

techfass

MREM 77 EISGRT

Reader module 13,56 MHz, 125 kHz

Introduction

The MREM 77 EISGRT RFID reader module (13.56 MHz reader / dual reader 13.56 MHz and 125 kHz) with integrated controller for one door control is designed either for connection to the RS 485 bus of the APS mini Plus access system or for autonomous operation. The module is also equipped with a Wiegand interface for connecting an input RFID reader with a Wiegand output for possible double-sided controlled door. Up to 32 MREM 77 E reader modules can be connected to one RS 485 communication line of the APS mini Plus system. The module can be covered with any standard cover intended for the KU 68 installation box.



a. Application

- Access control system, booking system
- Door access control

b. Parameters

- Input voltage $8 \div 28$ Vdc
- Typical current consumption 53 mA @ 12 V
- Maximum input power 1,1 W
- Reading id media MIFARE®, NFC, EM Marin, Jablotron
- 1x RS 485 (system bus APS mini Plus)
- 1x Wiegand (external RFID reader, GSM module, license plate camera) or next RS 485 (OEM)
- 1x Relay output 30 V / 2 A (lock)
- 2x INPUT (door contact, exit button, tamper)
- 1x Alert output (Alert notification)
- 1x I/O Port (Ext. tamper, reader module disabling – intruder alarm integration)
- Assembly in the installation boxes KU 68, LK 80.

c. Variants

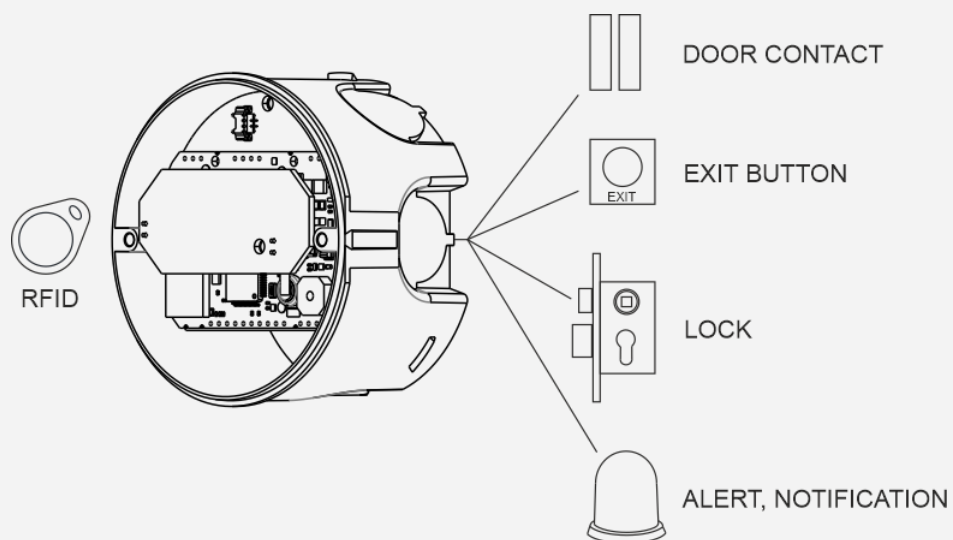
KATALOGUE NUMBER	PART NUMBER	SYSTEM	VARIANT	RFID frequency
534771A2	MREM 77 EISGRT-MF	APS mini Plus	KU 68-1901	13,56 MHz
53477311	MREM 77 EISGRT-EM	APS mini Plus	KU 68-1901	125 kHz
53477323	MREM 77 EISGRT	APS mini Plus	KU 68-1901	125 kHz, 13,56 MHz
53477412	MREM 77 FISGRT-MF	APS mini Plus	LK 80	13,56 MHz
53477401	MREM 77 FISGRT-EM	APS mini Plus	LK 80	125 kHz
534773F3	MREM 77 FISGRT	APS mini Plus	LK 80	125 kHz, 13,56 MHz

d. Marking

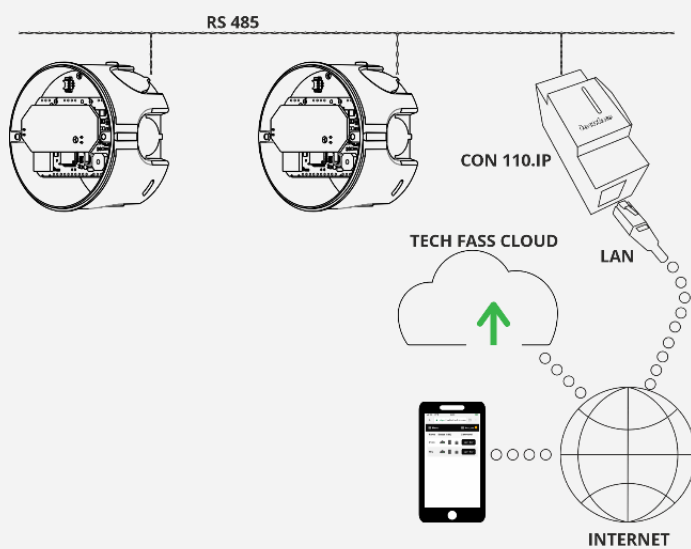
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
M	R	E	M			7	7			E	I	S	G	R	T	-	M	F						
System M: APS mini Plus N: APS 400				Product type REM: Reader module		HW type		Mechanics E: KU68-1901 F: LK 80			Environment I: Indoor t range T: -10 ÷ +55°C		Design Standard	Colour GR: Gray		Connection T: Terminal blocks		RFID technology MF: 13.56 MHz Blank: 13.56 MHz & 125 kHz						

