

MREM 82 HIK-MF

MIFARE® & NFC reader modules for HIK panels

User's guide



techfass®

1 Content

1	Content.....	2
2	MREM 82 reader module description.....	3
2.1	MREM 82 HIK-MF module	3
2.2	Product versions	3
3	Technical parameters	4
3.1	Technical features.....	4
3.2	Identification by the cell phone with OS Android® 4.4+	5
3.3	Mechanical design	5
3.4	Cabling	6
3.5	Cable wiring	6
3.6	Wiring description	6
3.7	Standard connection	7
3.8	LED Indication	7
3.9	Installation instructions.....	7
4	Wiring diagram	8
4.1	Simple connection of MREM 82 HIK-MF and DS-KD8003-IME1 without POE	8
4.2	Connection of MREM 82 HIK-MF and DS-KD8003-IME1 with POE	9
4.3	Wiring diagram of MREM 82 in DS-KD8003-IME1I integrated in system APS mini Plus	9
5	Setting parameters of the reader module.....	10
5.1	Configurable parameters.....	10
5.2	Reader module parameters setting	11
6	Reader module functioning	11
6.1	“Door Open” function description	11
6.2	Current limit of OUT 1 and OUT 2.....	11
6.3	Function permanent door lock release according to a time schedule	12
6.4	Alarm states.....	12
6.5	Standard operating modes.....	13
6.6	Programming mode	13
6.7	ID expiration function	17
6.8	ID with Alarm flag function	17
6.9	Antipassback function	18
6.10	Disabling function	18
6.11	Online authorization	19
7	Simplified access rights evaluation	19
8	Declaration of conformity	20
9	Electrical waste.....	20
10	Legislation	20

2 MREM 82 reader module description

The **MREM 82 HIK** reader module (13,56 MHz reader with an embedded single door controller) are designed for connection to the RS 485 bus of the **APS mini Plus** access control system. The module is equipped with a Wiegand interface for connecting additional reader with Wiegand output (for double-sided door control). The reader modules are designed for installation in **HIK** entry panels of **CAME** audio and video systems, where they occupy only one module space. The modules are customized for power supply and control from CAME entry systems. Next to classic RFID cards or tags based on **MIFARE®**, **MIFARE® DESFire®** and **NFC¹⁾** tag technology, the reader is compatible with mobile phones equipped with NFC technology and minimum OS Android® 4.4 Kit Kat (or higher). **TF Mobile ID** application needs to be installed. The mobile phone can be used for identification instead of classic cards (card emulation mode).

Pic. 1: MREM 82 HIK-MF

2.1 MREM 82 HIK-MF module

The module is designed for an installation into the modular entry panel Hikvision, and is delivered directly in module DS-KD-M.

2.2 Product versions

13,56 MHz group

Product version	Product designation	System	Panel	Surface	Catalogue number	Module features	
						NFC	MIFARE®
	MREM 82 HIK-MF	APS mini plus	HIKVISION	Brushed aluminum	53482024	✓	✓
	WRE 82 HIK-MF	X	HIKVISION	Brushed aluminum	51482024	✓	✓
	NREM 82 HIK-MF	APS 400	HIKVISION	Brushed aluminum	54482024	✓	✓

Table 1: The overview of the product versions for DS-KD-M module.

Notes:

¹⁾NFC – card emulation mode by cell phone or tag; MIFARE® – MIFARE® family UID media reading.

MIFARE®, MIFARE® Classic® and MIFARE® DESFire® are trademarks of NXP B.V. Android® is a trademark of Google LLC.

DS-KD-M represent the RFID module housing of Hikvision modular entry panel.

3 Technical parameters

3.1 Technical features

Technical features	Supply voltage		8 ÷ 28 VDC
	Input current	Nominal	42 mA @ 12V, 23mA @ 24 V
		Peak	124 mA @ 12V, 62mA @ 24 V
	Typical power		0,5 W
	Peak power		1,5 W
	ID technology	MIFARE®, NFC (13,56 MHz)	3 cm (card ISO MIFARE Classic®)
	Real-time clock		Yes, with 24 hrs. back-up
	Memory	Cards	2,000 ID, 2 programming cards
		Events	3,400
		Time schedules	64
	Inputs	1 st input	Logical potential-free contact
		2 nd input	Logical potential-free contact
	Output	Door lock ³⁾	1x open collector 0V active, max. 1A, 24V
		Alarm	1x open collector 0V active, max. 1A, 24V
	Signalization		1x LED 1x PIEZO
	Tamper protection		Optional connection to IN2
	System communication interface		RS-485
	Alternative data communication interface		Wiegand

Table 2: Technical features

³⁾ The DC type of door lock has to be used only.

3.2 Identification by the cell phone with OS Android® 4.4+

It is possible to use a cell phone equipped with NFC technology, operating system Android 4.4 Kit Kat (or higher) and installed *TF mobile ID* application for identification instead of the cards or chips. You can download the application on Google Play for free.



