Simply enter the desired locker number in the start-up screen (step 1) and you will automatically continue with step 2.



The terminal will be blocked for a maximum of 2 minutes when five consecutive incorrect PIN codes are inserted. Within those two minutes the terminal can only be unblocked with the master key. This is explained in paragraph 5.1.



3.3. Select the locker yourself (PIN-toggle mode)

This paragraph explains how visitors can select the locker they prefer. First off they need to select a free locker. The visitor selects a locker that has green LED light burning and is not locked.⁴ After whatever belongings that need to be locked have been put inside the locker the visitor closes the door and goes to the terminal.

- | | | |
|--------------------------|---|--|
| Step
01 |  | At the terminal the visitor presses the function key below "I have a locker" |
| Step
02 |  | Next the visitor enters the locker number and press the function key below "OK". |
| Step
03 |  | The visitor enters a random 4 digit PIN code. |
| Step
04 |  | The PIN code has to be repeated. |
| Step
05 |  | The locker is now bolted and a red LED light burns to indicate this. The display also suggests that visitors check whether the door is properly locked. Again, users have to remember the locker number and the PIN code themselves. |



At the terminal, visitors can press the function key below "INFO" to easily locate available lockers. The terminal randomly recommends an available locker. To obtain this locker the user has to go through steps 1 to 4 as described above.

⁴ With Locker Unit III a free locker's LED is off and an occupied locker's LED flashes red.

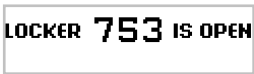


The visitor may want to open the locker to leave or to take something from the locker. The procedure to do so is as follows.

- | | | |
|--------------------|---|---|
| Step
01 |  | <p>The visitor enters the locker number and presses the function key below "OK"</p> |
| Step
02 |  | <p>The visitor enters the PIN code.</p> |
| Step
03 |  | <p>The locker is now unlocked and available for other visitors. In case the visitor is just removing or adding items the above mentioned steps 1 to 4 serve to lock the locker again.</p> |

3.4. Coin Acceptor (third party)

In case you wish visitors to pay rent or a deposit for their use of a locker, a coin acceptor can be made part of the system. Depending on the supplier of the coin acceptor system such an acceptor can consist of a coin detector (mechanical, with switch, or electronic, with coin identifying chip), a hopper to collect the coins in and a controller. Generally such a coin-acceptor is set to receive no more than one type of coin. At the terminal, the administrator can configure the amount of coins that needs to be inserted for the deposit or the rent. The coin acceptor only accepts coins after the visitor has pressed the function key below "I want a locker". Coins are returned immediately in all other cases.

- | | | |
|--------------------|---|---|
| Step
01 |  | <p>The visitor presses the function key below "I want a locker"</p> |
| Step
02 |  | <p>The terminal asks the visitor to insert a sufficient amount of coins in the coin acceptor.</p> |
| Step
03 |  | <p>The visitor enters the preferred PIN code.</p> |
| Step
04 |  | <p>The PIN code has to be repeated.</p> |
| Step
05 |  | <p>The locker is now unlocked. The visitor has 20 seconds to open the door. After belongings have been put into the locker it is locked by closing the locker door. One hears a soft 'click' and the red LED light turns from green to red. This indicates that the locker is in use.</p> |



It is essential to warn the users that they have to remember the locker number and the PIN code themselves.



When someone enters a wrong PIN code five times in a row, the terminal will block the locker concerned (see paragraph 3.2 for more information).

Opening a locker results in the question "just open" or "I will leave" and the procedure is the same as described in paragraph 3.2. The coin hopper returns the deposit in case "I will leave" is selected.



The main objective of operating the system with a deposit is to entice visitors to free up their lockers when they leave. At the terminal the administrator can configure the amount of coins for a deposit. Depending on the type of Coin Acceptor in some cases it is also possible to have the terminal add the deposit to the rent, so the total sum required for the use of a locker can be determined. Choices made with respect to this issue can be marked on the Configuration sheet (Appendix 9).



4. Operation with third-party keys

4.1. Principle

The Nedap LoXS system can be operated with a great variety of third-party electronic keys. Most common are magnetic stripe card or the barcode card. Also a fingerprint reader (third-party supplier) can be made part of the system if so desired. Whatever key or form of identification you choose, the accompanying third-party reader will be connected to the system's terminal. The logical consequence is that operating locks with third party keys is always done at the terminal. Therefore the method described here applies to locks with a reader, as well as the locker unit Smart.

4.2. Terminal allocates locker

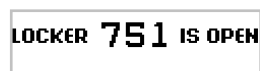
To obtain a locker, the procedure is as follows.

Step
01



Depending on the type of card or key your system uses, the visitor inserts/holds/swipes the card or key in/close to/through the card reader present.

Step
02



The terminal allocates a locker to the key and will, if necessary, unlock it. The visitor then goes to the locker, opens it and stores whatever belongings need storing. Next the visitor closes the door and it will immediately bolt with a gentle 'click'. The red LED light will now burn permanently, indicating the locker is in use.

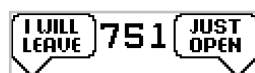
To reopen the locker, the procedure is as follows.

Step
01



Depending on the type of card or key your system uses, the visitor inserts/holds/swipes the card or key in/close to/through the card reader present.

Step
02



The terminal now asks whether the visitor wishes to leave or just needs to open the locker. The visitor selects either "just open" or "I will leave". The first option enables the visitor to remove or add items. The second option makes the locker available for other visitors.



To open a locker one gently presses the locker door; this unbolts the lock.



In case of multiple terminals in one room, visitors need to remember at what terminal they obtained their locker. They will be allocated another locker if they return and present their card or key to another terminal. This may lead to confusion among visitors.

4.3. Select a locker yourself

This paragraph explains how visitors with third party keys can select the locker they prefer. First they need to select a free locker. The visitor selects a locker that has green LED light burning and is not locked.⁵ After whatever belongings that need to be locked have been put inside the locker, the visitor closes the door and goes to the terminal.

Step
01



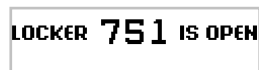
The visitor enters the preferred locker number and presses "OK". The terminal will show the message that the locker is available. (Or, if the number is not correct, that the locker is occupied or blocked.)

Step
02



Depending on the type of card or key your system uses, the visitor inserts/holds/swipes the card or key in/close to/through the card reader present

Step
03



The preferred locker is now unlocked and available to the visitor

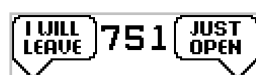
To reopen the locker, the procedure is as follows.

Step
01



Depending on the type of card or key your system uses, the visitor inserts/holds/swipes the card or key in/close to/through the card reader present.

Step
02



The terminal now asks whether the visitor wishes to leave or just needs to open the locker. The visitor selects either "just open" or "I will leave". The first option enables the visitor to remove or add items. The second option makes the locker available for other visitors.



At the terminal, visitors can press the function key below "INFO" to easily locate available lockers. To obtain this locker, the user has to go through steps 1 to 3 as described above.

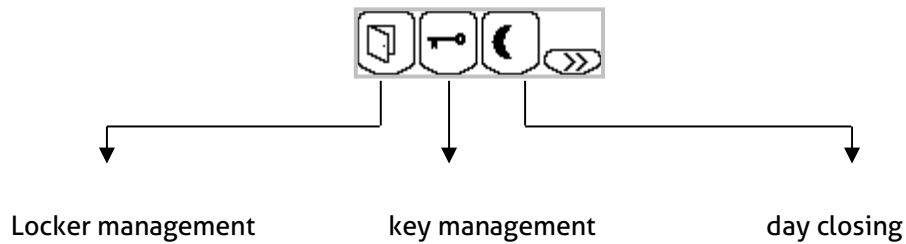
⁵ With Locker Unit III a free locker's LED is off and an occupied locker's LED flashes red.



Administrator Section

5. The administrator menu

Nedap electronic locker management is low on maintenance; however, the necessary upkeep has to be done carefully. The terminal provides several menus for administrators. You received one or more master keys at the time of installation. Hold the master key close to the black reader at the terminal to enter the administrator menu.



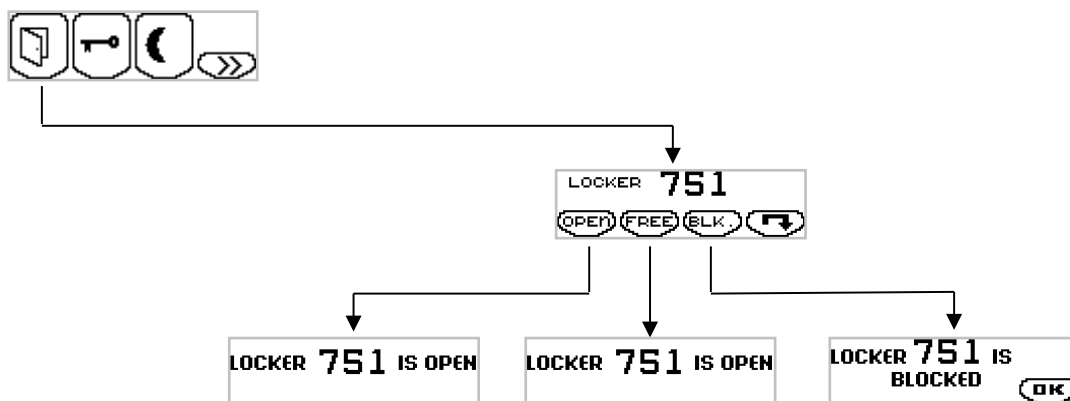
In the administrator menu, you can manage the lockers, manage master keys and release all lockers.

Available lockers locked? The pros and cons.....



When you maintain lockers that are not in use locked, the result is that all lockers are locked at all times. The advantage of this setting is that visitors cannot 'mess with' available lockers, as they are bolted and cannot be opened in any other way then by using the system. However, there are some disadvantages. For example, if the door of an available locker is not closed properly, someone – who did not check the terminal or locker number properly – may put belongings in the locker and close it. The locker will automatically bolt, and the visitor will assume that the locker is allocated to him or her. However, the visitor cannot open the locker mistakenly taken to be his, or hers. This is especially inconvenient when the terminal allocates this locker to another visitor, who will then find someone else's belongings in the locker. To avoid situations like this one the option to keep free lockers open at all times is available.

