

Access terminal MIFARE DESFire

protecting, managing, booking

Fields of application

- Access control
- Time recording
- Time and attendance
- Door management
- Parking systems
- Elevator control

Functions

- Contact less card reader for access control
- Reads serial number (UID) and memory information from MIFARE-DESFire EV1 (AID, File-ID) and MIFARE-Classic (sector, block) cards.
- In case of DESFire EV1 cards a AES-128 bit encryption can be used.
- The reading of MIFARE-Classic cards can be ignored by an option.
- Connection of up to 8 card readers to the door control units **K32/K32Lite** (SecuCrypt-protocol) – limited functionality in case of connection via UCI protocol at **XMP-K24^{plus}**.
- Possibility of firmware updating the card reader from operator station via **XMP-K12/K32/K32L**
- Power supply 12 - 24 V DC by door controller
- Address setting by micro dipswitches
- internal tamper switch
- Signaling elements: 3x LED, 1x buzzer
- Standard housing for mounting in standard outlet sockets
- Possibility of surface mounting by using finery frames (Accessory: XMP-TMC-860)
- Easy installation by connectors

Technical data

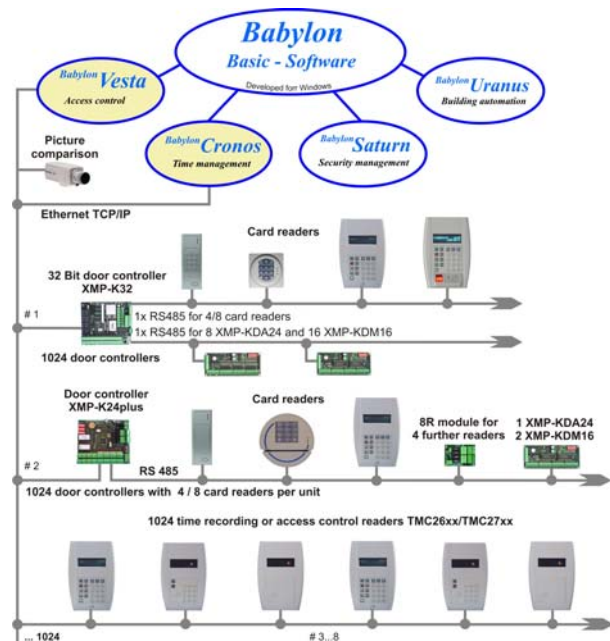
Housing:	ABS material (impact-proofed housing)
Color :	silver
Dimensions (WxHxD):	80 x 80 x 25 mm
Protection type:	IP 54
Power supply:	12-24 V (AC / DC)
Current consumption:	approx. 120 mA at 12V DC
Environmental conditions:	from -20°C to +70°C (operation and storage) UL tested ratings : 0 to +49°C
Interfaces:	RS 485 (2 wire) clock data (Omron Emulation)
Processor:	M16C
Program memory:	16 Bit; 16 MHz; CMOS-Design RAM 20kB Flash-Memory 256kB



XMP-TMC2452



XMP-TMC2462



XMP-TMC2452 / TMC2462

(up to 8 card readers can be connected to the door control units **XMP-K32Lite** / **XMP-K32**)

Legend

XMP-K12: Intelligent door control unit with RS485 and 10/100Mbit LAN interface. Up to 2 access control terminals are connectable. The **XMP-K12** is equipped with 4 digital outputs and supervised inputs.

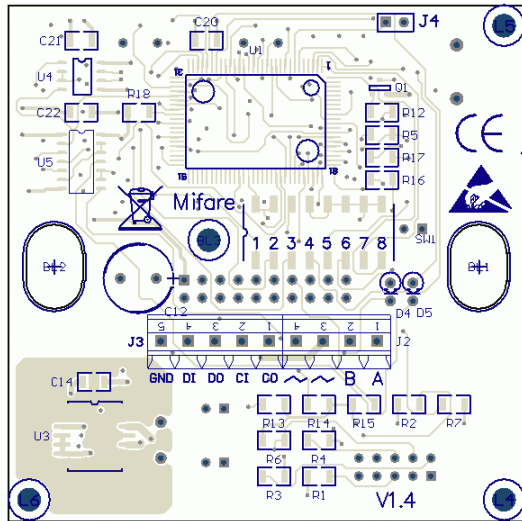
XMP-K32: intelligent door control unit with RS485 and 10/100Mbit LAN interface. 266MHz processor with Linux embedded operating system.

100.000 access levels, **500.000** master data (extendable on **2.000.000**). Up to **500.000** bookings can be stored. Up to 8 access terminals are connectable.