Pic. 2: Google Play and TF mobile ID

3.3 Mechanical design



Pic. 3: MREM 82 HIK-MF

Mechanical design	Weight		160 g
	Operating temperature		-25 ÷ 70 °C
	Humidity		5 ÷ 95%, non-condensing
	IP code		IP 65
	IK code		IK 07
	Cable length		2 x 0,4 m
	Color	MREM 82 HIK-MF	Black
	Dimensions (Height x Width x Depth)		98,5 x 100 x 33,7 mm

Table 3: Mechanical design

3.4 Cabling

The cable consists twelve wires AWG 26. The wires are not dedicated for heavy loads, OUT1, OUT 2 and appropriate power supply and ground wires are designed to be connected to standard electromechanical mortise lock, door openers or magnets where the DC current does not exceed the load of 1A. For inputs it is recommended to use signal ground (brown wire nr. 10).

3.5 Cable wiring

OUT2	OUT1	GND	GND	12V
1	2	3	4	5

Table 4: Power supply cable wiring

W1/B	W0/A	IN2	IN1	GND	B	A
6	7	8	9	10	11	12

Table 5: Data cable wiring

OUT 2 (Alarm)	OUT 1	GND	GND	8-28V	W1/B	W0/A	IN 2	IN 1	GND	RS-485 B	RS 485 A
---------------	-------	-----	-----	-------	------	------	------	------	-----	----------	----------

3.6 Wiring description

Wiring description	#	Color	Purpose
	1	Pink	Output 2; open drain, 1A (Alarm output)
	2	Violet	Output 1; open drain, 1A (Lock)
	3	Blue	GND power supply
	4	Blue	GND power supply
	5	Red	+ 8 ÷ + 28 VDC
	6	Brown-green	WIEGAND data 1 / alternatively RS-485
	7	White-green	WIEGAND data 0 / alternatively RS-485
	8	Grey	Input 2 (IN2), configurable function
	9	Yellow	Input 1 (IN1), configurable function
	10	Brown	GND (0V) signal ground
	11	White	RS-485 B
	12	Black	RS-485 A

Table 6: Wiring description

3.7 Standard connection

Connection	Input 1	Door contact, active when door closed; REX button
	Input 2	Request to exit button or handle contact, 0 V signal when button or handle active; Tamper; Disabling function
	Output 1 (OC)	Door lock control open collector

Table 7: Standard connection

The door monitoring contact (IN1) is operational after its first change of status since switching on the module. Full door lock timing acc. to *tab. 9* is used when the door status contact is not installed and no Door Forced and Door Ajar alarms are triggered.

3.8 LED Indication

LED indicators	Red	Continuously lit	Online operating mode via RS 485
		Flashing with 4 s period	Offline operating mode
	Green		ID media reading
	Red/Green switching		Address setting mode, RS 485 bus testing
	Yellow	Continuously lit / flashing	Programming mode
		Short flashing with 1s per.	Indicating door lock release

Table 8: LED indication

3.9 Installation instructions

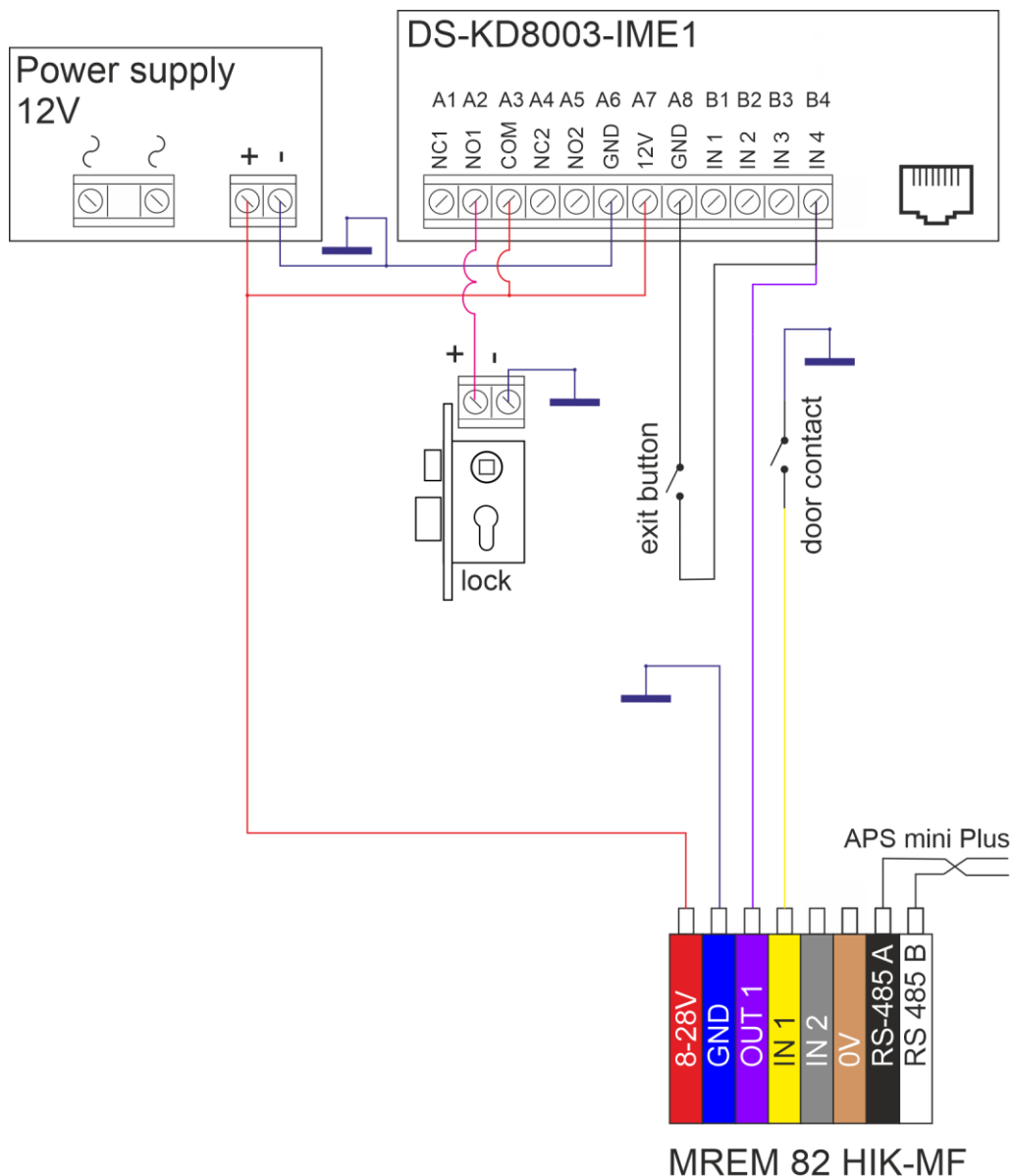
Generally, the noise can influence the reading functionality of the reader, so it is recommended to check the place of installation if there could be some source of noise.