5.1. Locker management



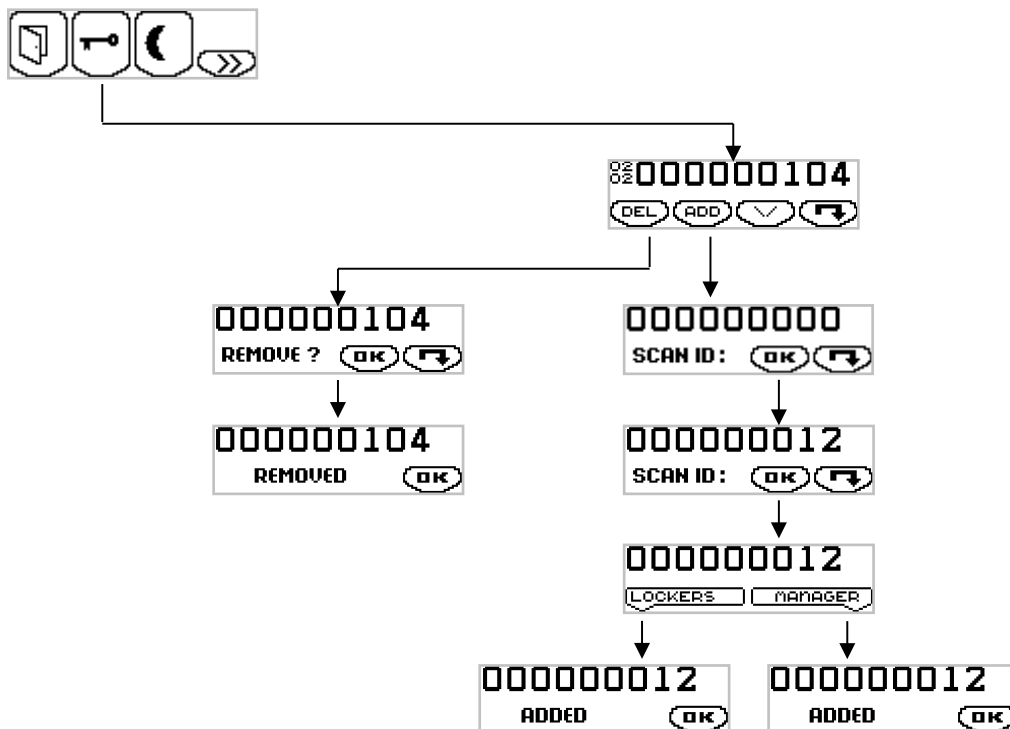


Lockers can be unlocked (open), released (free) and blocked (blk) in the locker management menu. Enter the locker number after selecting the 'locker icon' (image of the open locker door). Subsequently, you can select to unlock or release the locker. These options are most often used in case visitors forget their PIN code. The third option is to block a locker. This might be necessary when, for instance, a locker is not functioning properly due to hinges that were not adjusted correctly. A blocked locker will be bolted, show the 'in use' indication and will not be allocated to visitors anymore. A locker can be unblocked in the same menu by selecting "FREE" after you entered the locker number concerned.



In AEOS compatible mode the function Free and Block are disabled.

5.2. Key management



By selecting the 'key icon' you can add or remove master keys. Select "ADD" to add a new master key to the list. Subsequently, hold the electronic key, which you want to be the new master key, close to the terminal reader. The display shows the 10-digit key code of the electronic key as soon as it is read. Press "OK". There are two master key levels; locker level and manager level. The newly generated master key will only be valid to manage the lockers if you select the "locker" level (see paragraph 5.1). It will also be able to administer the "key management" (this paragraph) and to "release lockers" (paragraph 5.3) by selecting the "manager" level. If you want to delete a master key from the list; browse the key code of the concerned master key by using the arrow key (V) and press "DEL". You can as well enter the key code of the concerned master key if it is not available anymore. Confirm by pressing "OK".



You need to know the key codes of your master keys to be able to enter the key code of a missing master key. Therefore, it is strongly recommended to write down the 10-digit key codes of all master keys you generate and to administer who you give which master key.



The data of activated masterkeys are also copied to the locks, so the masterkeys can open them in case the electronic key or terminal fail to do so. This does not apply when the locker unit Smart is used.



In AEOS compatible mode you cannot add or remove Masterkeys.

5.3. Release all lockers



At the end of the day, the menu with the 'moon icon' needs to be selected to assure that all lockers are available for the next day. All lockers are released by selecting this option and, if applicable, all coins present in the coin hopper are disbursed. Press "OK" to confirm the release of all lockers and coins.



If you use rental or deposit for your lockers, all coins in the coin hopper are disbursed after releasing all lockers. Therefore, it is recommended to place a small cup under the coin ejector. By collecting the coins from the hopper this way, they will automatically be counted. When the hopper is empty, the terminal will show you the total of that day's revenue.

Additionally, it is possible to automatically release the lockers at a predetermined time. Options such as these are discussed, and selected or discarded prior to installation on the Configuration sheet (Appendix 9). However, in case you change your mind about the first configuration, or you want to work with different release moments, you can consult paragraph 7.1.9 of the Engineer section of this manual to adjust the system to your new wishes.



Manually blocked lockers (see paragraph 5.1) will not be released through this 'Release all lockers' menu.



In AEOS compatible mode this menu is disabled.



6. Frequently asked questions

We have both small and large lockers. Can visitors select the size they prefer at the terminal?

No. The terminal does not draw a distinction between the sizes of lockers. This would make the operation for visitors too complicated, especially with multiple locker dimensions. Nedap decided to include an option that enables visitors to select their own locker and to 'tell' this to the terminal (see paragraphs 2.3 and 3.3).

What happens in case of a power failure?

Nedap LoXS is an electronic system, which implies that it always needs electricity for complete and optimal operation. The best security for power failure is to connect the terminals and COM-units to an uninterruptible power supply (UPS, Nedap product number 9893733). This 'storage battery' feeds the system with energy for a limited amount of time in case of a power blackout. This gives visitors the opportunity to take their belongings from the lockers. All lockers keep their most recent status (for instance locked/unlocked) and all data are stored in case of an unexpected cut off from any power.

A visitor cannot open his/her locker. The master key does not work either. What is wrong?

There is usually a mechanical cause for this kind of problem. Sometimes large items in the locker exert pressure on the door. In such a case the door cannot unlock because it causes the pin tip to exert pressure on the bolting mechanism. This can easily be resolved by pushing gently against the door to release this pressure. Another cause can be the pin set. It is possible that, after a long time of operation, the pin set becomes somewhat loose, which creates a large margin within the lock. As a result, the pin set may become stuck in the lock. This can be resolved as well by pushing gently against the door and slightly relocating the pin set manually. When it turns out the pin set is screwed into the door too loosely it must be tightened.

How come sometimes two lockers are allocated to one visitor?

It is important that visitors return to the same terminal as where they obtained their locker, especially on locations with multiple terminals. A different terminal will simply allocate the visitor a new locker, because it cannot "know" another terminal already allocated a locker to this visitor.

This problem can be avoided though, through the use of the Nedap LoXS Webserver application (Nedap product number 8014833). The webserver is always connected to all terminals, whereby it can keep track of all lockers and users. In case a visitor who already has a locker (accidentally) tries to claim another locker, the webserver will not approve the claim. No second locker is ever allocated to one and the same electronic key.

Can I automatically release all lockers at night?

Yes, the system can, besides manual release of all lockers, release all lockers on a predetermined time. This is explained in paragraph 7.1.9.

Does the system automatically switch to daylight saving time (DST), and back?

The terminal has no software to keep track of DST. If necessary the system time can be adjusted manually. The procedure is described in paragraph 7.6.

A locker seems to be defective, what should I do?

Always close down any lock that is not functioning properly. This prevents any inconvenience for visitors. Paragraph 5.1 explains how to block a locker. Please report the problem to your service partner; a defective lock is no immediate problem and can generally be repaired or replaced during the next overhaul. At your request Nedap can supply a so called LoXS Help manual to help solve possible small malfunctions.



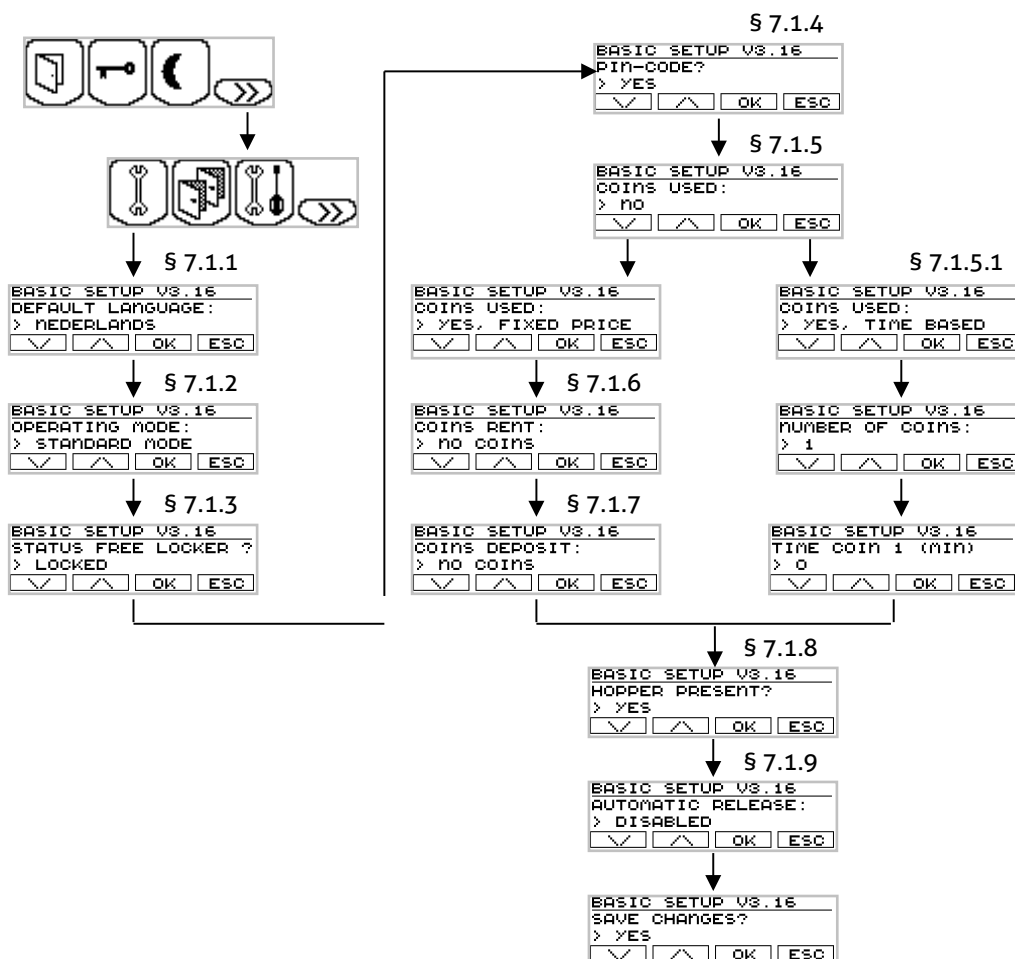
Engineer Section

7. Installation menu

Hold the master key close to the black reader of the terminal to enter the master key menu. This will first show you the administrator menus. Select next screen (⟹) to enter the first screen of the installation menu. This shows the setup for basic setup, hardware settings and advanced setup. Browsing further shows you the next installation menu, with the network settings, reset options and settings of the system clock.

