![APS mini Plus logo]

MREM 80 ThanGH

MREM 80 LithGH

APS mini Plus reader modules for Thangram and Lithos entry panels

User's guide

techfass®

1 Content

2 Product Description

The *MREM 80 ThanGH* and *MREM 80 ThanGH*[1] reader modules (125 kHz readers with an embedded single door controller) are designed for connection to the RS 485 bus of the *APS mini Plus* access control system. It is possible to connect up to 32 reader modules to a single line of the APS mini Plus system. In effect the number of lines is not limited.

The reader modules are designed for installation in *Thangram* / *Lithos* entry panels of *BPT* audio and video systems, where they occupy only one button space. The modules are customized for power supply and control from BPT entry systems.

2.1 MREM 80 ThanGH module

The modules are designed for installation in *Thangram* entry panels of *BPT* audio and video systems and come in *GH* (greyhound) color version of the buttons.
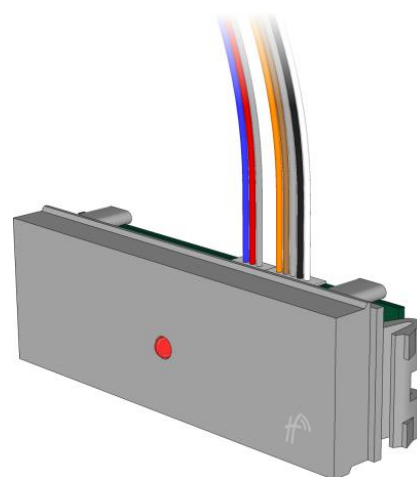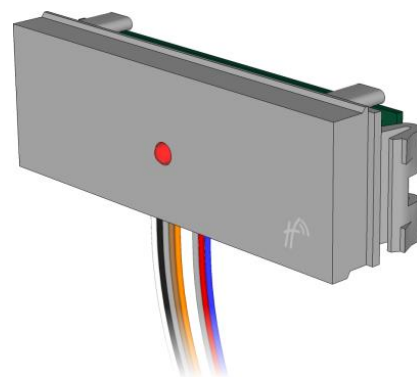

Pic. 1a: MREM 80 ThanGH

2.2 MREM 80 LithGH module

The modules are designed for installation in *Lithos* entry panels of *BPT* audio and video systems and come in *GH* (greyhound) color version of the buttons.

Pic. 1b: MREM 80 LithGH

[1] Commercial designation of available versions is described in *table 1*.

3 Technical parameters

3.1 Product version

Product version	Product designation	Module designed for panel	Catalogue number	Module features [2]	
				TF	EM
	MREM 80 ThanGH – TF	Thangram	53480000	✔	✘
	MREM 80 ThanGH – EM	Thangram	53480001	✔	✔
	MREM 80 LithGH – TF	Lithos	53480400	✔	✘
	MREM 80 LithGH – EM	Lithos	53480401	✔	✔

Table 1: Product version

[2] *TF* – TECHFASS factory 125 kHz ID media reading; *EM* – 125 kHz ID media reading;

3.2 Technical features

Technical features			
	Supply voltage		8 ÷ 28 VDC
	Current demand	Typical	60 mA (12 V), 25 mA (28 V)
		Maximal	90 mA (8 V)
	Version with keypad		N/A
	ID technology, typical reading range	EM Marin	5 cm (with ISO card)
	Real-time clock		Yes
	Memory	Cards	2,000 ID, 2 programming cards
		Events	3,400
		Time schedules	64
	Inputs	1st input	Logical potential-free contact
		2nd input	Logical potential-free contact
	Output	Door lock [3]	1x open collector 0V active, max. 2A, 24V
		Alarm	N/A
	Signalization		1x LED 1x PIEZO
	Tamper protection		N/A
	Communication interface		RS 485
	Alternative data input / output		N/A