e. Block diagram

Full door control, standalone case



- Bus system case with web control & administration



Content

1	Technical parameters.....	5
1.1	Electrical parameters.....	5
1.2	Communication interface.....	5
1.3	Mechanical parameters	5
2	Assembly.....	6
2.1	Connection of MREM 77 E / F plug-able terminal block.....	6
2.2	Installation instructions	7
3	Wiring diagram	8
3.1	Door control by RFID medium	8
3.2	Connection of multiple modules	8
4	RFID reading	9
4.1	Reading at 13,56 MHz	9
4.2	Reading at 125 kHz	10
4.3	Dual reading at 13,56 MHz &125 kHz	10
5	Settings	11
5.1	Setup procedure	11
5.2	Meaning of the LED indicator	12
5.3	Configurable parameters	13
6	Operating modes	14
6.1	Standard operating mode	14
6.2	External reader with Wiegand output	15
7	Function	16
7.1	Functions of the reader module	16
7.2	Function “Door open“	16
7.3	Permanent lock release based on valid time schedule	16
7.4	Function of ID with flag	16
7.5	ID expiration	16
7.6	Antipassback function (APB)	17
7.7	Disabling the reader module.....	17
7.8	Alerts and their signaling	17
7.9	Simplified access rights model	19
7.10	Offline setting (programming) mode	19
8	Other	23
8.1	Legislation	23
8.2	Declaration of conformity.....	23
8.3	Electrical waste.....	23



1 Technical parameters

1.1 Electrical parameters

PARAMETER	CONDITION	MIN	MAX	UNIT
Input voltage Vin		8	28	V
Typical current consumption lin	Vin = 8 V Vin = 12 V Vin = 24 V		75 53 30	mA mA mA
Peak current consumption lin	Vin = 8 V Vin = 12 V Vin = 24 V		106 73 42	mA mA mA
Typical input power			0,7	W
Maximum input power			1,1	W
Typical reading distance (ISO card)	125 kHz (EM Marin)	3	5	cm
	13,56 MHz (MIFARE® Classic®)	3	5	cm
Radiated H-field intensity @ 10 m	125 kHz		-11	dBuA/m
	13,56 MHz		-8	dBuA/m
RTC	Backup	24		h
Memory	ID media		2000	pc
	Events		3400	
	Time plans		64	
Signalization	RGB led		1	pc
	Piezo		1	

1.2 Communication interface

INTERFACE DESCRIPTION	TECHNOLOGY	PROPERTIES
System data bus	RS 485	19 200 bit / s, 8 data bits, even parity, 1 stop bit
Wiegand	Wiegand / RS 485	Formats 26, 32, 34, 37, 44, 46, 56 bits, custom

1.3 Mechanical parameters

PARAMETER	VALUE	UNIT
Weight	66	g
Dimensions D, h	D 73,5; h 43,5	mm
Mechanical mounting	Inside installation box KU68-1901 Or surface installation box LK 80	
Colour	Grey	
Material	Plastic	PVC
Environmental class	Indoor device general	
Temperature range	-10 ÷ + 55	°C

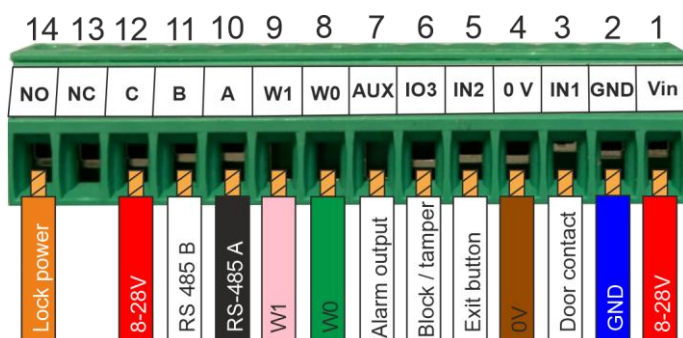
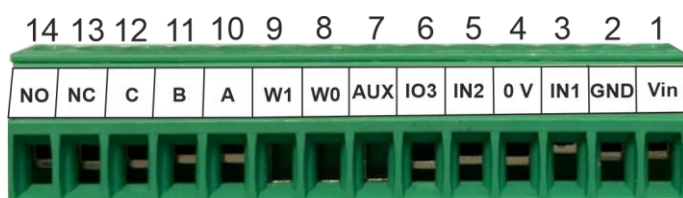
2 Assembly

2.1 Connection of MREM 77 E / F plug-able terminal block

MREM 77 E or F includes 14pins plug-able screwable terminal block to connect all wires.

MREM 77 E / F ISGRT

NUMBER	TERMINAL DESCRIPTION	WHERE IT LEADS*
1	Input voltage Vin 8 ÷ 28 Vdc	Power supply
2	Power ground GND	Power supply
3	IN 1	Door contact
4	Signal ground 0 V	0 V
5	IN 2	Exit button
6	Port I/O 3	Intruder alarm sys
7	Alert output	Alert signalization
8	Wiegand W 0	WIO 22 / ext. reader
9	Wiegand W 1	WIO 22 / ext. reader
10	Signal A system data bus	device APS mini Plus
11	Signal B system data bus	device APS mini Plus
12	Relay contact C	+ 12 V / + 24 V
13	Relay contact N C	Not connected
14	Relay contact N O	Lock + 12 V / + 24 V



Example: The reader module is able to control the door standalone or as part of the APS mini Plus bus system. In addition to the power supply, the module contains, 2 inputs, 1 input / output, alert output, wiegand input / output, RS 485 and relay.