7.1. Basic setup

You can configure the system in *Basic setup*. The overview below shows the various steps of the menu. A description of the settings is given in the corresponding paragraphs.



7.1.1 Default language

Select the default language that you prefer for the user interfaces. Use the arrow keys to browse the languages (Dutch, English, German, French, Italian, Spanish or Portuguese) and confirm with "OK". The administrator and installation menus are always in English.



7.1.2 Operating Mode

This entails the operating mode of the system.

Standard mode

The system operates in a standard mode which allocates lockers via the terminal (see paragraphs 2.2, 3.2 and 4.2). The system asks for the settings of the available lockers after activating this mode. Available lockers are, depending on the settings in 'status free lockers' (see paragraph 7.1.3), locked or not.

Toggle Mode

All available lockers are unlocked in this mode; they are only bolted if allocated to an electronic key (see paragraphs 2.3 and 3.3). The locker is unlocked and released after presenting the electronic key a second time. The system does not ask for the settings of available lockers after activating this mode.

Showcase mode

This mode sets the terminal and locks for showcases. This implies that an alarm will sound if a locker door is opened too long. All other basic setup configurations are skipped after enabling this mode.

7.1.3 Status Free Locker

This entails the state of available lockers, which can be either 'locked' or 'unlocked'. This configuration is only valid for Standard mode.

7.1.4 PIN code

The key pad needs to be activated to enable PIN code operation. Select "yes" to activate the key pad. The system will ask for settings for a possible coin acceptor and coin hopper after enabling this function (continue with paragraphs 7.1.5 through 7.1.9). in case "no" is selected here, no options for configuring the use of coins will be available (continue with paragraph 7.1.10).

7.1.5 Use of coins

Here you select whether or not visitors are required to submit a deposit or pay rent for their use of a locker. If so this can be done either *time based* (continue with paragraph 7.1.5.1) or with a *fixed price* (continue with paragraph 7.1.6).



A coin acceptor system is can only be supplied by a third party. It is not a Nedap product.

7.1.5.1 Coins time based

Are visitors required to pay a deposit for the time they use a locker? You can select how many coins must be deposited ('number of coins'; /\ to increase the number) for what amount of time. The amount of time is fixed by coin. For example: first coin – 30 minutes; second coin – 1 hour; fifth coin – 8 hours ('time coin in'; /\ to increase the number of minutes). When the system is configured to operate with a deposit, options for collecting rent are no longer available (continue with paragraph 7.1.10).

7.1.6 Coins rent

Are visitors required to pay rent for their use a locker or not? Here you can select 'no coins', 'one coin' or 'two coins'. The coins are generally € 0,20 or € 0,50 coins, depending on the coin



selector. Whether you choose no, one or two coins, the option for use of a deposit that is *not* time based will always follow (7.1.7) and subsequently the option to configure a hopper (7.1.8).

7.1.7 Coins deposit

Are visitors required to pay a deposit for their use a locker? Here you can select 'no coins', 'one coin' or 'two coins'. The coins are generally € 0,20 or € 0,50 coins, depending on the coin acceptor.

7.1.8 Hopper present

A coin hopper is a unit that can pay out coins. A coin hopper is required if you want visitors to pay a deposit, as the deposit needs to be returned when the visitor leaves. Select "yes" if a coin hopper is installed. This also affects the interface for PIN code. If no coin hopper is present, the PIN code screen will show an escape key to leave the screen. The escape key is left out in case a coin hopper is present.

7.1.9 Automatic release

This configuration determines at what hour the lockers are released. It must be set on "disabled" if it is not desired to release all lockers at a certain hour. The unit of time is an hour. The time is displayed in the administrator menu if automatic release is enabled. This enables the administrator to check the clock.



The terminal does not change automatically between standard time and daylight saving time, this must be changed manually (see paragraph 7.6).

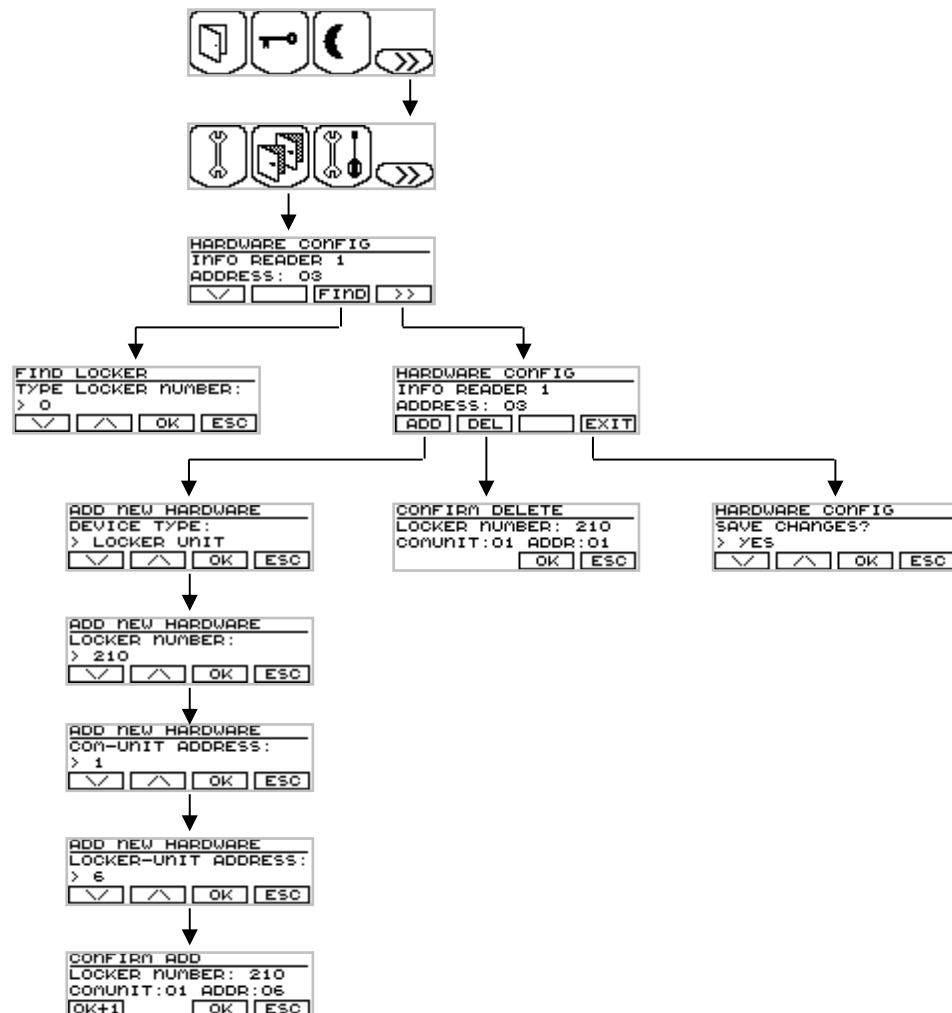
7.1.10 Save changes

The system asks to save all changed preferences. The system reboots and the user interface for locker management is displayed. You need to go through all steps of the menu, even if you change only one setting, for instance the default language. The system does not ask to "save changes" if no changes have been made.



7.2. Hardware configuration

This menu configures the hardware, including locker and COM-unit addresses. Additionally, the type of reader can be set here.



Hardware includes not only the locker unit, but an info reader, in reader, out reader, unlock reader and dummy reader as well. The reader settings determine the behaviour of the reader. All types of hardware are discussed in the following paragraphs.

7.2.1 Locker unit

Locker units need to be added to the terminal with every new installation or system expansion. The "ADD" key is used to add new hardware (please browse by pressing ">>" if "ADD" is not displayed). Next, the system asks what type of hardware is added; a locker unit or one of the various readers (§ 7.2.2 t/m 7.2.5). Select "locker unit" and press "OK" to add lockers. Subsequently, you need to enter the locker number, COM-unit address and locker address. Press "OK" to confirm your input or press "OK+1" to confirm your input and to add 1 to the locker number and locker address. You will return to the main menu of hardware configuration by pressing "OK".



After adding the lockers, the system enables you to browse the list of hardware. Each locker is represented by a locker number, COM-unit address, locker address and the status of each record.

We distinguish the following statuses:

NEW	newly added locker, but not saved yet.
FREE	available locker.
ERROR	locker with a line error.
BLOCK	Locker is blocked.
INUSE	Locker is in use.

Press "EXIT" to leave the menu. If any changes have been made, the system will ask to save these changes. Press "OK" to save the changes.

The Nedap logo is displayed and the terminal connects with all locks and in readers after the hardware is added. This may take a while, depending on the number of locks.

If you enter the hardware configuration menu after saving all changes, the lockers that are configured correctly are displayed with the status FREE and the lockers that could not be connected to are given the status ERROR. All entered records can be checked by pressing the "/" and the "\" keys.



This overview is useful for service and maintenance too: the service engineer can easily see which lockers are blocked and which are erroneous.

Hardware can be deleted by pressing "DEL". This key will remove the selected hardware from the list.



Press "Find" and enter the locker number to quickly go to a preferred locker. The system will jump forward to the number and all details are displayed directly.

7.2.2 Info Reader

If an info reader is added, the terminal reader will allocate a locker and display the locker number after presenting an electronic key. Also, the terminal will display the locker number when the key is presented again. The master key menu is opened by presenting a master key at the terminal reader.

7.2.3 In Reader

The terminal reader adds the presented electronic key to the white list (see advanced setup §7.3.7).

7.2.4 Out Reader

After presenting an electronic key, the terminal reader deletes the key and unlinks it from the allocated locker. This option is rarely used, but can be of use if the out reader is used to release a locker via a turn stile.



7.2.5 Unlock Reader

The terminal reader allocates a locker, displays the locker number and unlocks the concerned locker after presenting an electronic key. When the key is presented again, the terminal will display the (earlier allocated) locker and unlock the locker. The master key menu is opened by presenting a master key at the terminal reader.