Table 2: Technical features

[3] The DC type of door lock has to be used only! Suitable anti-parallel diode has to be connected to its coil as over-voltage protection.
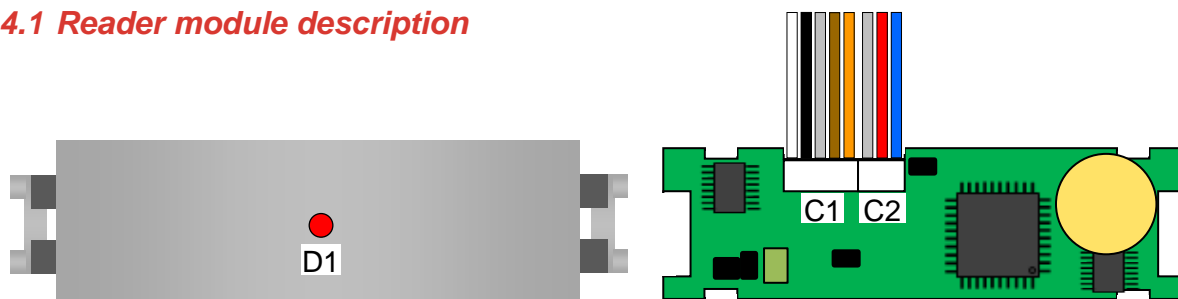
3.3 Mechanical design

Mechanical design		
Weight	0.017 kg
Operating temperature	-25 ÷ 60 °C
Humidity	Max. 95%, non-condensing
Housing	IP 54, IK 04 (built in the entry panel)
Cable length	2x0.4 m
Color	Greyhound (GH)
Dimensions (Height x Width x Depth)	17x53x13 mm

Table 3: Mechanical design

4 Installation

4.1 Reader module description

Pic. 2: MREM 80 reader module, front (left) and rear (right) view

Description	Designation	Purpose
	C1	Connector for C1 cable (5-wires) connection
	C2	Connector for C2 cable (3-wires) connection
	D1	Red-green LED indicator

Table 4: Connectors and LED indicators description

4.2 C1 and C2 cable wiring description

C1 cable		
Color	Function
White	B wire - RS485 line
Black	A wire - RS485 line
Grey	0 V (GND)
Brown	Input 1 (IN1)
Orange	Input 2 (IN2)

C2 cable	
Color	Function
Grey	0 V (GND)
Red	Power supply +8 ÷ +28VDC
Blue	Output 1 - OC

Table 5: C1 and C2 cable wiring description

All unused wires must be mutually isolated!

techfass®

4.3 Connecting the reader module with panel
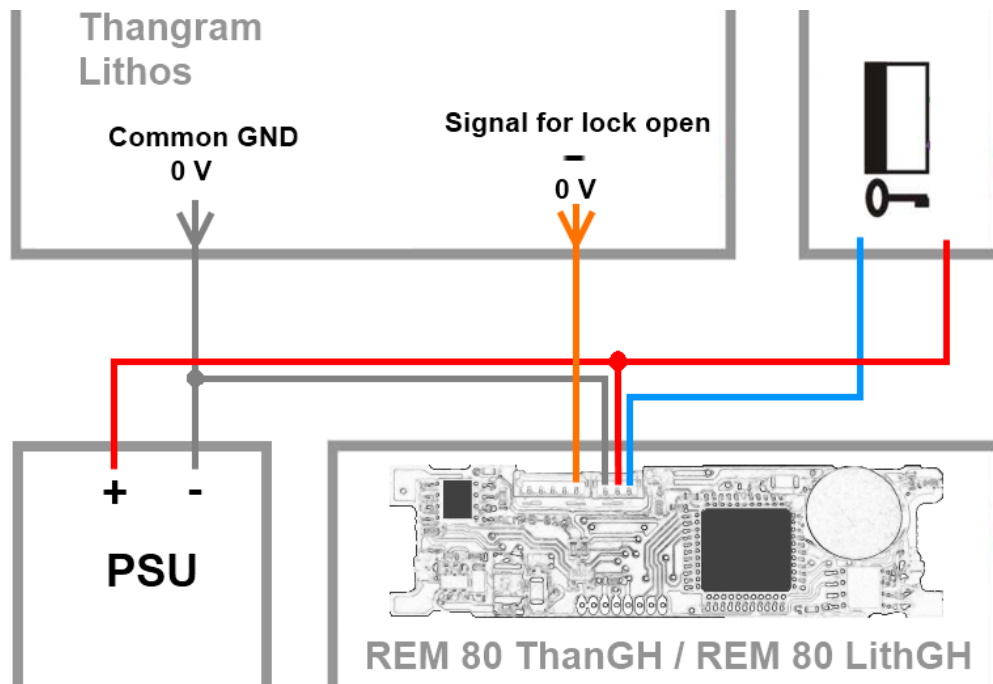
Pic. 3: Standard reader module connection with use of DC power supply and the lock opening contact of the Thangram / Lithos entry panel