2.1.2 Inputs & Outputs

INPUT / OUTPUT	DESCRIPTION
Input 1 (IN 1)	Door contact, active when door closed; REX button
Input 2 (IN 2)	Request to exit button or handle contact, active when button or handle pressed; Tamper; Disabling function
Output 1 (OUT 1)	Door lock control
Input / Output (IO 3)	Low power transistor output (+5 V in any alarm state)

2.2 Installation instructions

2.2.1 Reader module installation

The MREM 77 reader module is already assembled in the KU 68-1901 or LK 80 installation box. The reader module can of course also be installed in already installed installation boxes in masonry (KU 68-1901), the attachment is made with one screw. Standard UTP cables can be used, which, after connecting the detachable terminal block, fits well into the remaining place in the installation box. If the UTP cable does not meet the power requirements of the controlled lock or opener, it is of course necessary to use cable cores with an adequate cross-section according to the installation parameters. Shorten the cable so that you are able to snap the detachable terminal block, but at the same time so that the coiled cabling fits into the designated space in the installation box.

2.2.2 RS 485 bus termination

It is advisable to terminate the RS 485 system bus so that there is no reflection on the line. If this reader module is the last one on the bus, it allows the termination to be done by its own jumper - a jumper, which connects the already fitted termination resistor. By default, the termination resistor is disconnected.

2.2.3 RS 485 idle states

This reader module does not allow to set idle states of the system bus. Set the idle states on converters APSLAN or CON 110.IP if needed.

2.2.4 Radio signal interferences

If a 125 kHz reader is used, it is necessary to take into account another 125 kHz reader in direct range - for example when checking the door on both sides. In this case, the readers may interfere with each other. In the techfass system, it is possible to use the so-called synchronization of reading between the reader and the reading module, which then do not interfere with each other.

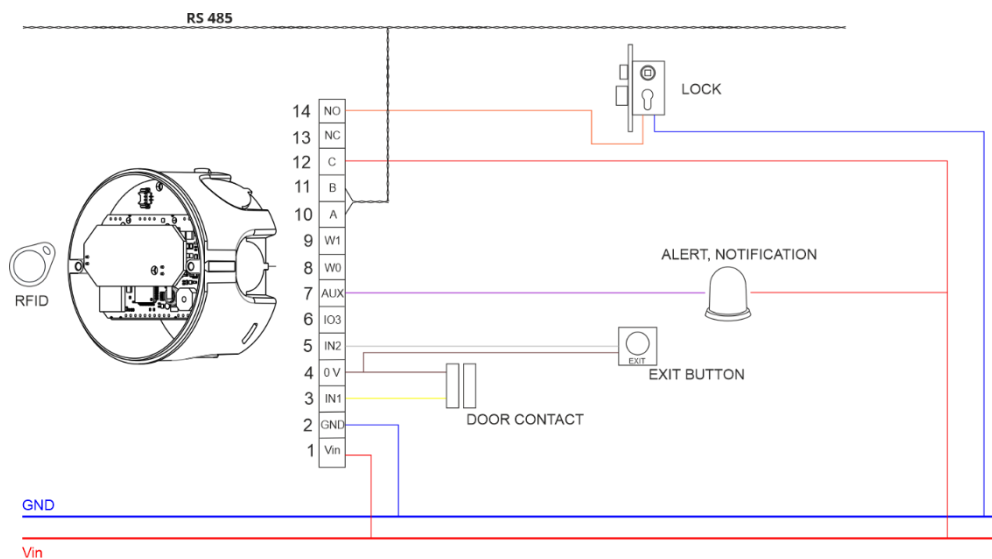
In general, if possible, we avoid mounting on metal substrates, it is recommended to perform a practical reading test or contact support@techfass.cz.

Interference along the line, e.g. from an interfering power supply, can affect the reading distance or the reader's own communication.

3 Wiring diagram

3.1 Door control by RFID medium

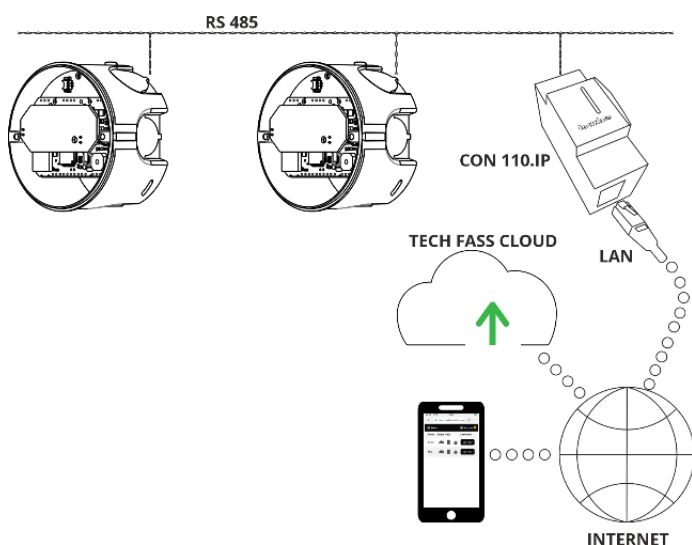
The following figure shows the standard connection of the reader module. After a valid card or other medium is read by the MREM 77 E reader module, this ID is evaluated directly by the MREM 77E module and, if valid, a relay is closed which connects the power supply / control signal to the lock. The relay output can be configured in the control software to switch standard, reverse or toggle, while setting the switching time.



Wiring diagram 1: Connection of one MREM 77 E reader module for control of one door. The module is also able to notify, for example, a knocked out or door ajar on its AUX output.

3.2 Connection of multiple modules

It is possible to connect up to 32 modules to one line of the APS mini Plus system behind the APSLAN converter or behind the cloud connector CON 110.IP. The lines can be further parallelized.