The reader uses passive RFID technology on 13,56 MHz frequencies, which could be sensitive to RF noise sources, either radiated noise or conducted noise to the cable. This noise could be generated by other equipment, which can generate strong electromagnetic field or by noisy power supply, which inject noise to the cable. If there are any doubts, it is recommended to perform a practical test before final mounting.

4 Wiring diagram

4.1 Simple connection of MREM 82 HIK-MF and DS-KD8003-IME1 without POE

One of the simplest wiring of MREM 82 HIK-MF and DS-KD8003-IME1 together is to use OUTPUT 1 of MREM 82 HIK-MF to short-circuit the exit button input of DS-KD8003-IME1. The 12V power supply can be used to power both, MREM 82 HIK-MF and DS-KD8003-IME1 module.



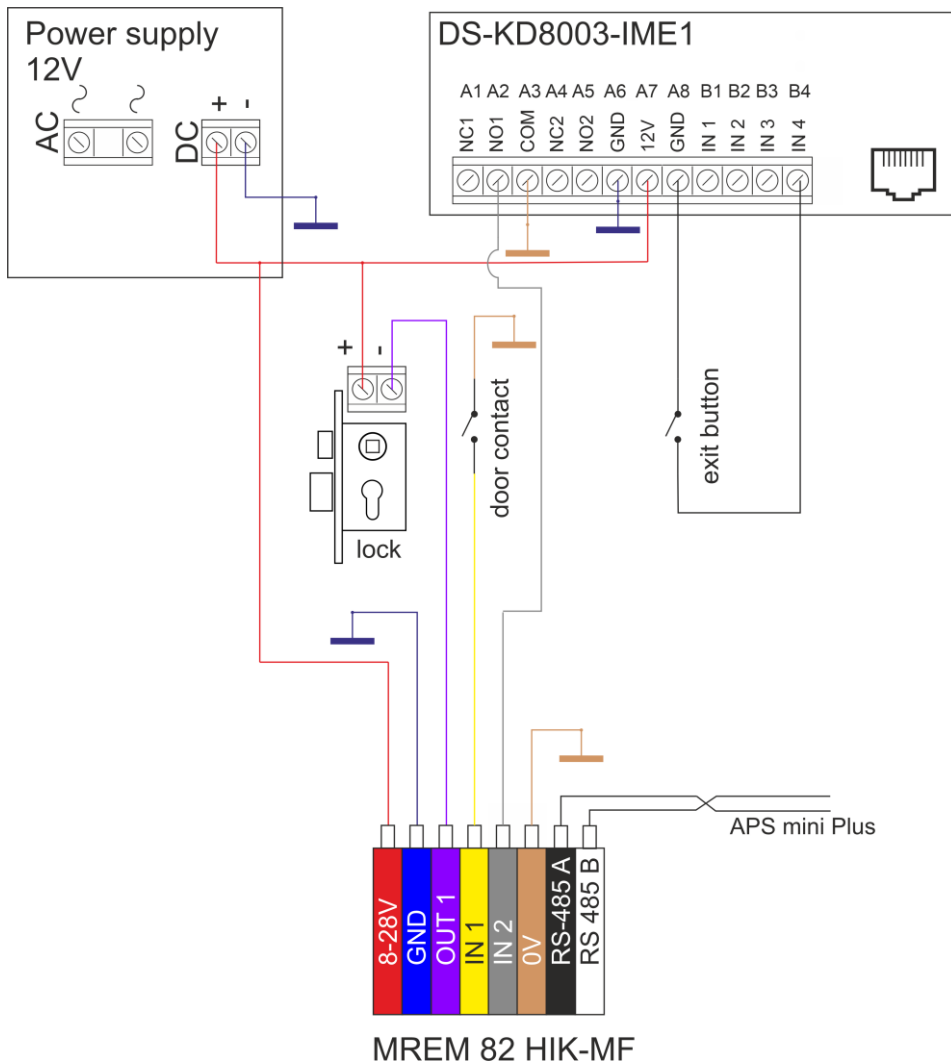
Pic. 4: Wiring diagram of MREM 82 HIK-MF and DS-KD8003-IME1 module for simple applications like family houses. RS-485 can be connected to LAN converter APSLAN to connect to the PC.