	Signal	Connection
Standard connection	+ 8 ÷ + 28 VDC	+ contact (power supplier unit), red wire of C2 cable (reader module), + contact (door lock)
	0 V (GND)	- contact (power supplier unit), grey wire of C2 cable (reader module), - contact for power supply of the entry panel
	Release lock from panel, 0 VDC active	Signal for door lock opening – (minus contact next to the ⚿ at the entry panel), orange wire of C1 cable (reader module)
	Release lock from reader	Blue wire of C2 cable (reader module), - contact (door lock)

Table 6: Standard reader module connection using the entry panel door lock release signal

This connection requires configuring the function of the *second input* of the reader module as *Request to exit button* (default module setting, see *pic. 4*). The standard entry panel door lock release signal is used as a signal for the reader module (orange wire) to release the door lock then. The door lock release is controlled by the output of the reader module (open collector, 0 V (GND) active – blue wire).

Pic. 4: Reader module setting

The reader module is powered by a *DC* power supplier. When using suitable power supplier and door lock type, you can power all components (entry panel, reader module and door lock) from a single power supplier. If an *AC* powered door lock must be used, it is necessary to use an individual *external relay* controlled by the OC signal from the reader module to control the door lock.

4.4 Standard connection

Connection		
	Input 1	Door contact, active when door closed; REX button
	Input 2	Request to exit button or handle contact, 0 V) 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. 8* is used when the door status contact is not installed and no Door Forced and Door Ajar alarms are triggered.

4.5 D1 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

4.6 Installation instructions

The reader module uses passive RF/ID technology, which is sensitive to RF noise sources. Noise sources are generally of two types: radiating or conducting.

Conducted noise enters the reader via wires from the power supply or the host. Sometimes, switching power supplies generate enough noise to cause reader malfunction, it is recommended to use linear system power supplies.

Radiated noise is transmitted through the air. It can be caused by computer monitors or other electrical equipment generating electromagnetic fields.

Consequently, a short distance between the reader modules themselves can cause reading malfunctions – for correct operation it is necessary to keep a minimum distance of 50 cm. Various metallic constructions may have a negative influence on this distance; if there are any doubts, it is recommended to perform a practical test before final mounting.

Nearby metal surfaces may cause a decrease in reading distance and speed. This is caused by the combined effects of parasitic capacitance and conductance.
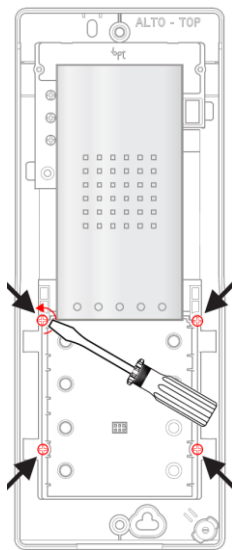
4.7 Mounting and removal the MREM 80 ThanGH module
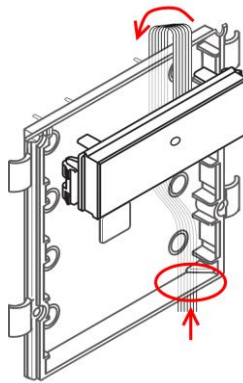
4.7.1 Module mounting

The first step is to unscrew all four screws holding the plastic lower cover for placing push buttons (thereinafter cover) of the *Thangram* panel (*pic. 5a*), then remove the cover. *Cut off the arrest* located at the bottom side of the cover as shown in the *picture 5c*. Then *place the reader module in desired position* and lead the cables as shown in *picture 5b*, that is *bend the cable over the top edge of the cover* and lead it behind the cover downwards. It is not necessary to place the reader module in the top position of the cover, it can be placed at any position of buttons; the cable must be lead similarly as shown in the picture. Then place the cover back to the panel with cable lead as shown in *picture 5d*. It is handful to lead appropriate wires *along the walls* of the panel upwards to the *power supply* and *door lock* contacts, and the rest of the wires *through the back side* of the panel. The last step is reassembling the cover in the installation box and screwing it in (*pic. 5e*).