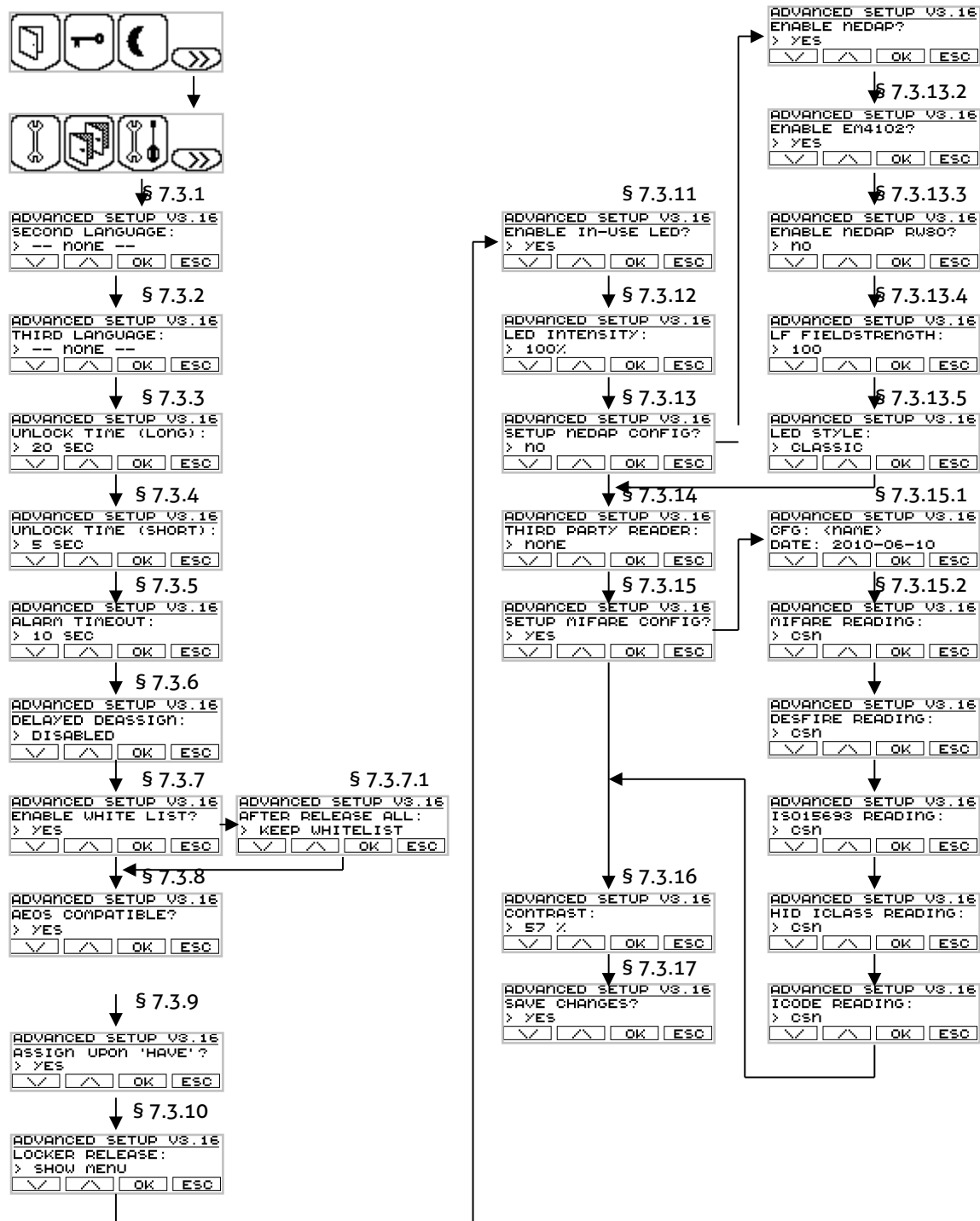
7.2.6 Dummy Reader

The terminal reader creates an event and sends it to a possible connected system or server using a LAN network, but no other action is executed. Nonetheless, the master key menu is opened by presenting a master key.



7.3. Advanced Set-up

The outline below shows the various steps of the advanced set-up menu. Further explanation of the configurations can be found in the corresponding paragraphs.





7.3.1 Second Language

This option enables you to select a second language (Dutch, English, French, Italian, Spanish or Portuguese), which visitors can select by pressing "B". The terminal automatically returns to the default language after the visitor is finished.

7.3.2 Third Language

This option enables you to select a third language (Dutch, English, French, Italian, Spanish or Portuguese), which visitors can select by pressing "C". The terminal automatically returns to the default language after the visitor is finished.

7.3.3 Unlock time (long)

The unlock time (long) is the time that a locker is unbolted after unlocking it from the terminal, for instance by using a PIN code. The locker will automatically lock after the unlock time is elapsed. However, the timer immediately stops if the locker is opened and closed again within the unlock time. 'Long' indicates that the locker is unlocked at the terminal. The unlock time (long) can be set at: 10, 20, 30, 40, 50, 60 seconds.

7.3.4 Unlock time (short)

The unlock time (short) is activated if a locker is unlocked by holding an electronic key close to the lock. The locker remains unbolted for the selected unlock time (short). The unlock timer immediately stops if the locker is opened and closed again within the unlock time. 'Short' indicates that the locker is unlocked at the lock. The unlock time (short) can be set at: 1, 2, 3, 5, 10, 20 seconds.

7.3.5 Alarm Timeout

An indicator which detects the position of the locker door (open/closed) is integrated in each lock. This indicator detects a sabotage alarm. This alarm activates the relay connected to all the COM-units. The time that the relays stay activated is set in this menu. This timer is immediately stopped if the administrator opens the master key menu with the master key. The alarm timeout can be set at: 10 sec, 30 sec, 1 min, 2 min, 3 min, infinite.

7.3.6 Delayed deassign

Used in combination with *toggle mode* this option is used to provide a delay between the moment a visitor takes something from the locker and the moment the locker is unlinked from the visitor's electronic key. Thus the visitor can take something from the locker without having to go through the steps for re-obtaining that same locker. The delay time can be set at 30 seconds, anything between 1 to 5 minutes and 10 minutes.

7.3.7 Enable White list

A white list is an inventory of all electronic keys valid for the concerned terminal. The terminal checks the white list before allocating a locker to an electronic key. Any electronic key can obtain a locker if the white list is disabled. An electronic key must be listed on the white list to obtain a locker if the white list is enabled. The terminal is usually connected to a server if the white list is enabled (marked as "yes").



7.3.7.1 After release all

When the system is configured to include a white list a subsequent question appears: what should happen to the white list once all lockers are made available again? You can select to either 'keep' the white list or to 'clear' it, i.e. erase it.

7.3.8 AEOS compatible

In case the administrator also uses the AEOS system for access control and so desires, her a connection can be made between LoXS and AEOS. In this mode the terminal automatically adjusts the configuration of the electronic keys and sets a default length for data from third-party readers.

Master key functions like free and block locker as well as adding and removing Master keys are disabled.

7.3.9 Assign upon 'have'

The terminal only asks this question if PIN code operation is used. With this option enabled ("yes"), users can select the lockers they want and obtain them at the terminal by pressing the function key below "I have a locker" (see paragraph 3.3). With this option disabled ("no"), only the terminal can allocate lockers (see paragraph 3.2).

7.3.10 Locker Release Menu

By enabling this function ("show menu"), the terminal asks, after presenting an electronic key the second time, whether the visitor wishes to just open the locker or wishes to leave. The terminal does not ask this question if the function is disabled ("skip menu"). This function is optional for all electronic keys except PIN code; the function is always enabled if PIN code operation is used. Additionally, lockers can be released after a predetermined time. The timer starts after a locker is allocated to a visitor's electronic key. Select "after 1-8 hour" to enable this timer.

7.3.11 Enable In Use LED

A locker that is in use or that has been blocked has a flashing red LED light. If desired, the LED light can be disabled in this menu by selecting "no".

7.3.12 LED intensity

With Nedap Locker Unit IV and Mifare locks it is possible to adjust the intensity of the LED lights to the wishes of the administrator. The intensity can be set at a scale from 10 to 100%. This setting will not be active until all changes have been saved (7.3.17).

7.3.13 Setup Nedap config

The software for the Locker Unit IV series comes with a number of extra options concerning the cards that are going to be used, the transmit power of the reader in the lock, and the functioning of the LED lights. These options only become available after selecting 'YES' (when no specific Nedap configuration is required you select 'NO' and continue with paragraph 7.3.14).



7.3.13.1 Enable Nedap

When the system is not going to be operated with Nedap cards, the compatibility of those cards with the system can be cancelled here by selecting 'NO'.

7.3.13.2 Enable EM4102

Select 'YES' to enable the card-reader Marin EM4102 to read electronic keys or 'NO' to disable the use of this type of electronic key.

7.3.13.3 Enable RW80

Select 'YES' to enable the card-reader Nedap RW80 electronic keys or 'NO' to disable the use of this type of electronic key.

7.3.13.4 LF Fieldstrength

The lock readers of Locker Unit IV have an adjustable output strength. The transmit power can be set anywhere between 0 to 100 (this prevents cross interference between the transmitting fields of the different lockers).

7.3.13.5 LED style

The Locker unit IV series has both a green and a red LED light. When locker systems older than IV are being used in combination with Locker Unit IV select 'classic' LED style. This setting makes sure only red LED lights will be used on all lockers, old and new.

7.3.14 Third Party Reader

Third party readers are readers other than Nedap readers, such as barcode-, 'other' RFID-, HID, magnetic strip card- or Technogym readers. The Nedap ConveXS reader can also be used as a third-party reader. This does require an RS485 to RS232 converter. The third party readers are connected to COM3 or USB of the terminal. The settings for the Technogym readers and barcode scanners from Datalogic are already installed on the terminal and can be selected with the browsing keys. The configuration for all other third party readers with a RS232 connection can be entered by selecting "other". Select the right transfer rate (1200, 2400, 4800, 9600, 19200 Baud) for the baud rate and select the right format for databits (5, 6, 7, 8 databits), parity (none, odd, even) and stopbits (1, 2 stopbits). 'TCP/IP socket' and 'Other' also have two additional options that appear on the display after 'stopbits'. Firstly appears the option to enter the manufacturer of the type of card that is going to be used, and secondly the subtype of this card can be entered. The reader must send a minimum of 4 and maximum of 20 characters and the message needs to be concluded by control characters Carriage Return and Line Feed (CHR13+CHR10); also see paragraph 7.9.



The lists of manufacturers and card types are so extensive that they have not been included in the menu. The numbers for reader manufacturers and reader subtypes (indent) are listed here':

- 0: Nedap
- 1: Serial interface (3rd party reader).
- 2: Magstripe
 - 1:Magstripe – track 1 iso
 - 2:Magstripe – track 2 iso
 - 3:Magstripe – track 3 iso
 - 4:Magstripe – raw data
- 3: Wiegand
 - 1:Wiegand – 26 bit
 - 2:Wiegand – 32 bit
 - 3:Wiegand – 37 bit
 - 7:Wiegand – 64 bit
 - 8:Wiegand – 128 bit
 - A:Wiegand – generic
- 4: Barcode
- 5: NXP/Mifare
 - 1:Mifare – CSN
 - 2:Mifare – Sector data
 - 3:DESfire – CSN
 - 4:DESfire – File data
 - 5:ICODE – CSN
 - 6:ICODE – Data
- 6: reserved
- 7: LEGIC
 - 1:LEGIC – Prime CSN
 - 2:LEGIC – Prime data
 - 3:LEGIC – Advant CSN
 - 4:LEGIC – Advant data
- 8: HID
 - 1:HID – iClass CSN
 - 2:HID – iClass data
- 9: EM-Marin
 - 1:EM-Marin – EM4102 data
 - 2:EM-Marin – EM4x50 data
- A: Pincode
- B: Suprema
- C: Technogym
 - 1:Technogym – standard
 - 2:Technogym – swipe



These numbers can be entered at *reader manufact no* and *reader subtype no*.