Order Numbers:

XMP-TMC2452

XMP-TMC2462 with PIN-Code keypad

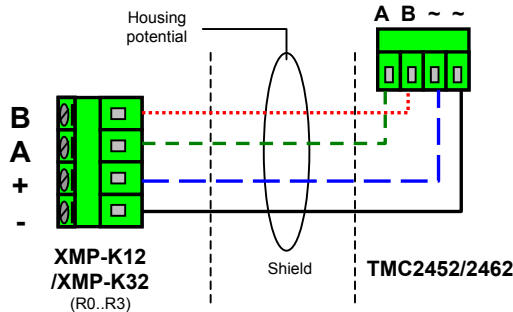


Reverse side of the card reader

XMP-TMC2452/2462 connectors

TMC2452 TMC2462	XMP-K12/K32 (R1..R4)	Description
~	+ or -	Power supply
~	+ or -	Power supply
B	B	Communication interface
A	A	Communication interface

Scheme for connection of the reader to the door control units XMP-K12 and XMP-K32



Details for wiring:

The power supply should be provided central by the XMP-K32 (recommendation). The connection can be realized star- or bus-like (Pay attention on fuse values!). One has to consider the following distances:

Distance	Cable type
until 200 m	2x2x0.8 (shielded)

Meaning of micro dip switches SW1

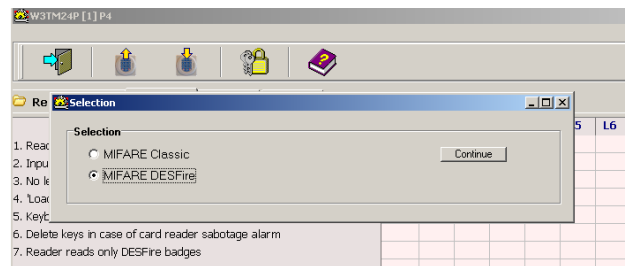
Switch	Meaning
1-3	For binary setting of reader addresses 0...7 (e.g. only switch 1 = ON – reader address 1, or only switch 3 = ON – reader address 4, or 1, 2 and 3 = ON – reader address 7)
4	Default OFF
5	Baud rate setting to K24/K32/K12 OFF = 9600 (recommended); ON = 19200
6	ON = UCI protocol active
7	Reserved
8	ON = Boot loader program activated

Details for reading methods

The TMC2452/2462 reads the **serial number or memory information** of MIFARE DESFire- and MIFARE Classic cards.

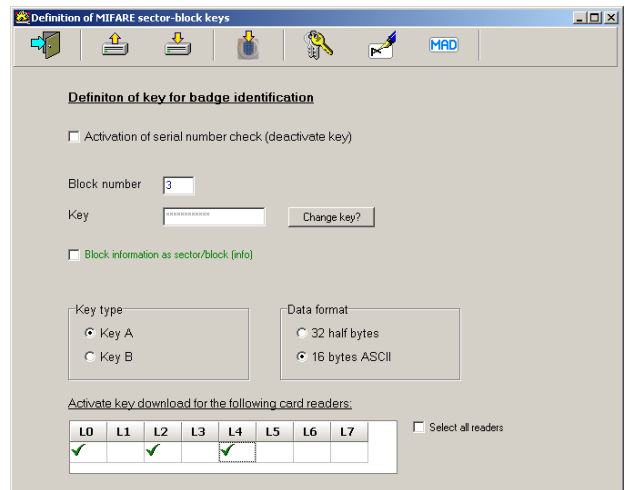
In case of MIFARE Classic cards the serial number of the card (UID) will be transmitted as decimal value (e.g. 40004403886360) and in case of MIFARE DESFire cards as 7 byte hexadecimal value (e.g. 801B76A1726F04) within 14 digits. After delivery the card reader always reads the serial number of a corresponding card.

The parameter setting for reading of special memory information is realized and downloaded into reader by the K32 utility program **W3TM24P**. To do this the reader must be connected to XMP-K32(lite)/K12 via the SecuCrypt communication protocol. The selection to enter the parameter settings for the desired card type is realized by an appropriate selection menu.



MIFARE Classic:

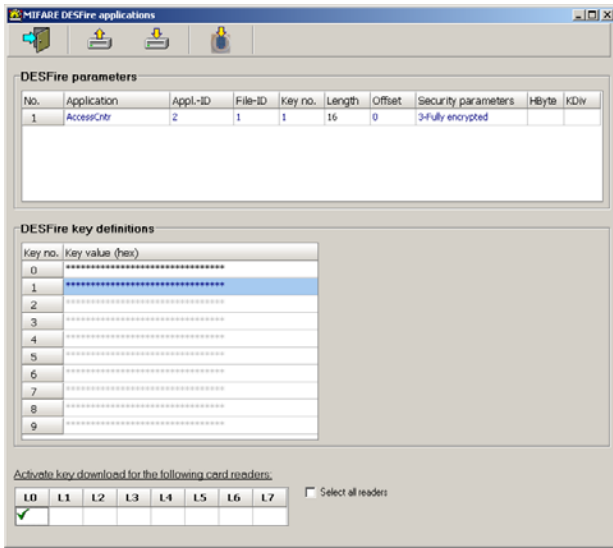
The memory information of a MIFARE Classic card are defined by following parameters: *block number (rel.)* = sequential number of usable blocks, 12 characters *key information*, *key type* and *data format*, which must be entered into the parameter setting program – corresponding to the requirements after the cards coding procedure .