4.7.2 Module removal

When disassembling the module use a similar procedure as described in the previous chapter, just remember to *unplug the panel and the reader module from the power supply first*!

Pic. 5b

Pic. 5a
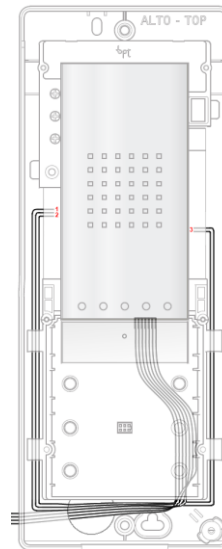
Pic. 5d
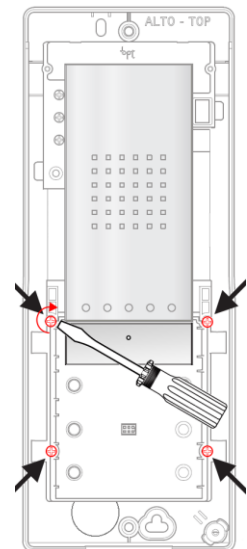
Pic. 5e
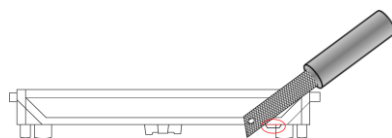
Pic. 5c

4.8 Mounting and removal the MREM 80 LithGH module

4.8.1 Module mounting

When mounting the module it is necessary to unscrew the *front metal plate* of the *Lithos* panel (*pic. 6a*). Then remove the *bottom pushbutton* (*pic. 6b*). *Uncover the plastic strip* (*pic. 6c*) and connect the appropriate wires according to the instructions for standard reader module connection. Lead the rest of the wires through the rear part of the panel (*pic. 5d*). Connect the cables in the way to be placed under the plastic strip, *insert the module* in the *bottom pushbutton position* (*pic. 6e*) and place the plastic strip back again. Fasten the front metal plate of the panel back again (*pic. 6a* – screw in the opposite way).

4.8.2 Module removal

When disassembling the module use a similar procedure as described in the previous chapter, just remember to *unplug the panel and the reader module from the power supply first*!
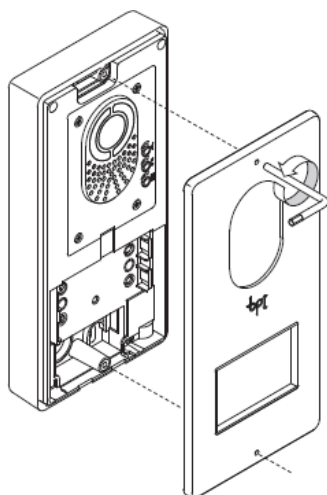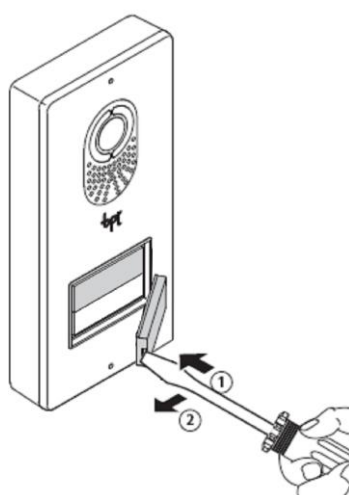
Pic. 6a	*Pic. 6b*	*Pic. 6c*