4.2 Connection of MREM 82 HIK-MF and DS-KD8003-IME1 with POE

In case of POE power supply, the 12V power supply has to be taken from the internal 12V wiring system of the DS-KD8003-IME1. The wiring stays the same as 4.1.

4.3 Wiring diagram of MREM 82 in DS-KD8003-IME1 integrated in system APS mini Plus

In larger application the MREM 82 HIK-MF reader can be a part of APS mini Plus access control system backed up with a battery. In this case, the power supply of access control system is separated from the power supply of the intercom system to be able to control the door when the main power grid is off and the intercom is off.



Pic. 5: Wiring of MREM 82 HIK-MF as a part of battery power backed up system APS mini Plus.

5 Setting parameters of the reader module

5.1 Configurable parameters

Configurable parameters	Parameter		Possible range	Default setting
	Door lock release time		0 ÷ 255 s	7 s
	Door lock control setting		Direct / reverse	Direct
	Door lock relay function setting		Standard / toggle / pulse	Standard
	Permanent door lock release according to a time schedule		Never / Schedule index	Never
	Door lock status indication		YES / NO	NO
	Acoustic signal of door lock release		YES / NO	YES
	Door ajar time		0 ÷ 255 s	20 s
	First input configuration		Door contact / REX button	Door contact
	Second input configuration		REX button / handle contact / external tamper / tamper / disabling function	REX button
	Acoustic signalization time - Forced door		0 ÷ 255 s	30 s
	Acoustic signalization time – Door ajar		0 ÷ 255 s	0 s
	Acoustic signalization time – APB alarm		0 ÷ 255 s	0 s
	Signalization time – Card alarm		0 ÷ 255 s	30 s
	Antipassback function setting		See <i>chapter 6.10</i>	Disabled
	Automatic summer time adjustment		YES / NO	YES
	Release lock with REX button when tamper alarm active		YES / NO	YES
	Online authorization timeout		0 ÷ 25500 ms	800 ms
	Standalone authorization after timeout		YES / NO	YES
	Saving events in the module's archive	Door opened	Enabled / Disabled	Enabled
		Door closed	Enabled / Disabled	Enabled
		Input 2 On	Enabled / Disabled	Enabled
		Input 2 Off	Enabled / Disabled	Enabled
		Strike released	Enabled / Disabled	Enabled
		Strike closed	Enabled / Disabled	Enabled

Table 9: Configurable parameters

5.2 Reader module parameters setting

Detailed instructions for setting reader module parameters are described in the *APS Reader* configuration program user's guide available at the address http://www.techfass.cz/files/m_aps_miniplus_reader_en.pdf.

6 Reader module functioning

The reader module supports the following functions:

- Standard "Door Open" function.
- Door status monitoring.
- Exit-devices contact monitoring.
- Acoustic signalization (and online) activated when any alarm condition occurs.

The "Door Open" function can be activated in 3 different ways:

- Reading a valid ID (card, key fob...).
- Pressing the exit button (according to configuration) – cannot be used in alarm condition.
- Via communication line (program request).

6.1 "Door Open" function description

In case the *standard function of the door lock relay* is set, the door lock is *released* and the *beeper activated* (when not disabled) when the "Door Open" function is activated. Both outputs stay active until the door is opened or the preset door lock release time has elapsed - see *configuration table*.

In case the *toggle function of the door lock relay* is set, the door lock relay status is *switched* and the *beeper* is *activated* (when not disabled) when the "Door Open" function is activated. The beeper stays active until the door is opened or the preset door lock release time has elapsed - see *configuration table*. The door lock relay status remains unchanged until another "Door Open" function is activated.

In case the *pulse function of the door lock relay* is set, the door lock relay status is switched for the time defined by the *Pulse width* parameter (ms) after the Door Open function is activated.

In case the standard function of the door lock relay is set, reading a valid card during door lock release resets the door lock release time.

6.2 Current limit of OUT 1 and OUT 2

There is a current limit protection on both outputs, 1 A. In case of capacitive load, the current limit can be activated and disable the output. If there is a short current peak, it is possible to turn on so called "*blanking time*". This function disables the current limit protection for the period set in the software to handle this short current peak. After this period the current protection get back on its limit 1 A.

By default, the blanking time is set to 6µs for the door lock output, and bit used for the alarm output.

6.3 Function permanent door lock release according to a time schedule

When the function is set, the door lock is permanently released when relevant time schedule is valid. Reading a valid ID is standardly announced via the communication line (in online operating mode). The forced door alarm cannot be raised when the door lock is permanently released.

The permanent door lock release function and the toggle function of the door lock relay are mutually exclusive.

6.4 Alarm states

The reader module can get in following alarm states:

- 1) Forced door alarm
- 2) Door ajar alarm
- 3) Antipassback alarm (Time APB alarm, Zone APB alarm)
- 4) ID with Alarm flag alarm

Alarm state reporting is performed as follows:

- Via communication line (statuses 1, 2, 3, 4)
- By acoustic signal (beeper) (statuses 1, 2, 3).