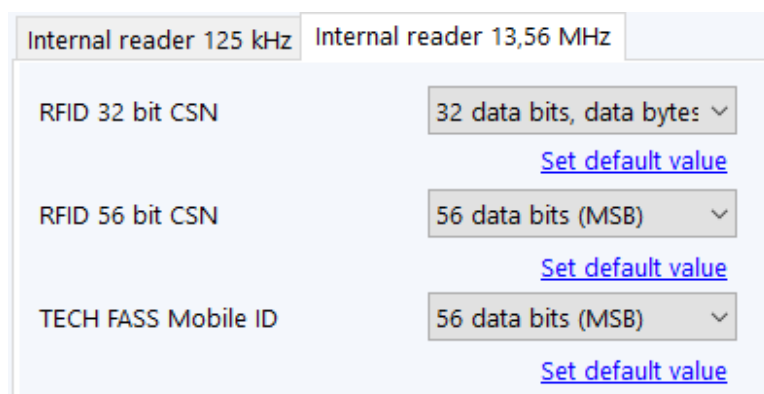


Wiring diagram 2: Up to 32 modules can be connected to one line of the APS mini Plus system and thus manage all doors centrally. A REP 485 repeater can be used for star connection.

4RFID reading

4.1 Reading at 13,56 MHz

The device can read media (cards, key fobs, stickers) according to ISO / IEC 14443A at the level of reading the so-called UID. Examples of media technologies used are NFC and the MIFARE® product family. The device is also ready for so-called sector reading, but it is not active yet.



Print screen from APS Reader application.

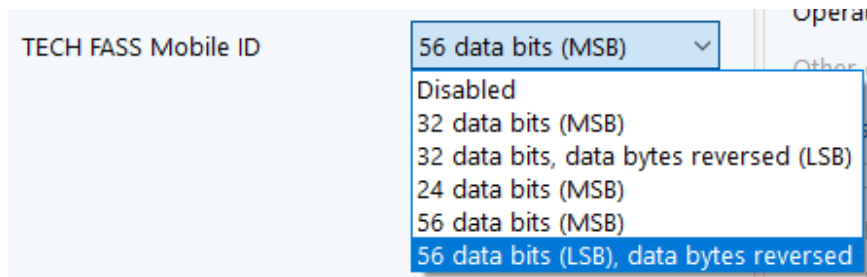
32 bit CSN	56 bit CSN	TF Mobile ID
Disabled	Disabled	Disabled
32 data bits (MSB)	32 data bits (MSB)	32 data bits (MSB)
32 data bits, reversed (LSB)	32 data bits, reversed (LSB)	32 data bits, reversed (LSB)
24 data bits (MSB)	24 data bits (MSB)	24 data bits (MSB)
Facility code 0x01 + 16 data bits (MSB)	Facility code 0x01 + 16 data bits (MSB)	Facility code 0x01 + 16 data bits (MSB)
	56 data bits (MSB)	56 data bits (MSB)
	56 data bits, reversed (LSB)	56 data bits, reversed (LSB)

For the frequency 13,56 MHz, the format and length options of the so-called "card serial number" can be set according to the table above. Similarly for the TF Mobile ID mobile application.

4.1.1 Identification by mobile phone with OS Android 4.4+

Mobile phones equipped with NFC technology, OS Android 4.4 Kit Kat (or higher) can be used for identification (replaces the usual RFID card). You have to download TF Mobile ID application and follow its manual. The TF Mobile ID application is available for free download on Google Play.



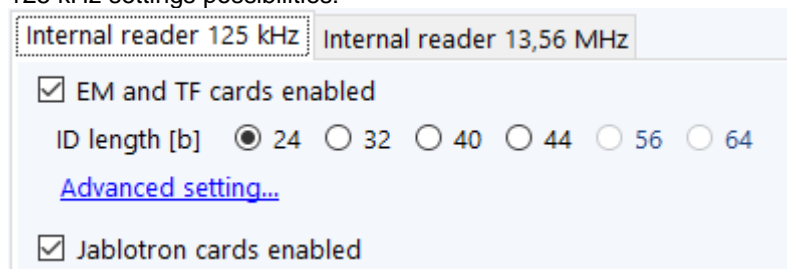


The TF Mobile ID read format and length setting options are shown in the image above (print screen from APS Reader).

4.2 Reading at 125 kHz

The EM or dual variant of the device can also read media with a frequency of 125 kHz like EM Marin (e.g. EM4200, EM4305). Next example of supported media technology is Jablotron ID.

125 kHz settings possibilities:



Default settings for 125 kHz.

4.3 Dual reading at 13,56 MHz & 125 kHz

The dual variant of the device allows reading media according to 3.1 and 3.2 at the same time.

MIFARE® a MIFARE Classic® are registrated trade marks of NXP B.V.
Android® je registred trade mark of Google LLC.

5 Settings

5.1 Setup procedure

If we want to set the reader module MREM 77 E / F, e.g. its HW address or configure its parameters, we must connect it to the computer and control software. Physical connection is possible using the device

via USB

APSUSB <https://www.techfass.com/cs/produkty/102/produkt/1216/apsusb>

via LAN

APSLAN <https://www.techfass.com/cs/produkty/102/produkt/94/apslan>

Alternatively, from anywhere with a web browser using

CON 110.IP <https://www.techfass.com/cs/produkty/102/produkt/1628/con-110-ip>

5.1.1 Software application

The desktop application for configuration

APS Reader <https://www.techfass.com/cs/produkty/101/produkt/389/aps-reader>

APS Hit <https://www.techfass.com/cs/produkty/101/produkt/1355/aps-hit>

The desktop application for administration

Small – medium installation: APS Hit <https://www.techfass.com/cs/produkty/101/produkt/1355/aps-hit>

Medium – large: APS Administrator <https://www.techfass.com/en/products/101/product/391/aps-administrator>

Web application for configuration & administration

WebHit <https://webhit.techfass.com/login>

5.1.2 HW address settings in APS Reader application

By MREM 77 E/FISGRT is possible to set HW address by software. The HW address can be set either in the desktop program APS Reader or APS Hit or directly in WebHit (online service Cloud TECH FASS available via web browser).

