MorphoAccess® VP MD

Installation Guide

Osny, France

Warning

Information in this document is subject to change without notice and do not represent a commitment on the part of IDEMIA.

This document contains information of a proprietary nature to IDEMIA and is submitted in confidence for a specific purpose. The recipient assumes custody and control and agrees that this document will not be copied or reproduced in whole or in part, nor its contents revealed in any manner or to any person except to meet the purpose for which it was delivered.

This caveat is applicable to all the pages of this document.

This manual makes reference to names and products that are trademarks of their respective owners.

Revision History

The table below contains the history of changes made to the present document.

Version	Date	Reference	Description
01	April 2019	2019_000000XXXX-V0	Document creation

Table of Content

Table of Figures

Section 1 : Introduction

MorphoAccess® VP MD terminals

Congratulations for selecting the MorphoAccess® VP MD, first ever Physical Access Control terminals to integrate the state of the art multimodal technology combining finger vein and fingerprint biometrics.

This terminal brings to access control systems the strong assets of the finger vein/fingerprint multimodality:

- the capability to address those individuals who usually experience difficulties to use mono-modal biometric devices,
- an excellent FRR@FAR ratio, which allows a high security level without affecting comfort of use,
- an enhanced resistance to spoofing (by combining the protection mechanisms intrinsic to each technology and also by making the most of the new characteristics resulting from the fusion of the two biometrics),

while offering the same easiness of use which makes finger biometrics-based systems quickly adopted by end-users.

In addition, the MorphoAccess® VP MD offers the following advantages:

- high quality optical sensor (IQS quality sensor),
- supports multiple input/output interfaces used in the physical access control industry,
- Local Area Network interface for easy interaction with other host systems ; LAN and WLAN possibilities (Wi-Fi™ as an option),
- practicality at installation and connection, as illustrated by this installation guide.

We definitely believe that our MorphoAccess® VP MD will come up to the expectations of our faithful and most demanding partners, as the ultimate solution for Security, Accuracy and Performance of their equipments!

To ensure the most effective use of your MorphoAccess® VP MD terminal, we recommend that you read this Installation Guide completely and attentively.

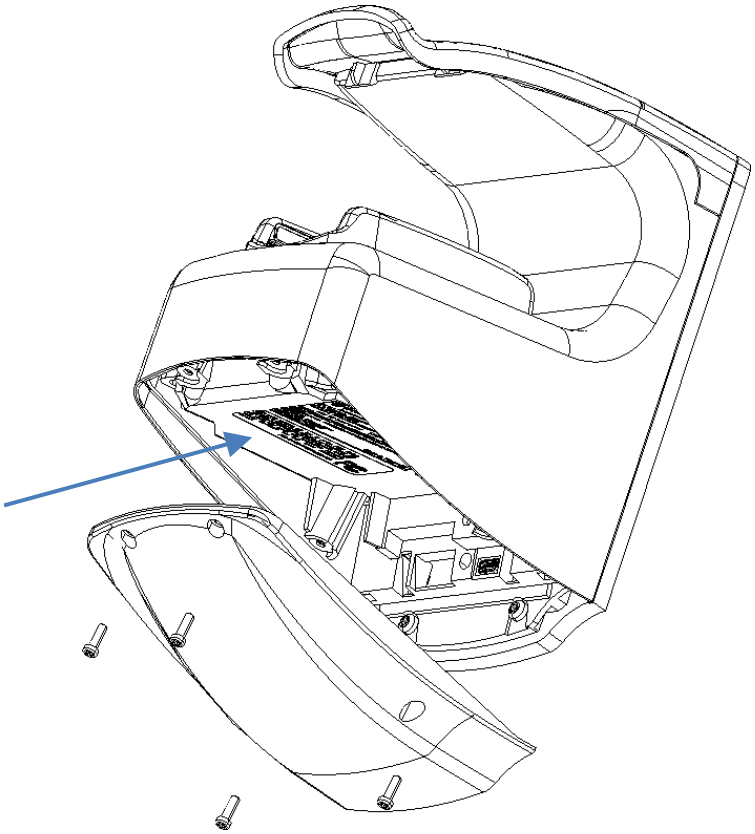
Scope of the document

This guide deals with the installation of MorphoAccess® VP MD, which is made up of following list of products:

MA VP DM Marketing Name	Multimodal finger vein/ fingerprint biometrics	MIFARE®/DESFire® Contactless smartcard readert	Water Resistant	Regulatory Model Number (*)
MorphoAccess VP MD	✓	✓	✓	MPH-AC005A

(*) The Regulatory Model Number is the main product identifier in the regulatory documentation and test reports associated to the product

The Regulatory Model Number and other product identification informations can be found on the stickers at the bottom of the product after removing bottom cover :



Safety Instructions

 means Direct Current (DC)

The installation of this product should be made by a qualified service Person and should comply with all local regulations.

It is strongly recommended to use a class II power supply at 12VDC 1A minimum in conformity with Safety Electrical Low Voltage (SELV). The power supply cable length should not exceed 10 meters.

This system must be installed in accordance with the National Electrical Code (NFPA 70), and the local authority having jurisdiction.

This product is intended to be installed with a power supply complying with IEC60950-1, in accordance with the NEC Class 2 requirements; or supplied by a listed IEC60950-1 external Power Unit marked Class 2, Limited Power source, or LPS and rated 12VDC, 1A minimum or 24VDC, 0,5A minimum.

In case of building-to-building connection (power source in a building, and terminal in another building), it is recommended to connect the 0V of the power supply to the earthing system of the building. And the terminal block Power Ground must be connected with the earthing system of the other building.

Note that all connections of the MorphoAccess® VP MD terminal described hereafter are of SELV (Safety Electrical Low Voltage) type.

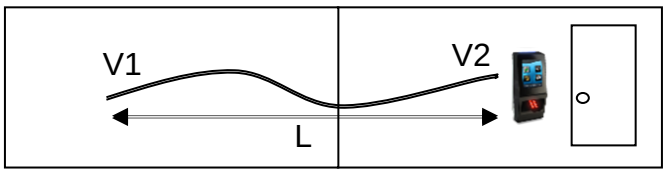
Wiring Recommendations

IDEMIA recommends using a gauge AWG20 for 12VDC power supply (when the terminal is not powered using POE feature).

The voltage must be measured on the product block connector and must be equal to 12VDC-24VDC (-15% / +10%)

For information, this table shows the maximum drop voltage observed on the terminal MorphoAccess® VP MD, depending on the length of the cable:

Gauge AWG	Diameter (mm)	Maximum drop voltage @ 1m (V)	Maximum drop voltage @ 5m (V)	Maximum drop voltage @ 10m (V)
18	1.02	0.02	0.11	0.21
20	0.81	0.03	0.17	0.33
22	0.64	0.05	0.26	0.53
24	0.51	0.08	0.42	0.84



Drop voltage = loss of power due to wire resistance and its length:

V2 = V1 – Drop voltage

Regulatory, safety and Environmental notices

European Union (CE) regulatory notices

Declaration of Conformity

CE

Products bearing the CE marking comply with one or more of the following EU Directives as may be applicable:

- EMC Directive 2014/30/EU.
- RED Directive 2014/53/EU.
- ROHS Directive 2011/65/EU.

Compliance with these directives is assessed using applicable European Harmonised Standards.

MorphoAccess® VP MD is intended to be used for professional application only (buildings, airport...).

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce magnetic emissions to prevent interference to the reception of radio and television broadcast.

The full Declaration of Conformity is available on demand to your reseller. Please, provide him the product model name or its Regulatory Model Number (Model on the label).

Products with wireless features (EMF)

This product meets the provisions of the EU's Council recommendation 1999/519/EC on the limitation of the exposure of the general public to electromagnetic fields (0 Hz to 300 GHz).