7.3.15 Setup Mifare config

The software of Mifare locks comes with a number of extra options for cards that might be used with the system. These options only appear when 'YES' is selected here (in case you select 'NO' continue with paragraph 7.3.16).

7.3.15.1 CFG: <name>

This option only appears after a Mifare configuration has already been done at the terminal by means of the SCCL PC-tool. When the name of that configuration file appears in the display all setting in paragraph 7.3.15.2 have already been configured. In case you need to make changes to that file, you can select to do so here. When no configuration file is present, the menu will automatically skip from 7.3.15 to 7.3.15.2.

7.3.15.2 CSN

Here you can enable or disable the use of different types of cards compatible with Mifare-locks. To enable you select 'CSN', to disable you select 'Disable'. You will be presented with the following successive options: Mifare reading; Desfire reading; ISO15693 reading; HID Iclass reading; an Icode reading.

When a prior Mifare configuration has been loaded (7.3.15.1) Mifare reading and DESfire reading have additional options, respectively 'sectordata' and 'Filedata'.

7.3.16 Contrast

The standard factory settings for the LCD screen contrast are for optimal convenience. However, it may be preferred to adjust the contrast if the LCD screen is installed lower or higher than eye level or placed under an angle. Use the arrow keys to change the contrast settings. The screen adjusts instantly to the changes made.

7.3.17 Save changes

The system asks to save all changed preferences. The system reboots and the user interface for locker management is displayed. You need to go through all steps of the menu, even if you change only one setting, for instance the second language. The system will not ask to "save changes" if no changes have been made.

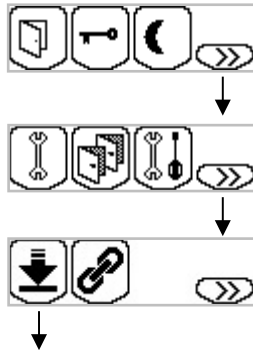


7.4. Update locker and reader firmware

The following hardware can receive a firmware update:

- Lock: all Mifare, Locker unit IV or Smart locks present
- Read: the info reader of the LoXS terminal
- Term: the kernel of the terminal

Go to the update function:

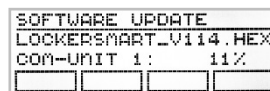
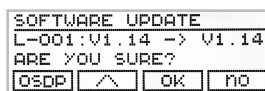


Here the following screen appears:



Select the part which needs to be updated.

For locker or reader firmware one of these screen appears, respectively:



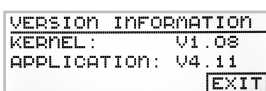
Click OK to activate the download for this update to the locks.

Choose OSDP to upgrade the firmware of the locks to the OSDP protocol, making them suitable for direct communication with a Blue controller. After a successful update the communication with the LoXS terminal stops and the Red-Green LEDs goes off.



After the OSDP firmware has been loaded, communication with the LoXS terminal is lost and it is no longer possible to go back to the original firmware!

This screen appears when selecting TERM and it shows the kernel and application version.





A kernel update will automatically complete at the next startup.
The application will be updated via the server, through an sftp connection.

7.4.1 Force download

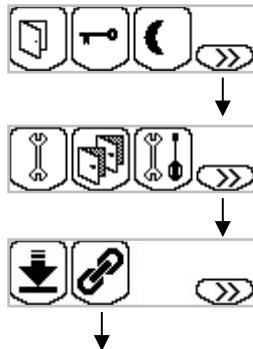
A firmware update can fail when the current version of the firmware cannot be read. In that case, you can force the hardware to start downloading the update. Press the "XTRA" button to open the "Force download" menu. Select your locker type and press "OK".



7.5. Assign system addresses to lockers

All locks must be assigned with a system address. The assigning procedure differs for locks with and without a reader. Both are described in Appendix 5 (for locks with a reader see 5A, for the locker unit Smart see 5B).

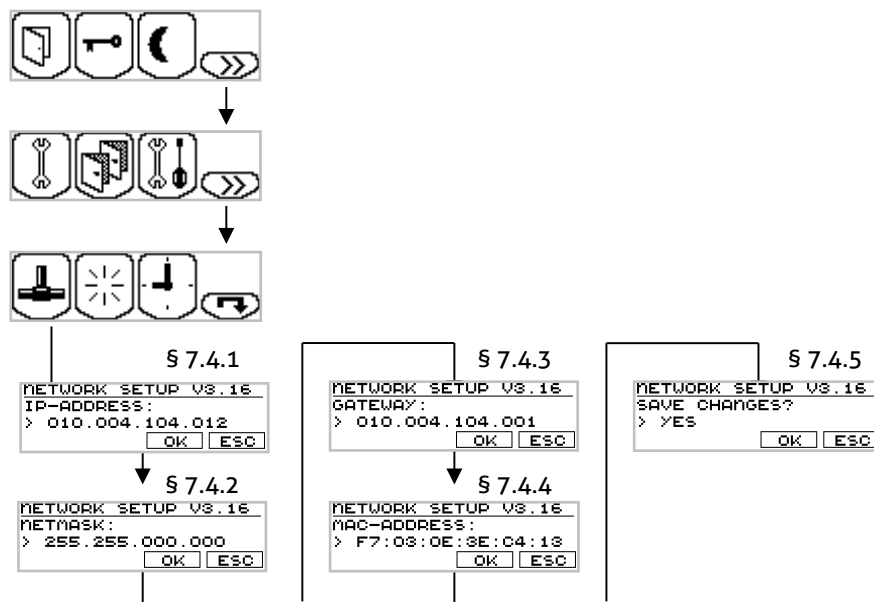
Go to the binding function to enter the appropriate addresses on the terminal:



See Appendix 5 for further instruction.

7.6. Network setup

The network setup contains all settings for the network. Network settings are required if the terminal communicates with a server/system using an IP connection. Settings are available at the concerned network administrator. The various menus are outlined below. The different configurations are discussed in the corresponding paragraphs.



7.6.1 IP-address

Enter the IP Address here. If needed, use the "." key to insert the IP address. You can delete your input in its entirety with the CLR key.



7.6.2 Netmask

Enter the netmask number here. If needed, use the "." key to insert the netmask address. You can delete your input entirely with the CLR key.

7.6.3 Gateway

Enter the gateway here. If needed, use the "." key to insert the gateway address. You can delete your input entirely with the CLR key.

7.6.4 MAC-address

Here you can find the unique network address of the terminal. There is nothing to configure here, but the address is important when the system will be operated with port protection. This address will have to be entered to enable such protection.

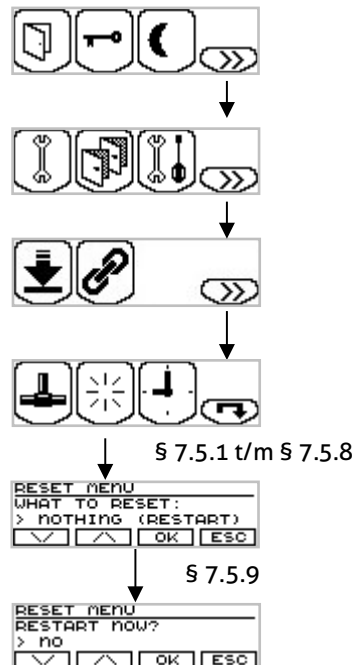
7.6.5 Save changes

The system asks to save all changed preferences. The system reboots and the user interface for locker management is displayed. You need to go through all steps of the menu, even if you change only one setting, for instance the IP address. The system will not ask to "save changes" if no changes have been made.



7.7. Reset Menu

This menu enables you to reset or erase various configurations. The various menus are outlined below. The different configurations are discussed in the corresponding paragraphs.



7.7.1 Nothing (restart)

The terminal restarts without resetting any configuration.

7.7.2 Terminal setup

This option erases all terminal configurations, namely, the configurations of the Basic (paragraph 7.1) and Advanced setup menu (paragraph 7.3).

7.7.3 Lockers config

This option deletes all lockers. The hardware list containing all lockers is now empty and the default info reader with address 3 is added.

7.7.4 Reset locker smart addresses

Select this option to undo the assigning of system addresses to Smart lockers. Note that this is not done automatically through resetting factory values (7.7.9). To reassign addresses to lockers the procedures described in Appendix 5 have to be executed again.

7.7.5 Keys database

This option erases the data of all types of electronic keys, including electronic keys for visitors, master keys and PIN codes. All lockers allocated to these keys are consequently released.



7.7.6 Nedap ID filter

The customer code is saved and communicated to all connected locks after presenting the first Nedap electronic key. The ID filter ensures that only electronic keys with your customer code can be read. The option 'Nedap ID filter' only deletes the ID filter. As a result, the terminal is now again accessible for a new (random) Nedap electronic key and its customer code.

7.7.7 Third Party ID filter

If a third party reader is used, such as a barcode or magnetic strip reader, the terminal will ask what part of the code is the customer code and what part is the key code after, presenting it the first time. The customer code, or ID filter, is used to block other electronic keys with different customer codes.

7.7.8 Mifare config

This option deletes all Mifare settings, including possible configuration files. Return to paragraph 7.3.15 in case you wish to review these settings.

7.7.9 All (Factory DFLT)

This option restores all factory settings, except the IP parameters (see Network setup, paragraph 7.6). All keys, lockers and ID filters are erased. The terminal settings go back to the factory default.



Restoring the factory settings does not erase the locker addresses from the locks. To reset locker addresses, see the previous paragraph.

7.7.10 Restart now?

The system asks to "restart/reset now" if "OK" is selected in one of the above-mentioned options. This is executed by selecting "yes". The system will restart, depending on the concerned option.

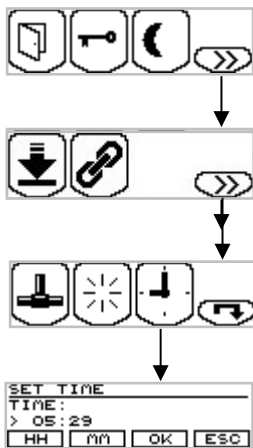


7.8. Set time

This menu sets the installed clock. The clock is used only if the automatic release is enabled (see basic setup).



The terminal does not automatically switch to daylight saving time (DST), this must be done manually.



Press the "HH" key to set the hours and press the "MM" key to set the minutes. The unit is 1; hence pressing the key once raises the concerned figure with 1. The key cannot be repeated automatically by holding it and needs to be pressed for each added hour or minute.

Press "OK" to leave the menu.