5.1.3 HW address settings in APS Reader application

The screenshot shows the APS Reader application window. The 'Communication' tab is selected in the top menu. In the 'Communication' section, the 'Serial line (COM port name)' is set to 'COM5'. Below this, the 'HW address setting' section is highlighted with a red box. It contains two radio buttons: 'Using confirmation ID' (unselected) and 'Knowing serial number' (selected). The 'Knowing serial number' option has a text field containing '80670000'. To the right of the text field are 'Set address' and 'Test 485' buttons. Other settings like 'Strike time [s]' (7), 'Strike control' (Direct), and 'Permanent door lock release' (Never) are visible in the background.

Step by step - If you know the serial number:

- Connect wires A, B, GND to APSUSB, connect APSUSB to PC, start APS Reader
- Select the required HW address
- Select the option "Known serial number", enter the SN of your product
- Press 'Connect' at the top of the blue menu
- Press "Set" (the selected HW address is set)
- Disconnect

5.1.4 HW address settings in WebHit

Setting HW address with SN

SN

device serial number

HW address

1

N/A

Commit

Close

- Click on line configuration in the left menu
- Click on set address with SN
- Fill in the device SN and needed hw address

5.2 Meaning of the LED indicator

COLOUR	ACTION	DESCRIPTION
Red	Continuously lit Flashing with a period of 4 s	Online communication of the RS 485 system bus Offline operation
Green	Flash	ID media reading
Alternation Red / green	Red / green flashing	Address setting mode / RS 485 system bus test
Yellow	Continuously lit, flashing	Programming mode
	Short flashing, period 1 s	Door lock release indication

5.3 Configurable parameters

PARAMETER	SETTINGS OPTION	FACTORY SETTINGS
Max. output switching time*	0 ÷ 255 s	5 s
Acoustic signalization of lock release	YES / NO	YES
Type of lock output control (Polarity)	Direct / Reverse	Direct
Output mode (Lock control)	Standard / Change of state / impulse	Standard
Permanent turn on of the output according to the schedule	Never / Time schedule	Never
Yellow LED signalization of lock release	YES / NO	NO
Input 1	Door contact / exit button	Door contact
Input 2	Exit button Handle contact Tamper Disable	Exit button
I / O port 3	Tamper Disable	Tamper
ALERTS		
Tamper (alert signalization time)	0 ÷ 255 s	0 s
Forced door (alert signalization time)	0 ÷ 255 s	0 s
Door ajar (alert signalization time)	0 ÷ 255 s	0 s
Door ajar (allowed opened door time)	0 ÷ 255 s	20 s
ID with Alarm flag (alert signalization time)	0 ÷ 255 s	0 s
Enable exit button in tamper state	YES / NO	YES
EVENTS		
Events archive saving options		
Door opened (input 1 off)	ON / OFF	ON
Door closed (input 1 on)	ON / OFF	ON
Input 2 off, input 2 on	ON / OFF	ON
Output 1 off, output 1 on	ON / OFF	ON
OTHER		
Automatic conversion to CEST & back**	YES / NO	YES
Max. online response time by online authorization***	0 ÷ 25500 ms	800 ms
Authorize autonomously after response time exceeded	YES / NO	YES

* Valid for standard output mode (lock control). Not valid for change of state option.

** In WebHit, the time shift is done automatically according to the selected time zone.

*** Online authorization function is not available yet in WebHit.

6 Operating modes

There are two basic operating modes for the MREM 77 reader module.

- Standard operating mode
- External reader with wiegand output

6.1 Standard operating mode

Main operating mode. In this mode, the module acts as a controller for one door, reads RFID media and determines in its memory whether or not the user should be authorized to enter and controls the lock output.

The module can be in online or offline standard operating mode. The function is identical in both modes, with the difference that in the online mode, the module statuses are reported via the communication line (after changing the mode from offline to online, the event archive is read from the module's memory). In both operating modes, the module can switch to programming mode (after reading the programming card).

6.1.1 Offline mode

Offline, or autonomous / standalone mode. One module alone or more modules on the RS 485 bus, but without connection to a PC. In this mode, events are stored in the module's internal memory, module authorizes users according to the stored set access rights. Settings / configuration are performed by default using a PC or programming cards.

6.1.2 Online mode

In Online mode, the module or more modules on the line are connected to a PC running the relevant application such as APS Hit or APS Administrator or the line is connected to the cloud using CON 110.IP and the administrator works in the WebHit web application. In this case, each event is immediately written to the application.

6.1.3 Online authorization

The APS mini Plus system implements the option of Online authorization of access authorization. In such a use, the connected PC decides on the validity of the read ID authorization. The reader must be MLO licensed to use it in this authorization mode.

! Note: This feature is currently only available on desktop applications.

6.1.4 Secure lock control with WIO 22 module

The MREM 77 module itself contains a switching relay and there are connected wires to control the lock. In this simple configuration, it is advisable to install the module in a safe zone, where we do not expect an attempt to overcome so that someone will want to get to the cabling to control the lock. If we need the module to switch "safely", we connect the WIO 22 module to its Wiegand output, we place WIO in a safe place, eg in a rack / cabinet or from the inside above the door, from where it already controls the lock. The WIO module must first be paired with the MREM 77 reader module.