USA (FCC) regulatory notices

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Responsible Party:

IDEMIA Identity & Security France

2, place Samuel de Champlain

92400 Courbevoie – France

NOTE: *This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:*

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded cables must be used with this unit to ensure compliance with category B FCC restrictions.

Canada (IC) regulatory notices

WARNING TO USERS IN THE CANADA / ATTENTION POUR LES UTILISATEURS AU CANADA

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada.
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) il ne doit pas produire de brouillage, et (2) l'utilisateur du dispositif doit être prêt a accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.
Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada.
Dans le but de réduire les risques de brouillage radioélectrique à l' intention d'autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

.

~~Note : UL LLC has not verified this product for compliance in respect to Canadian standards.~~

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada.
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Others recommendations

The MorphoAccess® VP MD incorporates a capacitive sensor for contactless finger presence detection.

In the presence of electromagnetic disturbances, this function can be activated inadvertently. This behavior remains normal (the electromagnetic field modifies the capacity of the sensor) and has no impact for the user (the access control remains functional) outside the light signal. To avoid the light signal, Idemia recommends the use of an EMI filter on the power lines and recommends, as far as possible, to install the MorphoAccess® VP MD at a sufficient distance from the antennas of potential RF transmitters.

Potential safety conditions notice

If you notice any of the following conditions (or if you have other safety concerns), do not use the product: crackling, hissing, or popping sound, or a strong odor or smoke coming from the product. It is normal for these conditions to appear when an internal electronic component fails in a safe and controlled manner. However, these conditions may also indicate a potential safety issue. Do not assume it is a safe failure. Turn off the product, disconnect it from its power source, and contact technical support for assistance.

Disposal of waste equipment by users

This symbol means do not dispose of your product with your other household waste. Instead, you should protect human health and the environment by handing over your waste equipment to a designated collection point for the recycling of waste electrical and electronic equipment.

Recommendations for terminal implementation

Every installation is unique. Sometimes the issues are well defined and can be handled in a standard fashion; sometimes the issues are very specific and may not be immediately recognizable.

IDEMIA recommends following these steps for a successful installation:

- **Plan the installation** - Choose the type of hardware required, decide if a network is required, and decide on the location and number of required terminals.
- **Unpack all items** - Unpack all items and check against the packing list.
- **Install network hardware components** - Install the cabling and components needed to run the system.
- **Install software** - Install the software needed to set up the terminals.
- **Pre-configure device** - Connect the terminals to the Ethernet, supply power to the terminals, and pre-configure the terminals.
- **Mount devices** - Mount the terminals in their final locations
- **Power distribution and device hook up** - Connect the terminals wiring via the back panel.
- **Power-up procedure** - Check the power connections, and then start the system safely.

To secure properly an access, IDEMIA recommends installing the MorphoAccess® VP MD terminal as a part of the typical Access Control environment, as the one described in the figure below.