7.9. Third party ID filter

The configuration of a third party electronic key needs to be set if it is used to operate the lockers. The menu below is not activated by presenting the master key, but is shown after presenting the third party electronic key for the first time.

```

?=?NUM .=?SKIP !=OPT
00101DEDOC7066
0
SEL NEXT OK ESC

```

The display shows the number of the key it has just read. You need to indicate what digits are of significance, or, in other words, how unique the third party electronic key needs to be.

The following configurations are available:

- ?=NR; each digit on this location is part of the key code;
- .=Ignore; this digit is not part of the customer code or key code and is therefore skipped;
- !=optional; here you can set a code of variable length of your own choosing – each ! Marks a digit;
- Match; the shown digit is part of the customer code.

You can switch between “match”, “.”, “!” or “?” by pressing “SEL”.

Press “NEXT” to accept the configuration and to go to the next digit.

Press “OK” after inserting all settings.

Press “ESC” and re-offer the third party electronic key if the settings are incorrect.



This menu cannot be entered after saving your settings. You can only erase your settings using "third party ID filter" in the Reset menu.

The maximum length of a key code is 20 digit and the minimum length is 4.
A key number can never exceed 2^{32} (4294967296).



Appendix 1 Terminal connections

Item:	Pin:	Definition:
1 (K7)	-	USB-b (console)
2 (K3)	-	USB-a
3 (K14)	1	+12Vdc output (200mA max.)
	2	Ground (GND)
	3	Digital input 1 (5Vdc max.)
	4	Ground (GND)
	5	Digital input 2 (5Vdc max.)
4 (K11)	6	Ground (GND)
	1	CAN – high
	2	CAN – low
	3	Ground (GND)
5 (K12)	1	NC – Relay1 **
	2	COM – Relay1 **
	3	NO – Relay1 **
	4	NC – Relay2 **
	5	COM – Relay2 **
	6	NO – Relay2 **
6 (K6)	-	RJ10 – RS485 (Combus)
7 (K7)	-	RJ10 – RS485 (Combus)
8 (D12)	LED1	Yellow – Ethernet 100BT
	LED2	Yellow – Ethernet Rx/Tx
	LED3	Green – Ethernet LINK
9 (K8)	-	100Mbit Ethernet
10 (SW1)	-	Reset switch (reboot)
11 (K15)	-	Power supply **
12 (SW4)	-	Alt-mode switch (test mode) *
13 (D2)	LED1	Red – input 2 (on/off)
	LED2	Red – input 1 (on/off)
	LED3	yellow – Txd(HW -> Contr.board)
	LED4	yellow – Rxd(Contr.board -> HW)
	LED5	Blue-Status(HWcontr.->flashing)
	LED6	Green – Power (on/off)
	LED7	Red – Control board error
	LED7	Red – Control board error
14 (K1)	LED8	Red – CAN bus error
		3rd party reader(s) RS232

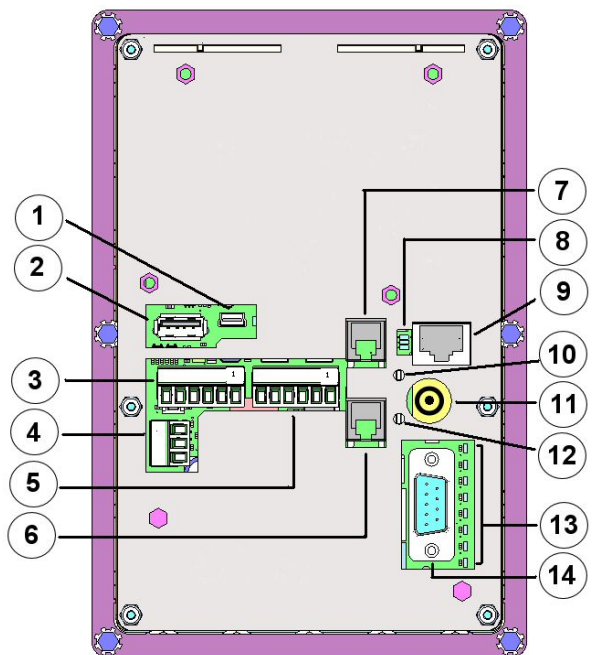
* alleen voor test doeleinde.

** zie appendix 9 voor maximum specificaties.

Terminal connections for coin acceptor and coin hopper. ***

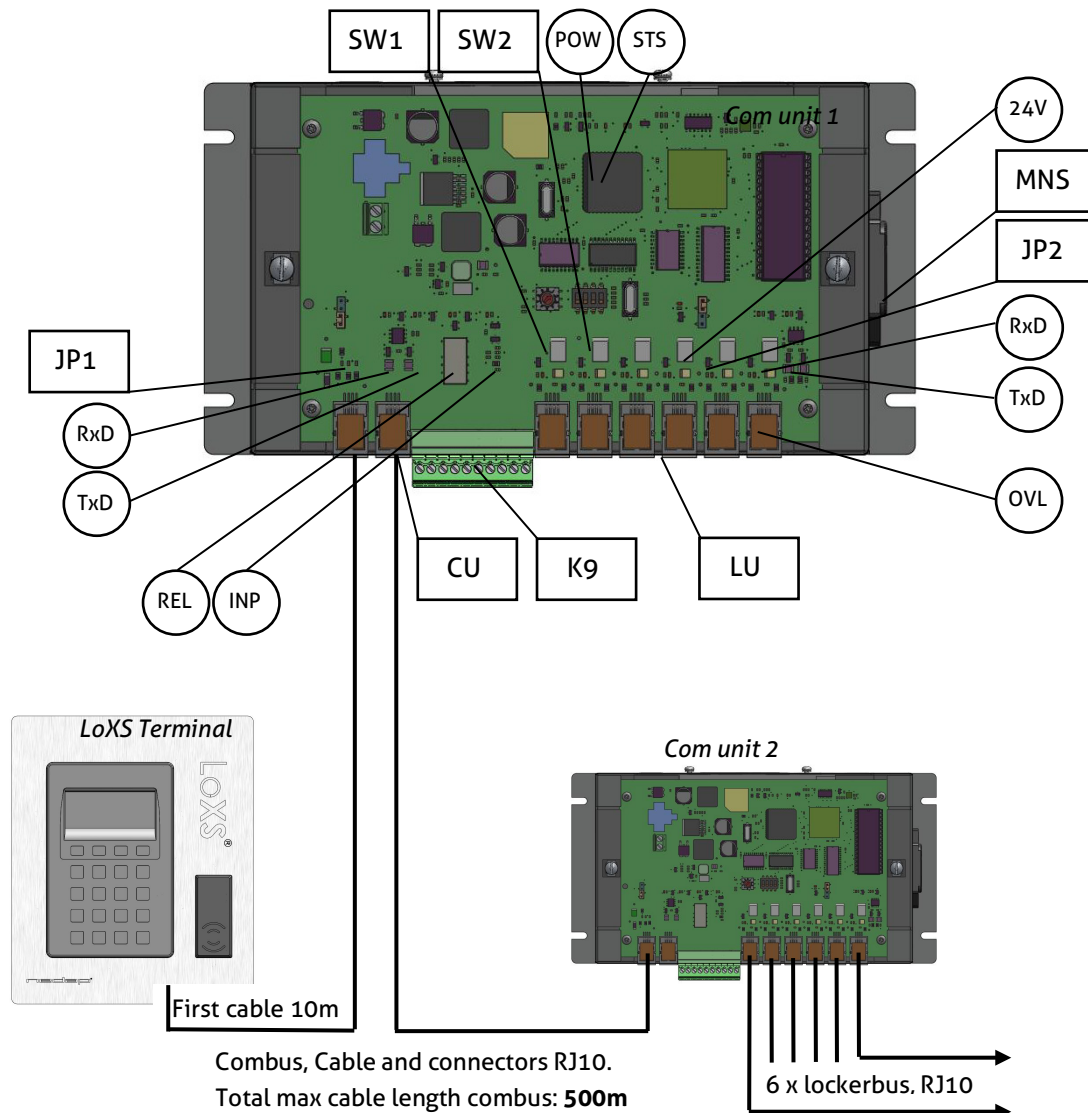
Item:	Pin:	Definition:	Function:
3(K14)	3	Digital input 1	Floating contact coinacceptor (NO)
	4	Ground (GND)	Floating contact coinacceptor (COM)
	5	Digital input 2	Coin dropped, output from coin hopper
	6	Ground (GND)	Gnd power supply
5(K12)	2	COM – Relay1	Gnd power supply
	3	NO – Relay1	Start pulse, to coin hopper

*** Mechanische muntproever met maakcontact en Cube Hopper MKII met stuurprint 10-0150-1.





Appendix 2 Installation schematic

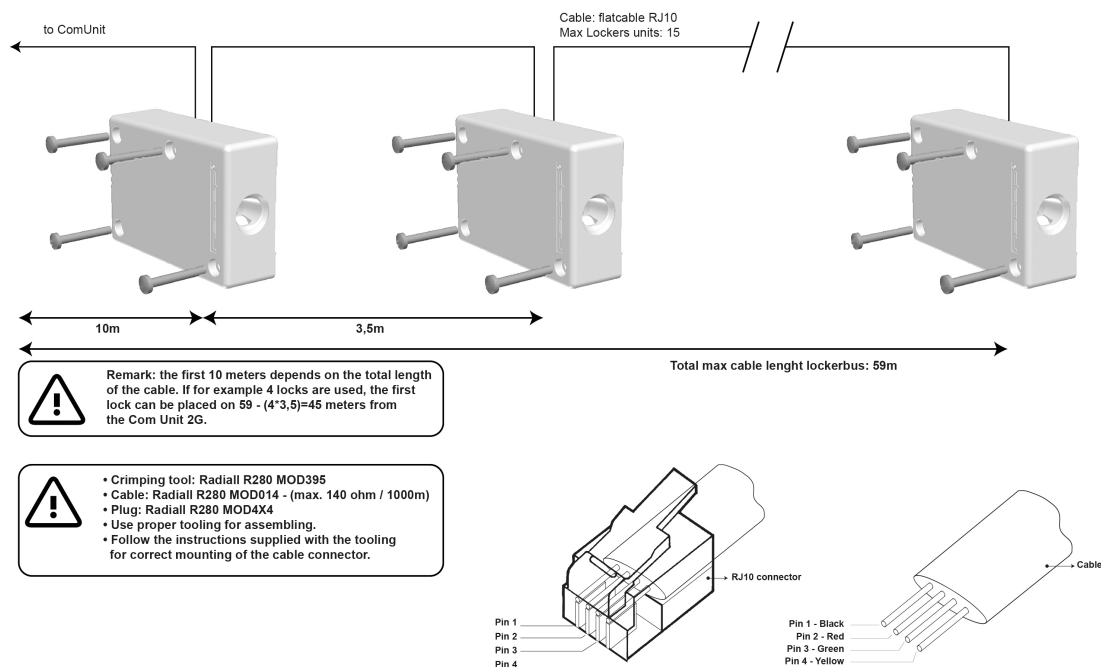


LEDs		Connectoren		Jumpers en Schakelaars	
POW	Power	MNS	Power	SW1	Address 1 .. 9
STS	Status	LU	6 x Lockerbus (RJ10)	SW2	Spare. 1 .. 4 = off
24V	Locker voltage	K9.1	+ Combus	JP2	Voltage lockerbus 15/24V *
RxD	Receive Lockerbus	K9.2	A line RS485	JP1	Terminator Combus
TxD	Transmit Lockerbus	K9.3	B line RS485		
OVL	Overload Lockerbus	K9.4	- Combus		
INP	Entrystatus	K9.5	Shielding Combus		
REL	Relaisstatus	K9.6	NC alarmrelais		
RxD	Receive Combus	K9.7	NO alarmrelais		
TxD	Transmit Combus	K9.8	COM alarmrelais		
		K9.9	Input TBD		
		K9.0	Gnd		
		CU	2 x Combus (RJ10)		

* 15 Volt for Locker Unit III and 24 Volt for Locker Unit IV and Mifare.