Alarm signaling via communication line requires online running PC with relevant software suitable for online operation (APS Administrator).

Two ways of acoustic signaling is carried out:

- Steady signal (tamper).
- Intermittent signal (forced door and/or door ajar, APB alarm).

Acoustic alarm signaling is stopped after a valid ID is presented or pre-set time interval is elapsed, see the configuration table.

If any of the relevant alarm states (*with setting of the signaling timer > 0*) occurs, the alarm state is announced on the communication line.

After terminating all alarm conditions the alarm status announcement is deactivated.

The alarm signaling is triggered by any alarm condition.

6.4.1 Forced Door alarm

The “Forced Door” alarm state is activated when the door is opened without activating the “Door Open” function. The only exception is opening the door with the second module input IN2 active and configured as a handle contact.

6.4.2 Door Ajar alarm

If the door stays open until the pre-defined Door ajar timeout expires – see *Tab. 9*, the “Door Ajar” alarm is activated.

6.4.3 Antipassback alarm

The *Antipassback alarm* is raised when an ID is read during the *Time APB* counter is running or when the ID is blocked by a *Zone APB*.

6.4.4 ID with Alarm flag alarm

ID with Alarm flag alarm occurs when an ID with the Alarm flag is read.

6.4.5 Reading ID during alarm state

Reading an ID doesn't affect the alarm state, reading a valid ID only terminates the acoustic alarm announcement followed by “Door Open” function. Reading an invalid ID only interrupts the acoustic announcement of the alarm state while signalinging “Invalid ID”.

6.5 Standard operating modes

The reader module can be in either *online* or *offline* operating mode. The module's functionality is identical in both operating modes; the events archive is read from the reader module's memory when the module goes online. When a programming card is read (while in either online or offline mode), the module goes into programming mode.

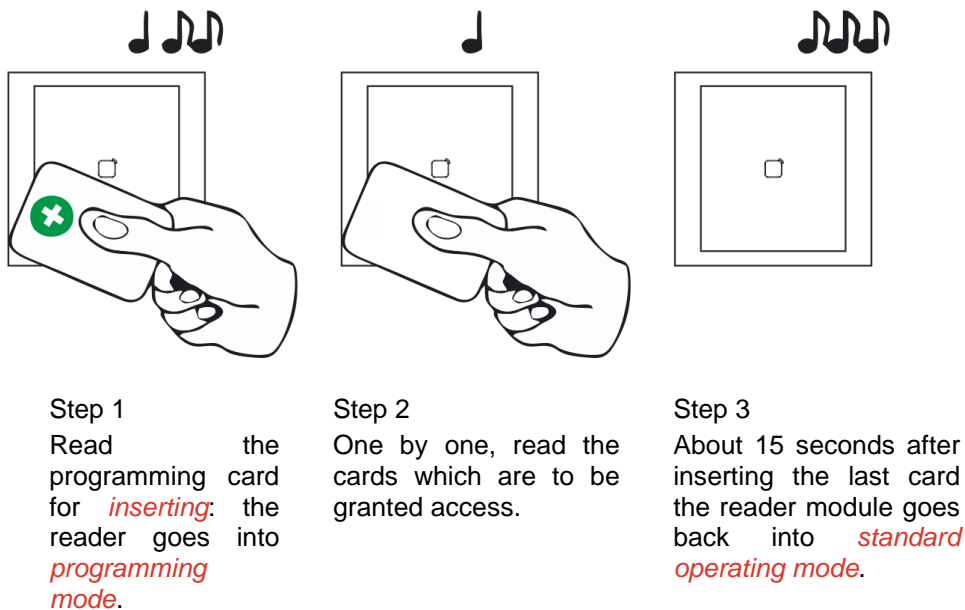
6.6 Programming mode

The module enters programming mode by reading one of the two *programming cards* (cards “+” and “-“). The programming mode cannot be entered while the module is in hardware address setting mode (for modules with HW address setting via the communication line). The module's functionality in programming mode can be seen in *pictures 5 a-d*.

It is not possible to use time schedules when inserting cards in programming mode, therefore cards are always valid.

6.6.1 Inserting cards into the reader's memory

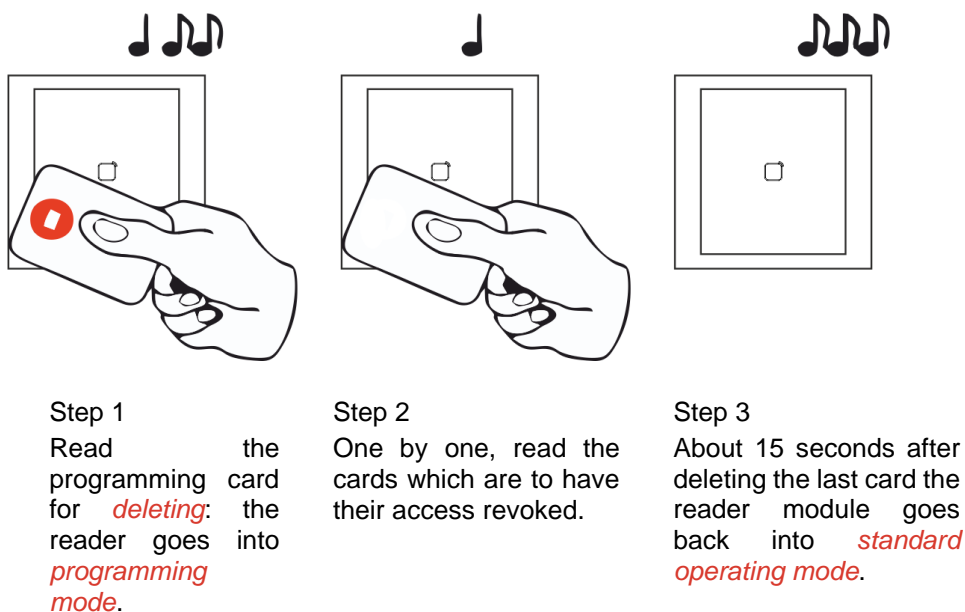
Follow these steps for inserting cards into the reader module's memory:



Pic.6 a): Inserting cards

6.6.2 Deleting cards from the reader's memory

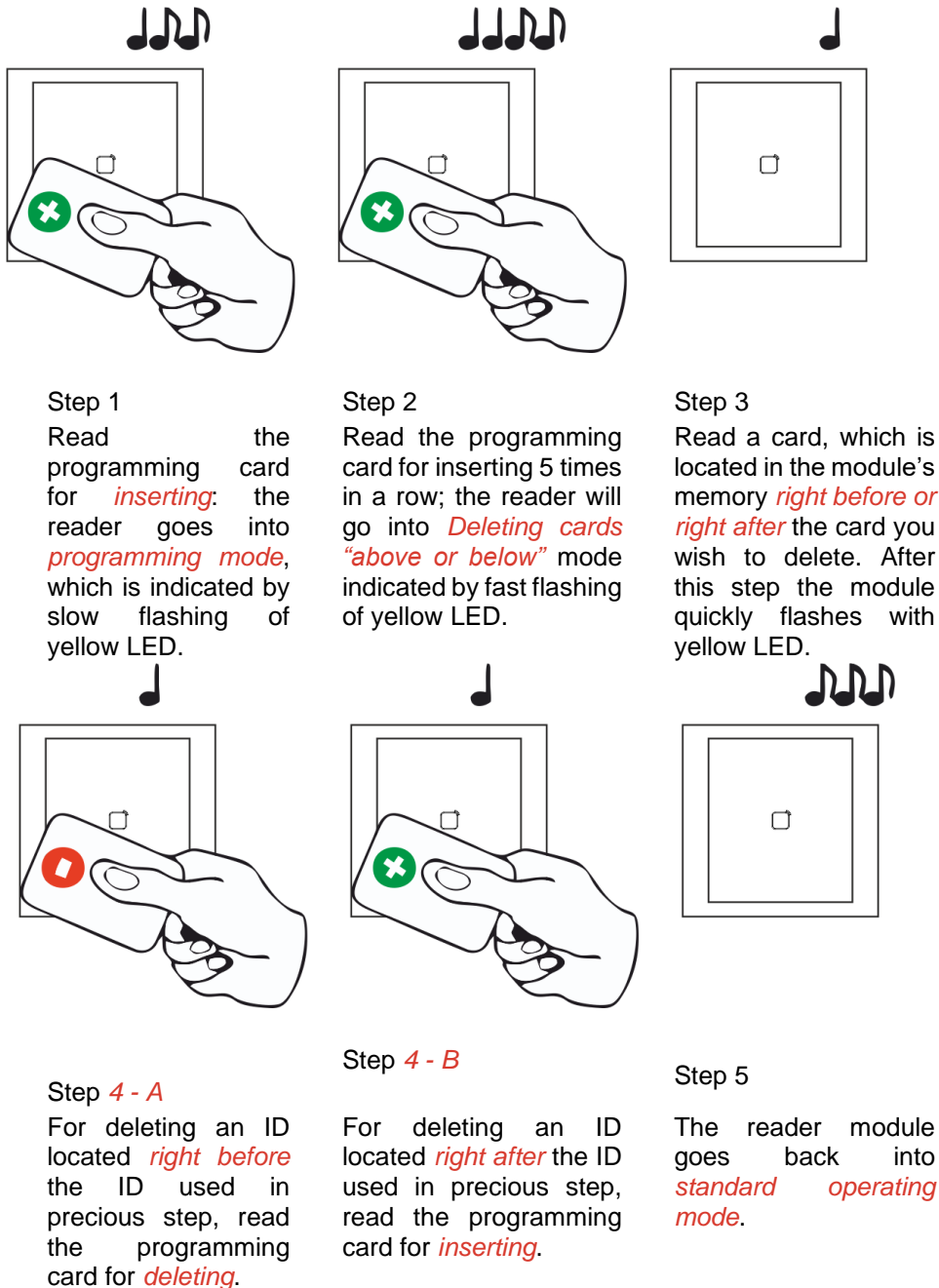
For deleting the cards from the reader module's memory use following steps:



Pic.6 b): Deleting cards

6.6.3 Deleting cards „above or below“

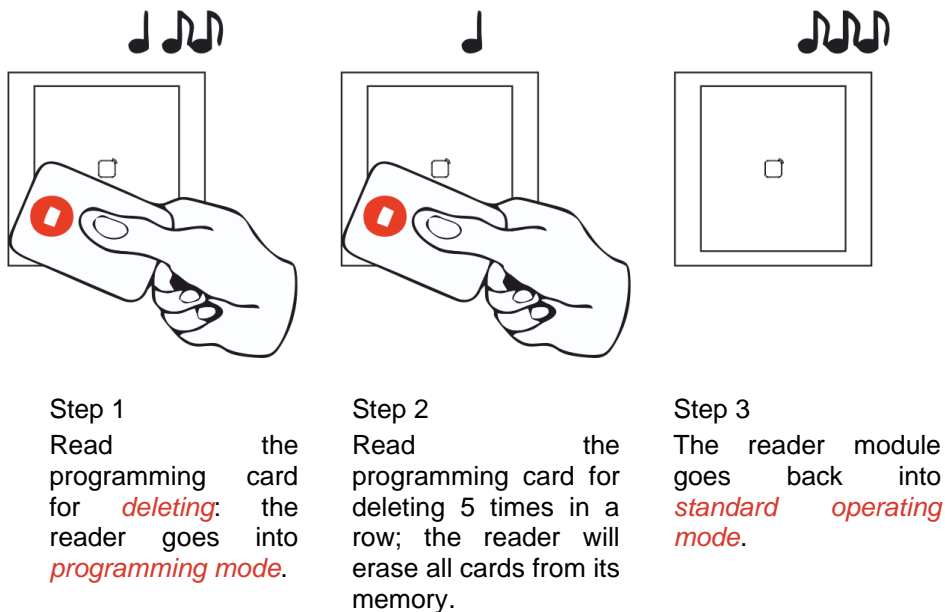
If a user loses his ID medium, it is usually impossible to delete the ID from the memory with the procedure described in the previous chapter, since the medium is no longer available (with an exception of entering the code at the keypad). Following procedure can be used for deleting such ID. The procedure *requires using an ID medium*, which was inserted *right before or right after the ID medium*, which should be deleted.



Pic.6 c): Deleting cards "above or below"

6.6.4 Deleting all cards from the reader's memory

Follow these steps for deleting all cards from the reader module's memory:



Pic.6 d): Deleting all cards

6.6.5 Recommended method for access rights management (using prog. cards)

In case of managing access rights of plenty of users (using programming cards only), it is appropriate to establish a table, which summarizes operation with the reader module memory. All operations (adding and deleting cards) should be stored in the table. Following example shows correct usage of the programming cards and proper filing of the actions:

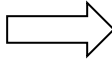
- Inserting *5 new cards* using the procedure from *chapter 6.6.1 – Read + (inserting) programming card*, read *cards 1-5*, after 15 s the programming mode is exited, *create a table*.

position	card
1	card 1
2	card 2
3	card 3
4	card 4
5	card 5

Pic.6 e): Table after inserting 5 cards

- Card 3 gets lost* – Delete it *using the card 4*, which is available, and using the procedure from *chapter 6.6.3 – Read + (inserting) programming card*, then *5x + (inserting) programming card* again, then *card 4*, and finally – *(deleting) programming card*. Register the change in your table.

position	card
1	card 1
2	card 2
3	card 3 (lost)
4	card 4 (available)
5	card 5

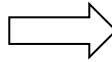


position	card
1	card 1
2	card 2
3	card 3
4	card 4
5	card 5

Pic.6 f): Deleting card 3 using the card 4, table after deleting card 3

Card 4 gets lost – Delete it *using the card 2*, which is available, and using the procedure from chapter 6.6.3 – Read + (inserting) programming card, then 5x + (inserting) programming card again, then *card 2*, and finally + (inserting) programming card again. *Register the change in your table.*

position	card
1	card 1
2	card 2 (available)
3	card 3
4	card 4 (lost)
5	card 5



position	card
1	card 1
2	card 2
3	card 3
4	card 4
5	card 5

Pic.6 g): Deleting card 4 using the card 2, table after deleting card 4

- It is necessary to **add another card** (card 6). We proceed with the procedure from chapter 6.6.1 again. 1 – Read + (inserting) programming card, read *cards 1-5*, after 15 s the programming mode is exited. *Register the change in your table.*

position	card
1	card 1
2	card 2
3	card 3
4	card 4
5	card 5
6	card 6

Pic. 6

h): Table after inserting card 6

A new card is always inserted at the position after the last inserted card. In case of deleting all cards using the procedure described in chapter 6.6.4, it is necessary to create a new filing table.

6.7 ID expiration function

It is possible to set an **Expiration date** for every **ID** stored in the module. When the date occurs, the ID becomes invalid (expired). The expiration evaluation is performed on every date change in the module's RTC and when the access rights are downloaded.

6.8 ID with Alarm flag function

This function is implemented since the FW version 5.0.

It is possible so set an **Alarm – ID flag** for every **ID** stored in the module. When the ID is read, relevant alarm is raised for preset time.

6.9 Antipassback function

The Antipassback function is defined in two ways:

- **Time APB** – user cannot repeatedly use his ID for defined time
- **Zone APB** – user cannot repeatedly enter an area, where he is already present

The Antipassback function is used *only for the users*, whose access is driven by a *time schedule*. The users with access always granted are not affected by the Antipassback function.