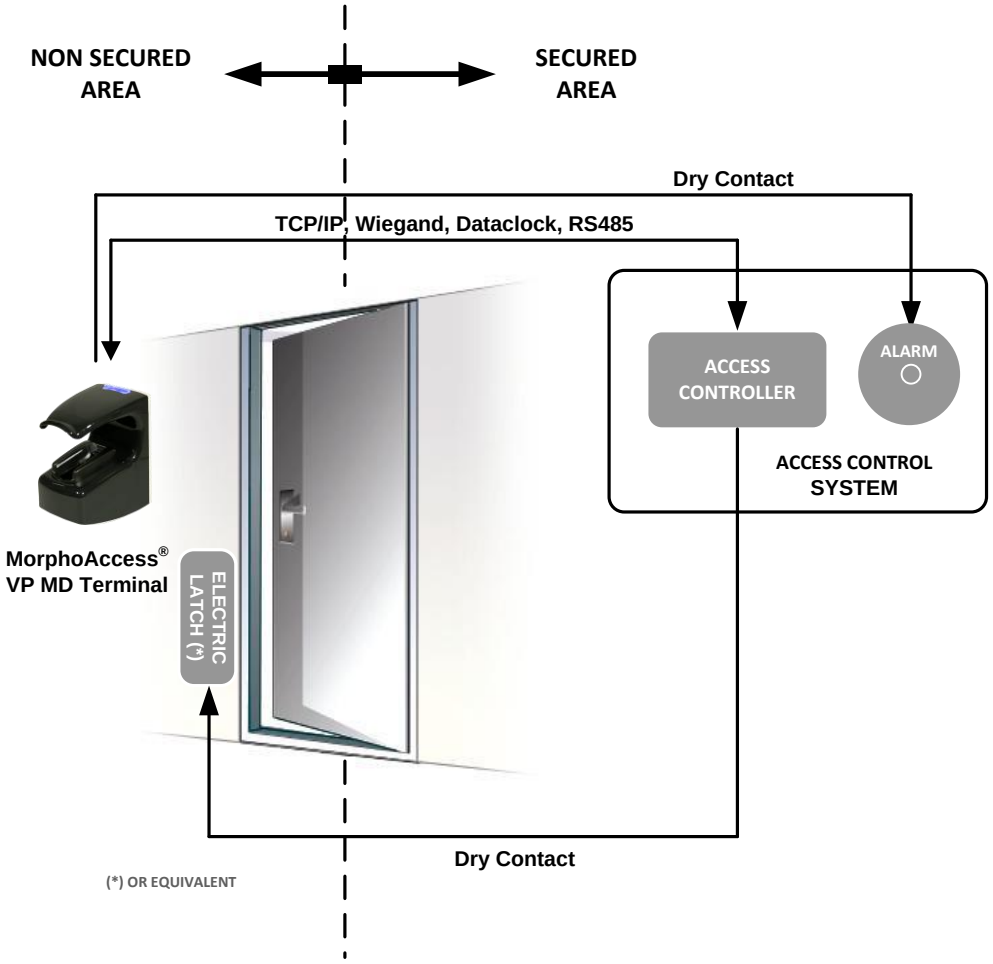


Figure 1: Implementation Recommandations

This environment comprises:

The MorphoAccess® VP MD terminal itself

Its role is to perform one-to-many multimodal biometric identification or one-to-one multimodal biometric verification, i.e. to identify the individual who is presenting his finger on the terminal sensor by comparing his biometric data with the references previously stored in the terminal database (in the form of multimodal biometric templates) or to verify his identity using the reference stored in a contactless card presented to the terminal.

An Access Controller (3rd party product)

The Controller is the element which controls the access rights of the individuals to the secured area. For that reason, it must be located in the secured area.

The individuals who are authorized to access the secured area have their User ID listed in a so-called "authorized user List" (in contrast with a banned card list).

The MorphoAccess® VP MD terminal and the Controller are communicating using one of the available protocol (TCP/IP, Wiegand, Dataclock, or RS485). The typical process is described below:

- After access request, and local checks, the MorphoAccess® VP MD terminal sends the User ID, and the result of local checks, to the Controller
- The Controller performs additional checks, and sends its decision to the MorphoAccess® VP MD terminal (which displays GREEN light if access is granted or RED light if denied), and to the electric latch of the door (though a door controller) if access is granted to the user
- The MorphoAccess® VP MD terminal sends an alarm signal to the Controller as soon as a malicious operation is detected (terminal pulled out from the wall or opened); please refer to the paragraph dealing with anti-pulling and anti-tamper switches for more explanations.

The Controller is part of the global Access Control System of the secured area, which can provide useful features such as manage:

- authorized user lists (i.e. for VIP),
- banned card lists (i.e. for lost user cards),
- an access request log (who and when, access granted or denied,..),
- an event log (i.e. tamper detection, access control for evacuation of the building,...).