<https://www.techfass.com/cs/produkty/102/produkt/402/wio-22>

6.2 External reader with Wiegand output

The MREM 77 reader module can be configured in external reader mode with Wiegand output in the following formats:

6.2.1 125 kHz

Enable / Disable options

- Standard em marin & proprietary tf ID
- Jablotron ID

*Default settings: All enabled.

ID length

125 kHz	bits				
ID length	24	32	40	44	56

*Default settings: 40 bits format.

Wiegand output setting

125 kHz	bits				
Data length	26	32	42	44	56

*Default settings: 42 bits format.

6.2.2 13,56 MHz

32 bit CSN	56 bit CSN	TF Mobile ID
Disable	Disable	Disable
32 data bits (MSB)	32 data bits (MSB)	32 data bits (MSB)
32 data bits, reversed (LSB)	32 data bits, reversed (LSB)	32 data bits, reversed (LSB)
24 data bits (MSB)	24 data bits (MSB)	24 data bits (MSB)
Facility code 0x01 + 16 data bits (MSB)	Facility code 0x01 + 16 data bits (MSB)	Facility code 0x01 + 16 data bits (MSB)
	56 data bits (MSB)	56 data bits (MSB)
	56 data bits, reversed (LSB)	56 data bits, reversed (LSB)

7 Function

7.1 Functions of the reader module

- Standard "Door open" function
- Lock control
- Door status monitoring
- Exit button status monitoring
- Activation of the alarm output / buzzer signaling when an alarm condition is indicated

The "Door open" function can be activated in three different ways

- By reading a valid ID (card, key fob,...)
- By pressing the exit button (depending on the configuration) - cannot be used during the alarm
- Software, via communication line

7.2 Function “Door open“

In the case of the standard lock control mode, after activating the "Door open" function, the release of the lock relay and the buzzer are activated (unless disabled by configuration). This state lasts until the door is opened, but no longer than the time set by the "Lock activation time" parameter. Then the lock output is deactivated and the standard function is terminated.

In the case of the toggle lock control mode, after activating the "Door open" function, the relay output toggles and the buzzer is activated (if it is not disabled by the configuration). The acoustic signaling lasts as set. The relay output remains unchanged until the next activation of the "Door open" function.

In the case of the pulse lock control mode, after activating the "Door open" function, the relay output is activated for the time given by the parameter Pulse width (ms).

In the case of the standard lock control mode, reading a valid card during lock activation will cause a new lock timing.

Online authorization

If the reader module reads the ID card during the "Door open" function via the communication line (in online mode) and if the read ID is not valid, it is signaled by an acoustic signal "invalid ID" regardless of the configuration of the acoustic lock release message.

7.3 Permanent lock release based on valid time schedule

When this function is set, the lock is permanently released during the validity of the respective schedule, the reading of a valid ID is reported via the communication line (in online mode). When the lock is permanently released, the alarm state of the forced door does not occur.

The setting of the permanent release of the lock according to the time schedule and the toggle lock control mode are mutually exclusive.

7.4 Function of ID with flag

It is possible to set a flag for each ID, which will cause an alarm “ Alarm - ID with the flag “ when reading the appropriate ID (and will activate the alarm output for a defined time).

7.5 ID expiration

It is possible to set a date for each ID at which the ID expires and will no longer be valid. The expiration is evaluated every time the data in the RTC module changes and when new access rights are loaded.

! Note: This feature is currently only available on desktop applications.

7.6 Antipassback function (APB)

Antipassback can be implemented in two ways:

- Time - the user must not use the ID medium repeatedly for a defined time
- Zone - the user must not repeatedly enter the area in which he is present

The antipassback function is used only for users who have defined access according to a schedule. The function does not apply to users with permanently valid access.

Zone and time antipassback IDs can be reset by re-inserting the IDs using the programming cards. After reloading the access rights by the program, the antipassback flags are reset for all IDs.

The zone and time antipassback flag is written according to the configuration either immediately after reading the ID, or only after opening the relevant door (opening the relevant door contact).

7.6.1 Time antipassback

The time antipassback is defined by setting the duration (in minutes), which is set for the given ID when passing at the given address. The next time the ID is identified at the relevant module address during the timer run for the given ID, a time APB alarm is triggered. The following parameters affect the time antipassback function:

- Default value of the APB timer - the time for which the APB timer alarm is triggered at the next ID identification, the timer is set for the given ID when passing at the given address.
- Enable door opening after time APB alarm - if the function is enabled, the Door opening function is started in case of time APB alarm.

7.6.2 Zone antipassback

Zone antipassback is defined by enabling / disabling this feature. The zone antipassback flag is set for the user after passing. Upon further identification, a Zone antipassback alarm is triggered in the case of a flag set for the given ID. The following parameters affect the zone antipassback function:

- Enabled - global enable / disable of the zone APB flag setting function.
- Enable offline mode - if not set, the module works in offline mode as if the zone antipassback function was not implemented at all.
- Enable door opening after APB alarm - if the function is enabled, the Door opening function is started in case of a zone APB alarm.

7.7 Disabling the reader module

Disabling of the reader module function can be configured on the second input or on the third I / O port of the module. The function activation logic on each port is configurable. The function is activated if at least one of the ports is active and set as disable.

The module in the disabled state exhibits the following behavior:

- Users with set time schedule cannot trigger the door open function if it is disabled
- Disable does not apply to the users with permanently valid access (no time schedule)
- The remote door opening function cannot be performed
- Remote door opening with ID is blocked for users with time schedule.

Changes in the status of the disable function and the blocked action are recorded in the event archive. This function is useful for example in combination with intruder alarm system.