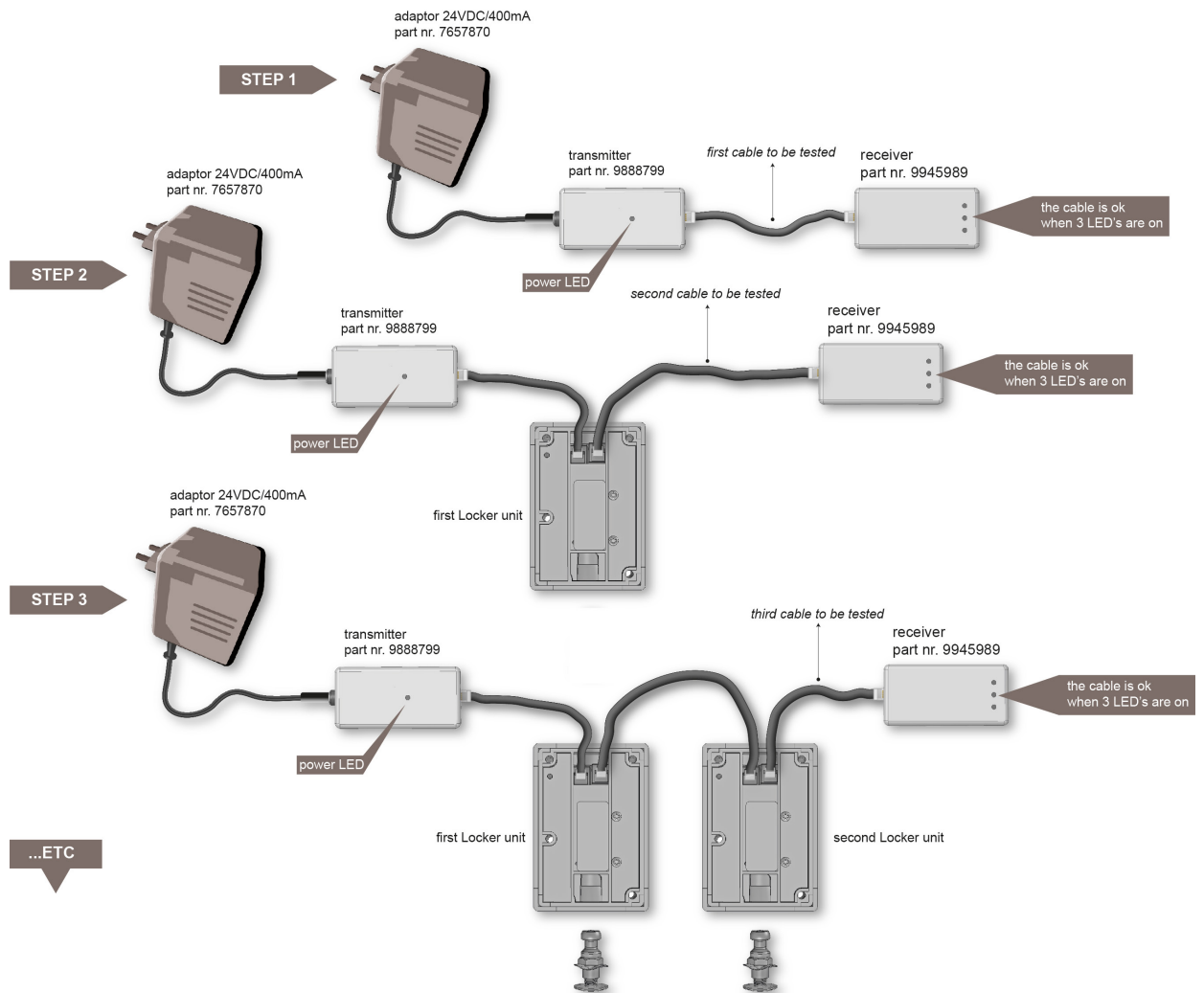


Appendix 3 Lockerbus





Appendix 4 Cable testing





Appendix 5 Addressing locker units

Lockers with a reader can be assigned a system address through the use of a binder. For the locker unit Smart a different procedure needs to be applied. Therefore this appendix is split up in two parts:

- 5A Lockers with reader
- 5B Locker unit Smart

5A - Assigning addresses to lockers with a reader

The binder unit (9887075) is used to wirelessly provide the locks with a system address. The locks need to be powered before starting the addressing procedure.

Select the preferred address with the tumble wheels on the binder unit.

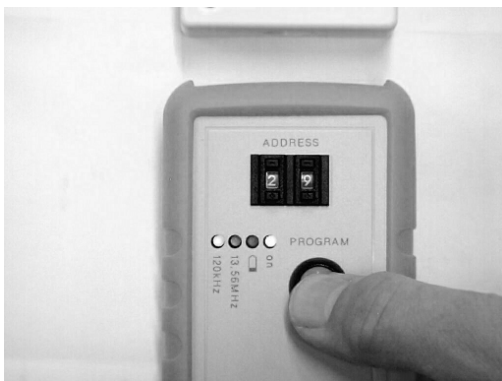
Press the power button while keeping the binder unit close to concerned lock to keep the binder unit in reach of the integrated reader.

The red LED light starts flashing if the new address is received and stored correctly.

Make sure that all locks connected to the same COM-unit receive a unique address between 1 and 62.

Address 90 is reserved for resetting the small lock to factory settings.

The binder is automatically off when it is out of range of the small lock. The light signalling the 'low-battery' flares when the battery is almost empty.



Addressing the Nedap Locker Units III en IV



Addressing the Mifare lock.

The light with caption 120 kHz signals that a lock with a 120 kHz frequency is close to the binder; this can be either Locker Unit III or Locker Unit IV.

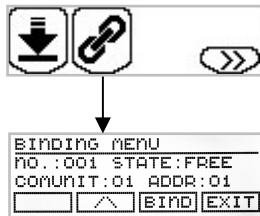
The light with caption 13,56 mHz signals that a Locker Unit Mifare is close to the binder.

In this manner one can also determine whether or not locks emit sufficient transmission signals and whether there are any interfering metal parts nearby.

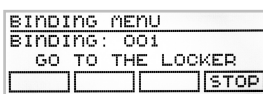


5B - Assigning addresses to Smart locks

After the hardware has been added the process of assigning system addresses to the locker unit Smart can commence. All LEDs are flashing green at a slow pace. Select the shackles icon.



Select the locker number that needs to have a system address assigned and press BIND. The green LEDs now start to flash faster.



Go to the locker with the number indicated by the terminal and execute the next few steps:

1. In case the locker is open, close it first.
2. Open the locker: the green LED goes out; wait for it to start flashing again.
3. Close the locker: the green LED goes out again; wait for it to start flashing again.
4. Open the locker: the LED will now stop flashing and stay on in the colour of the present status (red or green).

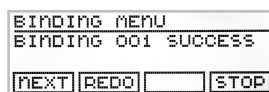
The LEDs of all locks that yet have to receive a system address once again slowly flash green.

When the red LED starts flashing an error has occurred. This happens when the locker door is opened and closed too quickly. If this happens, retake steps 1 to 4 as described above.



The execution of these steps, in this order, is necessary to ensure that every Smart lock receives the appropriate system address and to ensure that the terminal knows when this has been done and the next locker can be assigned one.

The following screen is shown when the procedure has been completed successfully:



Press 'Next' to go to the next locker number, 'Redo' to start over with the same locker number or 'Stop' to close this screen.

'Stop' can also be used to abort the procedure intermittently.



Appendix 6 Assembly rules for the LoXS terminal

The terminal is designed to offer maximum installation flexibility. However, we strongly advise you to observe some recommendations concerning PIN code operation, to optimize convenience and safety.

We advise you to install the terminal under a certain angle, preferably 45 degrees, to prevent people from copying someone's PIN code.

The most convenient installation height depends on the user group. Nedap advises a standard height of 135 cm from the floor to the centre of the terminal. However, the terminal needs to be installed lower if children or disabled persons are going to be using it.

Appendix 7 Dimensional sketches

The dimensional sketches of the various LoXS components are not a part of this manual. They have their own product codes:

- | | |
|---|----------------------------|
| ☐ LoXS terminal | document number: T1090-470 |
| ☐ Locker Unit III, IV | document number: 5262690 |
| ☐ Locker Unit Mifare | document number: 5277671 |
| ☐ Locker Unit Mifare Flush | document number: 5280591 |

Appendix 8 Electronic keys

Electronic keys Nedap

When the system is configured to work with Nedap keys the following subtypes are available:

- ☐ Nedap standard
- ☐ Marin EM4102
- ☐ Nedap RW80

Electronic keys Mifare.