The Antipassback flags for an *ID* can be *reset* by *inserting the ID again* with use of the *programming cards* (offline solution). *All Antipassback flags* are also *reset* whenever new *access rights data are downloaded* from the program.

Both Zone and Time Antipassback flags are written either immediately *after an ID is read*, or after relevant *door is opened* (relevant input is disconnected).

6.9.1 Time Antipassback

The *Time Antipassback* is defined by the *ABP timer initial value* (in minutes), which is set to the ID after passing at the reader module. If the users uses the ID at the address during the timer for the ID is running, the Time APB alarm is raised. Following parameters affect the Time APB function:

- **APB timer initial value** – defines the Time APB flag (timer) value set to the ID after passing at the reader module. If a user uses the ID again before the timer elapses, Time APB alarm is raised.
- **Open door after APB time alarm** – if the option is enabled, the Door open function is performed after the Time APB alarm is raised.

6.9.2 Zone Antipassback

The *Zone Antipassback* is defined by *enabling the option* for the relevant address. The Zone APB flag is set for the ID when passing at the reader module. If a user uses the ID again when the Zone APB flag is set, the Zone APB alarm is raised. Following parameters affect the Zone APB function:

- **Enabled** – enable/disable general Zone APB flag setting.
- **Enable in offline mode** – if the option is not set, the module operates in offline mode like if the APB function was not implemented.
- **Open door after APB Zone alarm** – if the option is enabled, the Door open function is performed after the Zone APB alarm is raised.

6.10 Disabling function

This function is implemented since the *FW version 5.08*.

The *module disabling function* can be set at the second input. The logic of the function is configurable. The module behavior is as described below when the disabling function is active:

- User with access driven by a time schedule cannot run the door open function
- User with access always granted is not affected by the disabling function

- Remote door open function cannot be performed
- Remote identification with ID is disabled for users with access driven by a time schedule

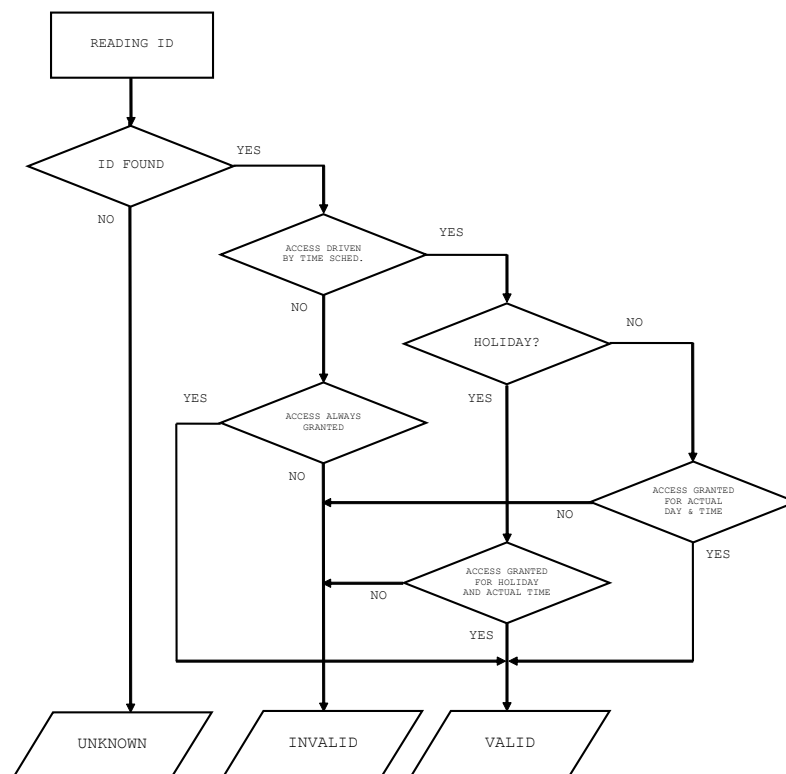
The disabling status changes and disabled actions are logged in the events archive.

6.11 Online authorization

The *Online authorization of ID* can be used in APS mini Plus system. When the feature is used, the ID validity is resolved in connected PC. To be able to use this authorization mode, the reader module has to be equipped with a *MLO* license.

7 Simplified access rights evaluation

The model of access rights contains time schedules and a table of holidays. A block diagram for access right evaluation can be seen in *Pic.6*.



Pic. 6: Simplified access rights evaluation

8 Declaration of conformity



The manufacturer TECH FASS s.r.o. declares, that the product follows legal requirements and fulfils necessary European directives. The declaration of conformity document can be downloaded from our web site:

<https://www.techfass.com/en/download/11/conformity-declaration>

9 Electrical waste



According to WEEE directive (2012/19/EU), this product cannot be disposed of as unsorted municipal domestic waste and has to be returned to recycling center after its lifetime is over.

10 Legislation

The product complies following harmonization legislation of EU

Legislative	Product	European harmonization legislation
	MREM 82 HIK-MF WRE 82 HIK-MF NREM 82 HIK-MF	2014/53/EU; "RED"
		2014/30/EU; "EMCD"
		2014/35/EU; "LVD"; EN 62368 – 1
		2011/65/EU "RoHS"
		"REACH"

Table 10: Legislation