7.8 Alerts and their signaling

The following alert conditions may occur during the reader module operation:

- 1) Tamper.
- 2) Forced door.
- 3) Door ajar.
- 4) Antipassback alert (time, zone).
- 5) Alarm ID with flag.

To deactivate any alert, please set its value to "0".

Alerts are reported as follows:

- In software, by system bus (alerts 1, 2, 3, 4, 5)
- Acoustic (alerts 1, 2, 3, 4)
- Activating the alert output (alerts 1, 2, 3, 5)

The alarm message via the communication line assumes an online connected PC with the appropriate software suitable for online operation (APS Administrator).

The audible alert message is twofold:

- Continuous tone (distortion)
- Intermittent tone (knocked out and long open door, APB alarm)

The acoustic message ends either after the set time (see configuration table) or after reading a valid ID on the relevant module.

When one of the relevant used alarm conditions occurs (signaling time alarm must be greater than 0) the alarm output will be activated. On this output is it is possible to connect the alarm device directly or to further process its signal.

The triggering of the alarm is controlled by a logical connection or between individual types alarms.

The alarm condition is terminated by restoring all idle conditions (closing the door, fitting the cover, etc.).

7.8.1 Tamper

The MREM 77 E / F reader module is not equipped with a Tamper sensor to detect that the lid is open. This is due to the variability of the covers that can be used with it. The module itself is ready for the connection of the tamper, for possible installation it is necessary to share the intended cover and agree in advance by contacting support@techfass.cz.

The "Violation" alarm state is generated by activating the Tamper signal by opening the cover of the reader module, or by changing the state of the 2nd or 3rd input in the tamper configuration.

The Violation alarm state is evaluated only after the first idling state after switching on the reader module, if it is not installed, there is no need to configure the module in any way.

7.8.2 Forced door

The "Forced door" status occurs when the IN1 input of the module is opened without first activating the "Door open" function. The only exception is the exit button / handle contact signal activation from the inner side of the door.

7.8.3 Door ajar

The "Dopr ajar" status is activated by opening the door for a longer time than allowed (set), see the configuration table.

7.8.4 Antipassback alarm

Antipassback alarm is generated when a valid card is read at the time of blocking the user by Time APB, or when the user is blocked by a Zone APB.

7.8.5 Alarm ID with flag

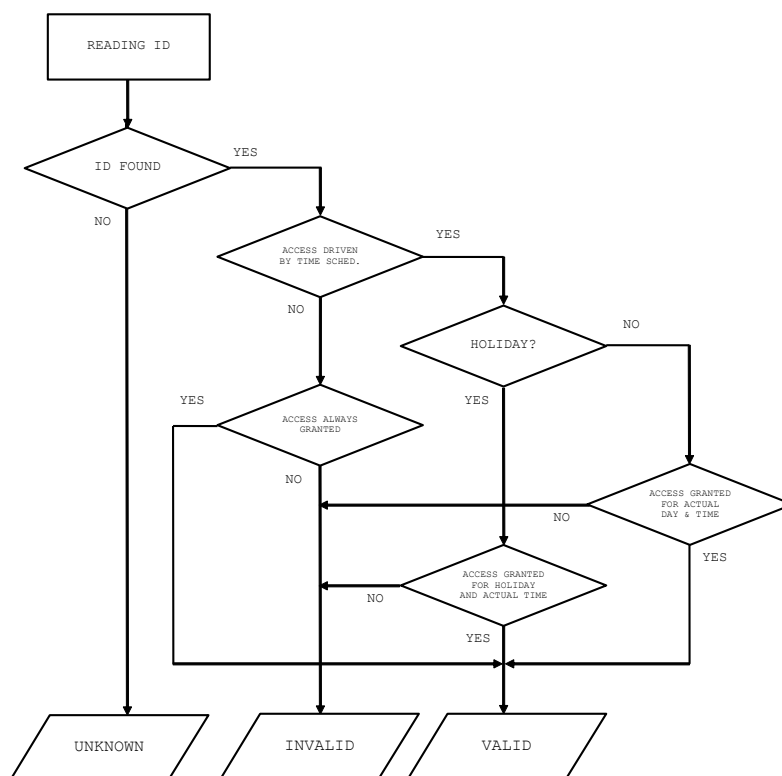
Alarm ID with a flag occurs when a card (ID) with flag is read.

7.8.6 Reading ID in time of alert

Reading a valid ID has no effect on the alarm conditions themselves. It is terminated with a valid ID only an audible alarm, followed by the "door open" function. Reading an invalid ID only interrupts the audible alarm for the duration of the "invalid ID" signaling.

7.9 Simplified access rights model

The access rights model includes schedules and a holiday table. The block diagram for access evaluation is shown in the following figure.



7.10 Offline setting (programming) mode

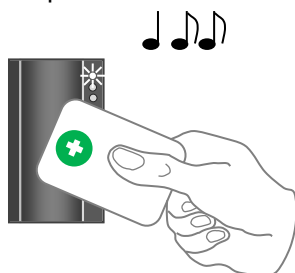
For small simple autonomous installations, users can be set up using programming cards. The module enters the programming mode by reading one of the pair of programming cards ("+" and "-" cards). It does not enter the programming mode while waiting for the card confirming the address setting (for modules with address setting via the communication line). The behavior of the modules in the programming mode is evident from Fig. 5 a-d.

When inserting cards using programming cards, it is not possible to work with time schedules, so the cards are still valid.