Pic. 6d	*Pic. 6e*

techfass®

5 Setting parameters of the reader module

5.1 Configurable parameters

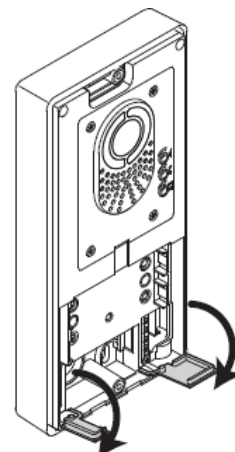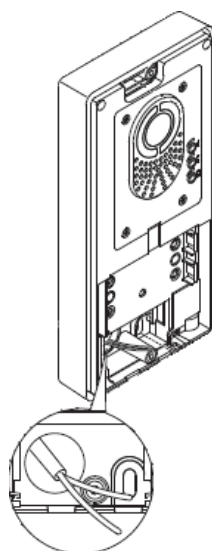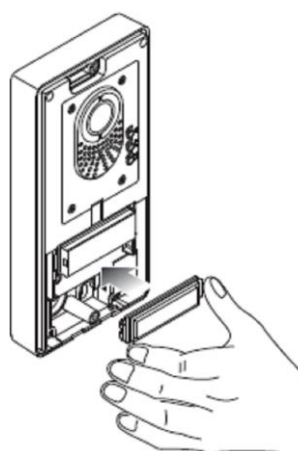|	Parameter		Possible range	Default setting
Configurable parameters	Door lock release time		0 ÷ 255 s	7 s
	Door lock control setting		Direct / reverse	Direct
	Door lock relay function setting		Standard / toggle / pulse	Standard
	Permanent door lock release according to a time schedule		Never / Schedule 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 - Tamper		0 ÷ 255 s	30 s
	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 *chapter 6.10*	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 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.

6.3 Alarm states

The reader module can get in following alarm states:

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

Alarm state reporting is performed as follows:

- Via communication line (statuses 1, 2, 3, 4, 5)
- By acoustic signal (beeper) (statuses 1, 2, 3, 4).

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.

6.3.1 Tamper alarm

In case of tampering the module (by tearing-off or opening the cover or changing the status of input 2 in proper configuration) the "Tamper" state is activated [3].

> [3] The Tamper alarm handling is operational after their first change of status since switching on the module. There is no need to configure the module when the tamper protection is not used.

6.3.2 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.

6.3.3 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.

6.3.4 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*.

6.3.5 ID with Alarm flag alarm

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

6.3.6 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 signaling "Invalid ID".

6.4 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.

6.5 Read ID media format

6.5.1 EM Marin ID media format

The EM Marin ID media format can be changed into selected 24, 32 or 40 bits length of ID code. The default length is 40 bits. This setting is only used when unifying of the ID media codes length is required – in combined systems with WIEGAND output readers with a fixed WIEGAND data format IDs (more information in *APS Reader* user's guide available at http://www.techfass.cz/files/m_aps_miniplus_reader_en.pdf).

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 7 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:

Step 1	Step 2	Step 3
Read the programming card for *inserting*: the reader goes into *programming mode*.	One by one, read the cards which are to be granted access.	About 15 seconds after inserting the last card the reader module goes back into *standard operating mode*.
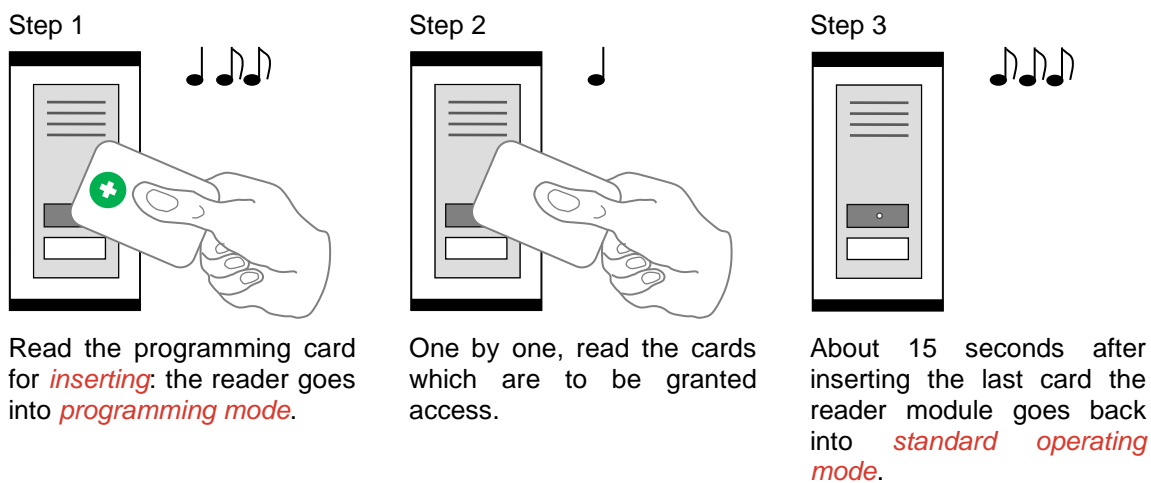
Pic.7 a): Inserting cards