The block contents can be transmitted to the controller as 16 digit (Ascii format) or as 32 digit (half-byte like) information. There is the possibility to download up to five different keys into the card reader. The card reader supports MAD1 (mifare application directory) for MIFARE Classic cards.

MIFARE DESFire:

If „MIFARE DESFire“ was selected the corresponding page for setting the parameters of DESFire specifications.



Up to 10 keys (128 bit AES keys) can be downloaded into the card reader and assigned to a corresponding application (currently, only „AccessCntr“). An AES-128 bit key consists of 32 characters in the range from 0..9,A..F, e.g.:

„A0A1A2A3A4A5A6A7A8A9AAABACADAEAF“

The input of the DESFire parameters and DESFire keys must be adapted to the corresponding card coding parameters. In detail the meaning of the parameters is as follows:

Designation	Meaning
No.	Sequential number of application (currently, only „AccessCntr“ available).
Application	Name of application: AccessCntr = access control by using DESFire memory information UID = reading of the DESFire cards serial number
Appl.-ID	Application ID (also called AID): Application number as decimal value (0..16777215)
File-ID	File number as decimal value (0..15)
Key no	Number of the key (see „DESFire Key Definitions“ in the upper image), that must be used for decryption. Important: The key number must correspond, absolutely, to the key number, that was used also during the coding procedure!
Length	Length of the „return“ information in bytes. If this value exceeds the really coded length on card, the reader will not return any information to the system.
Offset	Designates the number of the start byte, from which the badge information will be returned with number of →“Length” bytes. If the sum of „Offset“ and „Length“ exceeds the really coded length on card,

	the reader will not return any information to the system.
Security parameters	Defines the transmission type (encryption, data integrity) for the air interface. <ol style="list-style-type: none"> Plain, without key → no authentication for access on application required. Plain, with key → access on application is only possible with correct authentication (128 bit AES keys). Data, which are read from card will be transmitted plain to the card reader. Fully encrypted → access on application is only possible with correct authentication (128 bit AES keys). Data, which are read from card will be transmitted fully encrypted (including checksum) to the card reader. The decryption of the card information is realized within the card reader. MACed with key → access on application is only possible with correct authentication (128 bit AES keys). Data, which are read from card will be transmitted plain to the card reader in connection with a special 8 byte checksum (MAC) that is attached to the data. Basis for calculation of the MAC checksum is also the 128 bit AES keys. Only in case of a positive check the badge information will be forwarded to the door controller.
HByte	If the badge information is not coded as ASCII it is also possible to transmit these information to the door control unit as half-byte information. <u>Example:</u> ASCII data: ..'1234'.. As half bytes→..31323334...
KDiv	Currently, the key diversification is not available.

Remarks to reading distance

Besides other, the reading distance depends on environmental conditions, badge types and reading method just used. In case of MIFARE-Classic badges the reading distance is maximum 70 mm. In case of DESFire cards the reading distances are maximum 60 mm if no AES encryption is activated. If the encryption is active the reading distance will reduce on approx. 20..30 mm. Metal parts in a distance of 120 mm can reduce the reading distance, too. The distance between two installed card readers should be minimum 20 cm, because of the fact, that the electro-magnetic fields of the readers – concerning the reading distances - affect each other in disadvantageous way.

Recommended card types: ISO Standard

Meaning of the LEDs

yellow: operation state
yellow blinking: no communication
red: not authorized
green: authorized
Reverse side D4: communication TXD
Reverse side D5: communication RXD

Communication protocols

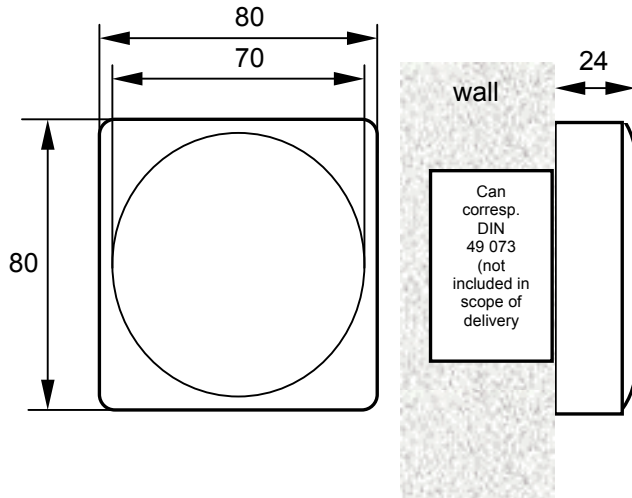
SecuCrypt® - Blowfish encryption

(Hint: only available for XMP-K32/K32lite/K12)

UCI - Omron 5 bit format (magnet stripe)

(Hint: XMP-K24^{plus} – firmware version: 3.8)

Dimensions in mm



Card reader with stable finery frame **XMP-TMC-860**
Frame dimensions: 86.0 x 86.0 x 23.3mm

Important customer info!

Defective plates must be disposed professionally.

Batteries and accumulators are hazardous waste.

The packing can be used again or must be disposed. The green filling material can be disposed as Bio waste.