7.10.1 Inserting cards (ID codes) into the memory

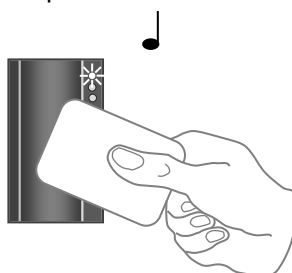
Follow these steps for inserting cards into the reader module's memory:

Step 1



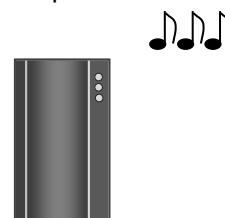
Read the programming card for *inserting*: the reader goes into *programming mode*.

Step 2



One by one, read the cards which are to be granted access.

Step 3

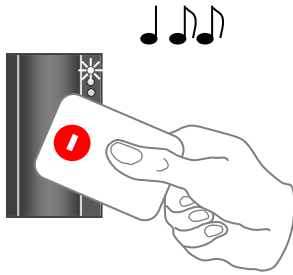


About 15 seconds after inserting the last card the reader module goes back into *standard operating mode*.

7.10.2 Deleting cards from the reader's memory

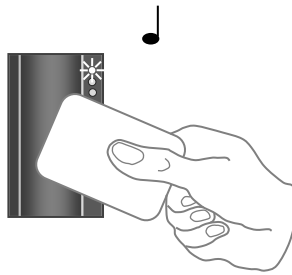
For deleting the cards from the reader module's memory use following steps:

Step 1



Read the programming card for *deleting*: the reader goes into *programming mode*.

Step 2



One by one, read the cards which are to have their access revoked.

Step 3



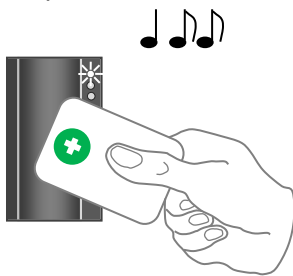
About 15 seconds after deleting the last card the reader module goes back into *standard operating mode*.

Pic.5 b): Deleting cards

7.10.3 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.

Step 1



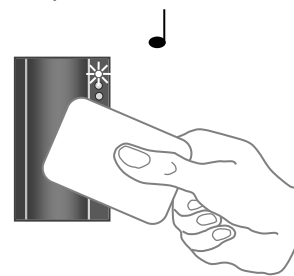
Read the programming card for *inserting*: the reader goes into *programming mode*, which is indicated by slow flashing of yellow LED.

Step 2



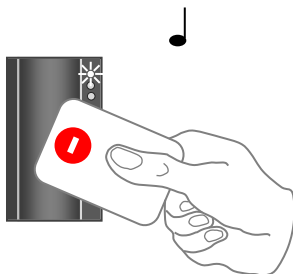
Read the programming card for inserting 5 times in a row; the reader will go into *Deleting cards „above or below“* mode indicated by fast flashing of yellow LED.

Step 3



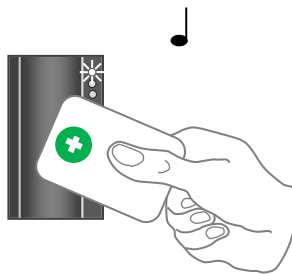
Read a card, which is located in the module's memory *right before or right after* the card you wish to delete. After this step the module quickly flashes with yellow LED

Step 4 - A



For deleting an ID located *right before* the ID used in previous step, read the programming card for *deleting*.

Step 4 - B



For deleting an ID located *right after* the ID used in previous step, read the programming card for *inserting*.

Step 5



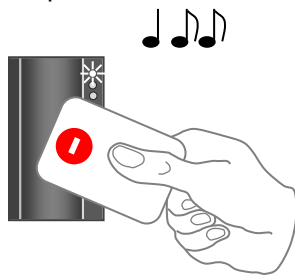
The reader module goes back into *standard operating mode*.

Pic.5 c): Deleting cards „above or below“

7.10.4 Deleting all cards from the reader's memory

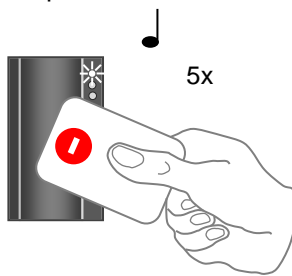
Follow these steps for deleting all cards from the reader module's memory:

Step 1



Read the programming card for *deleting*: the reader goes into *programming mode*.

Step 2



Read the programming card for deleting 5 times in a row; the reader will erase all cards from its memory.

Step 3



The reader module goes back into *standard operating mode*.

Pic.5 d): Deleting all cards

7.10.5 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 7.10.1 – 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

after inserting 5 cards

Pic.5 e): Table

- Card 3 gets lost* – Delete it *using the card 4*, which is available, and using the procedure from chapter 7.10.2 – 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

➡

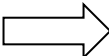
position	card
1	card 1
2	card 2
3	card 3
4	card 4
5	card 5

Deleting card 3 using the card 4, table after deleting card 3

Pic.5 f):

- Card 4 gets lost* – Delete it *using the card 2*, which is available, and using the procedure from chapter 7.10.3 – 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

Deleting card 4 using the card 2, table after deleting card 4

Pic.5 g):

- It is necessary to *add another card* (card 6). We proceed with the procedure from *chapter 6.7.1* 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

Table after inserting card 6

Pic. 5 h):

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 7.10.4*, it is necessary to create a new filing table.

8 Other

8.1 Legislation

The product is compliant with following harmonized directives of European Union.

EU HARMONIZATION RULES, STANDARDS, REGULATIONS
2014/53/EU; "RED"
2014/30/EU; "EMCD"
2014/35/EU; "LVD"; EN 62368 – 1
2011/65/EU "RoHS"
(ES) č. 1907/2006 "REACH"

8.2 Declaration of conformity



The manufacturer TECH FASS Ltd. 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>

8.3 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.

techfass

TECH FASS s.r.o.

Věštinyá 1611/19, Praha