6.6.2 Deleting cards from the reader's memory

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

Step 1	Step 2	Step 3
Read the programming card for *deleting*: the reader goes into *programming mode*.	One by one, read the cards which are to have their access revoked.	About 15 seconds after deleting the last card the reader module goes back into *standard operating mode*.
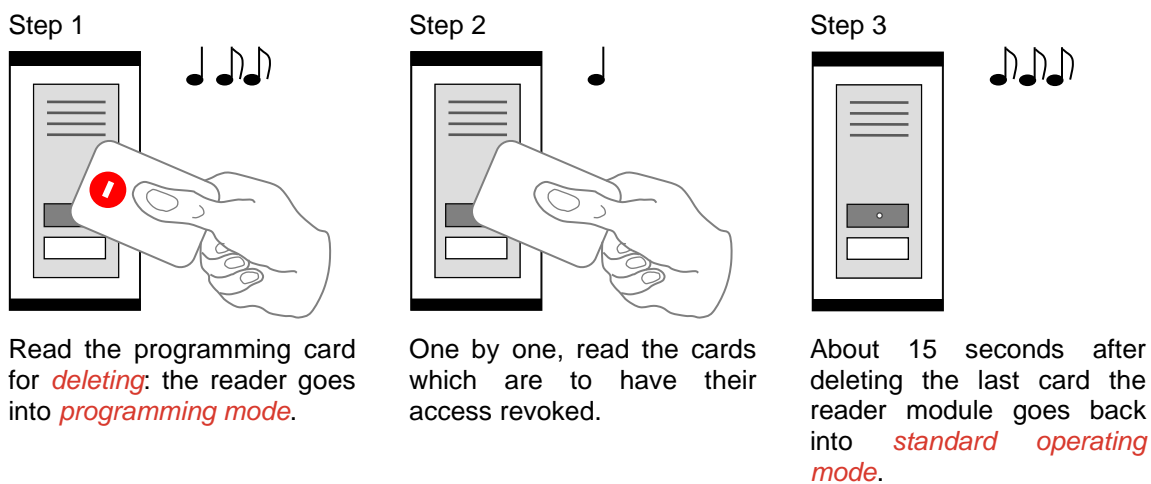
Pic.7 b): Deleting cards

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.

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 precious step, read the programming card for *deleting*.

Step *4 - B*

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

Step 5
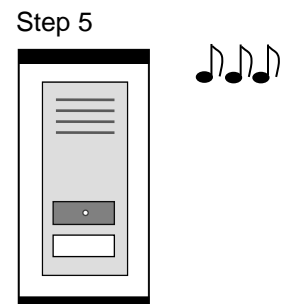
The reader module goes back into *standard operating mode*.

Pic.7 c): Deleting cards "above or below"
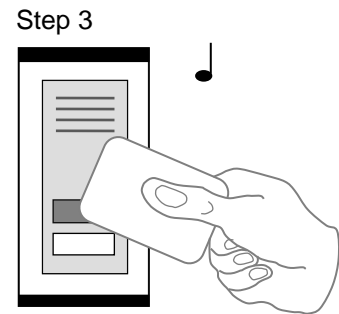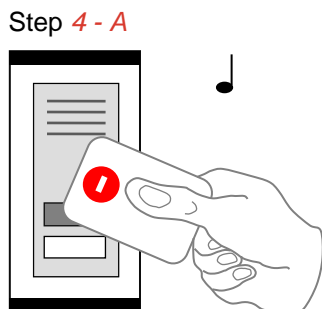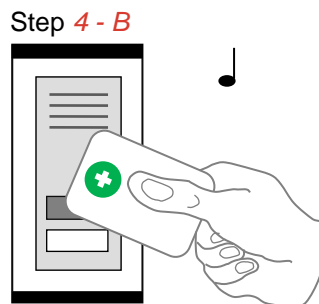
6.6.4 Deleting all cards from the reader's memory