When the system is configured to work with Mifare keys the following subtypes are available:

- ☐ Ultralight Card Serial Number
- ☐ Ultralight Sector Data
- ☐ Classic Card Serial Number
- ☐ Classic Sector Data
- ☐ DESfire Card Serial Number
- ☐ DESfire File Data
- ☐ Plus

Besides Mifare the following keys are also available:

- ☐ ISO 15693
- ☐ HID iClass Card Serial Number
- ☐ ICODE-I Card Serial Number
- ☐ ICODE-SLI Card Serial Number
- ☐ Legic Advant Card Serial Number



Appendix 9 Technical specifications

LoXS Terminal / MIFARE

Nedap product no	▪ 9561889 / 9561862
Dimensions	▪ 53 x 177 x 120mm (hxbxd).
Housing	▪ Stainless steel / Aluminium
Temp. range	▪ Operating from 0 to 60°C Storage from 0 to 75°C
Humidity	▪ 10% to 90% RH (Non-condensing)
Approvals	▪ CE: - Safety: EN60950 (2006) + A11(2009) + A1(2010) + A12(2011) - EMC emission: EN61000-6-3 (2007) EN61000-3-2 (2006) + A1(2009) + A2(2009) EN61000-3-3 (2008) - EMC immunity: EN61000-6-2 (2005)
Power	▪ 24 Vdc (12Watt max).
Power supply	▪ MEAN WELL. Model: FRA024-S24-I Input: 100-240Vac 50/60Hz. (Class II) Output: 24Vdc – 1A 24W max. (NEDAP Article no. 9560483)
Fuse	▪ 1A. Self-resetting fuse (PPTC)
Terminals	▪ 1x COM DB9 Male RS232 2x RJ11 RS485 1x USBa 1x USBb 1x RJ45 100-BaseT Ethernet 1x power-jack supply connector 1x 3-pol. not-isolated CAN connector (inactive) 1x 6-pol. digital inputs & 12Vdc output connector (inputs inactive) 1x 6-pol. double NO/NC relay contacts (inactive)
Relay contact (switch capabilities)	(for more information: see appendix 1) ▪ 15 VA (max.) where a maximum voltage of 30V(ac/dc) is allowed.
Installed battery	▪ CR2032 lithium coin cell battery (3V)
Altitude	▪ Maximum useable height is 2.000 meters above sea level (850 mbar)
MTBF	▪ 2,8 Year

WARNING

- The LoXS terminal holds a lithium coin cell battery. Replacing this battery incorrectly and/or by other battery type than listed above, can cause a hazardous situation.
- Do not let foreign objects into the loXS terminal.

CAUTION

- In order to guarantee CE safety approval(s), all third party components connected to the product must be in compliance with the EN 60950-1 or similar EN standard.
- In order to guarantee CE safety and EMC approvals, always use the power supply mentioned in the specification above.

**NOTE**

- Do not block any ventilation opening of the LoXS terminal.
- The mains fuse/circuit breaker in the building has to comply with the country's (common) standard.

CLEANING

- The front of the LoXS terminal may be cleaned with a moist cloth. Use a dry cloth only, for cleaning the back panel.

COM-unit 2G

Nedap product no	▪ 9899197
Dimensions	▪ 230X120X90
Weight	▪ 1.2 kg
Housing	▪ Metal (powder coating) plastic front
Temperature	▪ Operating temperature from +10 to 40°C.
Relative air humidity	▪ 10% to 90% (non-condensing).
Standards	▪ CE: Safety EN60950. ▪ EMC: immunity EN50082-2, emission EN50082-1.
Input	▪ 100-240 VAC; 50/60 Hz; 60 W.
Efficiency	▪ 85%
Power connection	▪ IEC
Fuse	▪ Primary built-in (non-replaceable). Secondary: electronic limiter
Output capacity	▪ 50W
Lockersbus	▪ 6 x RJ10
Commbus	▪ 2 x RJ10
MBTF	▪ 25 Year



	Locker Unit III	Locker Unit IV	MIFARE Light Grey	MIFARE Charcoal	MIFARE FLUSH	locker unit Smart
Nedap product no	9891420	9945032	9871500	9961968	9207937	9981942
Dimensions	95 x 65 x 27mm					
Housing	ABS					
Weight	130 gram					
Protection	IP 30					
Colour	White	White	Grey	Grey	Grey	Black
LEDs	Red flashing	Red and Green				
Pulling resistance	> 200 kg					
Operating frequency	120 kHz	120 kHz	13.56 MHz	13.56 MHz	13.56 MHz	No RFID
Detection range for ISO card	>45mm	>45mm	> 30 mm	> 30mm	>30mm	Not applicable
Detection range for Keyfob and wristband	>35mm	>35mm	>20mm	>20mm	>20mm	Not applicable
Detection range for DESfire card	Not applicabl e	Not applicabl e	>15mm	>15mm	>15mm	Not applicable
Temp. range	Operating from 0 to 50°C Storage from -20 to 70°C					
Humidity	10% to 90% RH (Non-condensing)					
Approvals	CE: Safety EN60950, EMC: immunity EN50082-2, emission EN50082-1					
Power supply	15 VDC, 6mA average, 80mA peak	24 VDC, 19mA average, 95mA peak	24 VDC, 27mA average, 100mA peak			24 VDC, 19mA average, 80mA peak
Terminals	Two RJ10 connectors for supply and data, wired in parallel pinning: 1=+V, 2=data-a, 3=data-b, 4=0V					
MTBF	30 years	30 years	27 years	27 years	27 years	30 years

MIFARE Handle

- Dimensions
- Weight
- Housing
- 81 x 55 x 28 (71)
 - 140 gr including mounting plate
 - PC/ABS with microban - PUR – Ms + Ni

Pin set

- Nedap product no
- Material
- Weight
- 9891536 (short) / 9891544 (long)
 - Chrome plated brass
 - 115g



Appendix 10 Configuration sheet

Please indicate your configurations of the terminal below.

Basic setup

Default Language ☐ Nederlands ☐ English ☐ Deutsch ☐ Francais ☐ Italiano ☐ Espanol ☐ Portugs	Coins used ☐ No ☐ Yes, fixed price ☐ Yes time based	If Fixed Price, Coins rent ☐ No Coins ☐ 1 coin ☐ 2 coins
Operating Mode ☐ Standard Mode ☐ Toggle Mode ☐ Showcase mode	If Time Based, Number of coins ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Coins Deposit ☐ No Coins ☐ 1 coin ☐ 2 coins
If Standard Mode, Status Free Locker ☐ Unlocked ☐ Locked	If Time Based, Time coin [1-5] (min) ☐ __ min. ☐ __ min. ☐ __ min. ☐ __ min. ☐ __ min.	If Coins rent=1 or 2, Hopper present ☐ Yes ☐ No
Pincode ☐ Yes ☐ No		Automatic release ☐ Disabled ☐ At __: __ hour

Advanced setup

Second Language ☐ Nederlands ☐ Engels ☐ Deutsch ☐ Francais ☐ Italiano ☐ Espanol ☐ Portugs ☐ None	Alarm Timeout ☐ 10 sec ☐ 30 sec ☐ 1 min ☐ 2 min ☐ 3 min ☐ Endless	Locker Release ☐ Show menu ☐ Skip Menu ☐ After __ hours
Third Language ☐ Nederlands ☐ Engels ☐ Deutsch ☐ Francais ☐ Italiano ☐ Espanol ☐ Portugs ☐ None	Delayed deassign ☐ Disabled ☐ 30 sec ☐ 1 min ☐ 2 min ☐ 3 min ☐ 4 min ☐ 5 min ☐ 10 min	Enable In Use LED ☐ Yes ☐ No
Unlock time (long) ☐ 10 sec	Enable White list ☐ Yes ☐ No	LED intensity ☐ __ %
		Setup Nedap config [*]
		Third Party Reader ☐ TechnoGym ☐ TechnoGym Swipe ☐ Barcode Datalogic ☐ Pinpad ☐ HID Proxpro Serial ☐ TCP/IP (socket) [**] ☐ Other (CR/LF) [***]



☐ 20 sec	After Release All	☐ None
☐ 30 sec	☐ Clear whitelist	
☐ 40 sec	☐ Keep whitelist	Setup Mifare config [****]
☐ 50 sec		
☐ 60 sec	AEOS compatible	Contrast [display]
	☐ No	☐ __ %
Unlock time (short)	☐ Yes	
☐ 1 sec		
☐ 2 sec		
☐ 3 sec		
☐ 5 sec		
☐ 10 sec		
☐ 20 sec		

*** In case Setup Nedap Config = Yes**

Enable Nedap	Enable Nedap RW80	LED style
☐ No	☐ No	☐ Classic
☐ Yes	☐ Yes	☐ Red + Green
Enable EM4102	LF fieldstrength	
☐ No	☐ __ (0-100)	
☐ Yes		

**** In case Third Party Reader = Other (CR/LF) or TCP/IP (socket)**

Reader manufact no	Reader subtype no
☐ -----	☐ -----
[name]	[name]
☐ __ [number]	☐ __ [number]

***** In case Third Party Reader = Other (CR/LF)**

Baudrate	Parity	Reader manufact no
☐ 1200	☐ None	☐ -----
☐ 2400	☐ Even	[name]
☐ 4800	☐ Odd	☐ __ [number]
☐ 9600		
☐ 19200	Stopbits	Reader subtype no
	☐ 1	☐ -----
Databits	☐ 2	[name]
☐ 5		☐ __ [number]
☐ 6		
☐ 7		
☐ 8		

****** In case Setup Mifare Config = Yes**

CFG : -----	DESfire Reading	HID ICLASS Reading
[name]	☐ Disabled	☐ Disabled
DATE: -----	☐ CSN	☐ CSN
Mifare Reading	ISO15693 Reading	ICODE Reading
☐ Disabled	☐ Disabled	☐ Disabled
☐ CSN	☐ CSN	☐ CSN



Hardware configuration

Please indicate the numbers of the lockers and the address of each first and last locker connected to each COM-unit. If a COM-unit is connected to an interrupted locker series, enter the locker numbers of each series.

		<i>First locker</i>	<i>Last locker</i>	<i>Start address</i>
COM-unit 1	Series 1			
	Series 2			
	Series 3			
	Series 4			

		<i>First locker</i>	<i>Last locker</i>	<i>Start address</i>
COM-unit 2	Series 1			
	Series 2			
	Series 3			
	Series 4			

Device type

- ☐ InfoReader
- ☐ InReader
- ☐ OutReader
- ☐ UnlockReader
- ☐ DummyReader

Network setup

IP-address _ _ . _ _ . _ _ . _ _

Netmask _ _ . _ _ . _ _ . _ _

Gateway _ _ . _ _ . _ _ . _ _

MACaddress _ _ . _ _ . _ _ . _ _

Comments

.....

.....

.....

.....



Copyright

Copyright © Nedap N.V. All rights reserved. The information in this document is subject to change without notice, it is not to be reproduced in any way, in whole or in part, without the written consent of Nedap N.V. Nedap AEOS is a registered trademark of Nedap N.V. All trademarks referenced belong to their respective owners.

Disclaimer

Nedap N.V. has made every effort to ensure the accuracy of the information contained in this document. However, Nedap N.V. makes no representations or warranties whatsoever whether express or implied as to the accuracy, correctness, completeness or fit-for-purpose or suitability for the purpose of this product. You use the products at your own risk. Nedap N.V. excludes any liability to the maximum extent permitted by applicable law for the damages caused by errors or failures made during the installation or improper use of this product or by not applying the instructions stated in this document.

Nedap N.V. reserves the right to make improvements or amendments to this document and/or the products described therein at any time without any notification. The latest version of this document can be found on portal.nedapsecurity.com. Please download the latest version of this document and keep a copy for your own records.

This document can be published in various languages but only the English version will prevail. Nedap N.V. assumes no responsibility for any errors due to translations into other languages.

Nedap Security Management

P.O. Box 103

NL - 7140 AC Groenlo

+31 (0)544 471 111

info@nedapsecurity.com

www.nedapsecurity.com