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

Step 1

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

Step 2

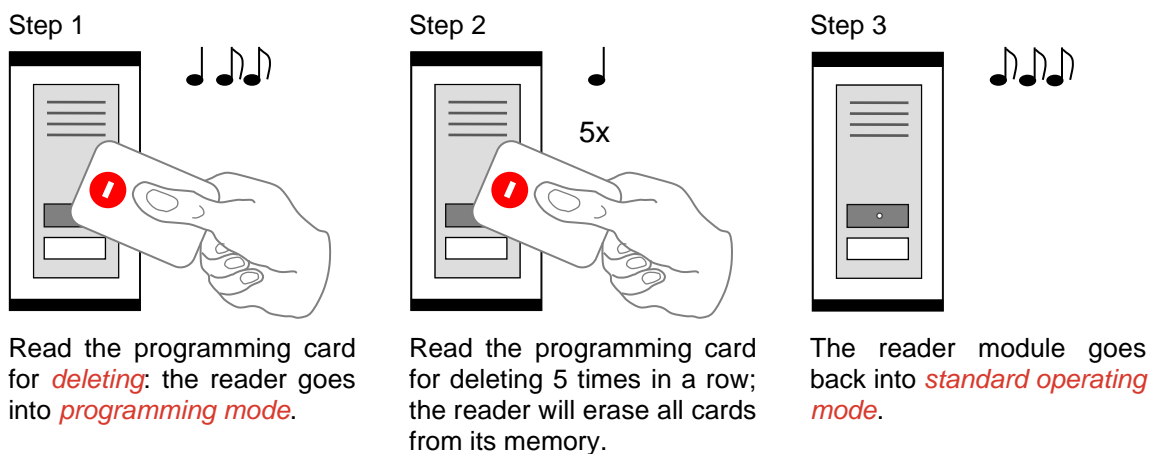Read the programming card for deleting 5 times in a row; the reader will erase all cards from its memory.

Step 3

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

Pic.7 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.7 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
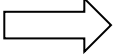
position	card
1	card 1
2	card 2
3	card 3
4	card 4
5	card 5

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

![techfass logo]

- *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.7 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. 7 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

This function is implemented since the FW version 5.0.

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

This function is implemented since the FW version 5.0.

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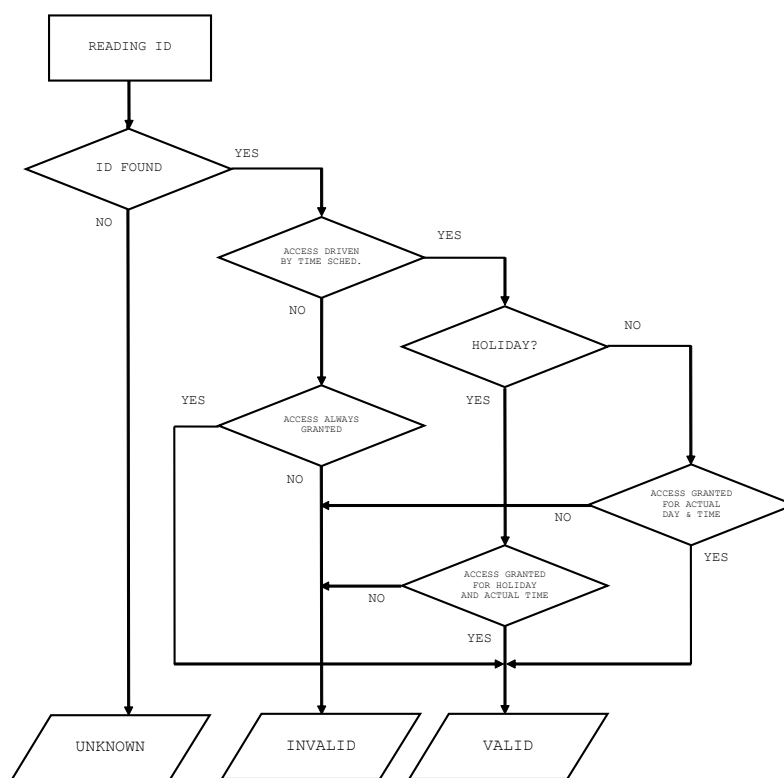
The disabling status changes and disabled actions are logged in the events archive.

6.11 Online authorization

Since the *FW version 5.11* 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.8*.

Pic. 8: Simplified access rights evaluation

8 Useful links

- Wiring diagrams: http://techfass.cz/diagrams-aps-mini-plus-en.html
- Program equipment: http://techfass.cz/software-and-documentation-en.html