The MorphoAccess® terminal is able to work alone, without Controller, but the protection level of the secured area is lower.

An Alarm (3rd party product)

This element is connected to the MorphoAccess® VP MD terminal through a dry contact.

The MorphoAccess® VP MD terminal sends the command to activate the Alarm as soon as a malicious operation (terminal pulled out from the wall or having its bottom cover opened out of maintenance operations) is detected; please refer to the paragraph dealing with anti-pulling and anti-tamper switches for more explanations.

A Electric door strike or equivalent (3rd party product)

The activation of this element, open the door or the gate, to provide the physical access to the protected area. The Controller is the one which sends the command to activate the strike if access is granted (i.e. if the individual's User ID is listed in the Controller authorized user List). Connection between these two elements is done through a dry contact.

Section 2 : General Description

Box opening

At the box opening, components shall be extracted from the protection casing as depicted in the pictures below.

Extract the bottom cover and the wall plate (which are not screwed to the terminal) and keep them separate until the installation of the terminal is completed. The screwing of the bottom cover is the last stage of the installation.

Do not forget to withdraw the sachet of screws, bolts and connectors from the white protection casing.

Figure 2: Box Opening

Components of the initial package

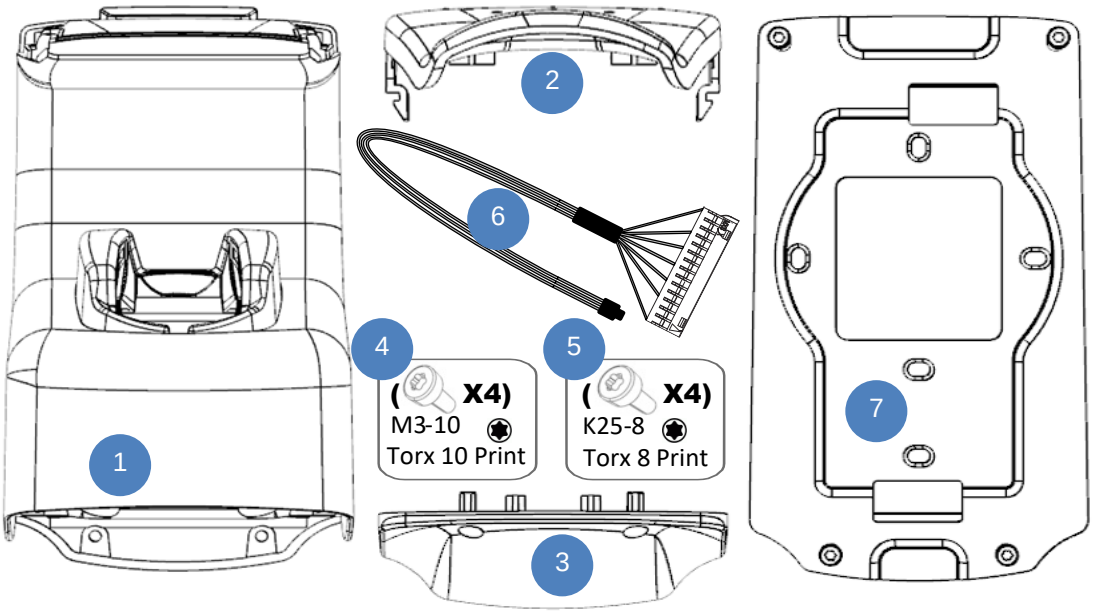


Figure 3: Box Content

1. One (1) Terminal's body
2. One (1) top cover fixed at the body of the terminal
3. One (1) bottom cover
4. Four (4) M3X10 Screws (for terminal fixing to the wall plate) – T10 Torx and 4mm flat print
5. Four (4) K25x8 Screws (Bottom cover fixing) – T8 Torx Print
6. One (1) Connection cable
7. One (1) Wall frame

Terminal's front view description

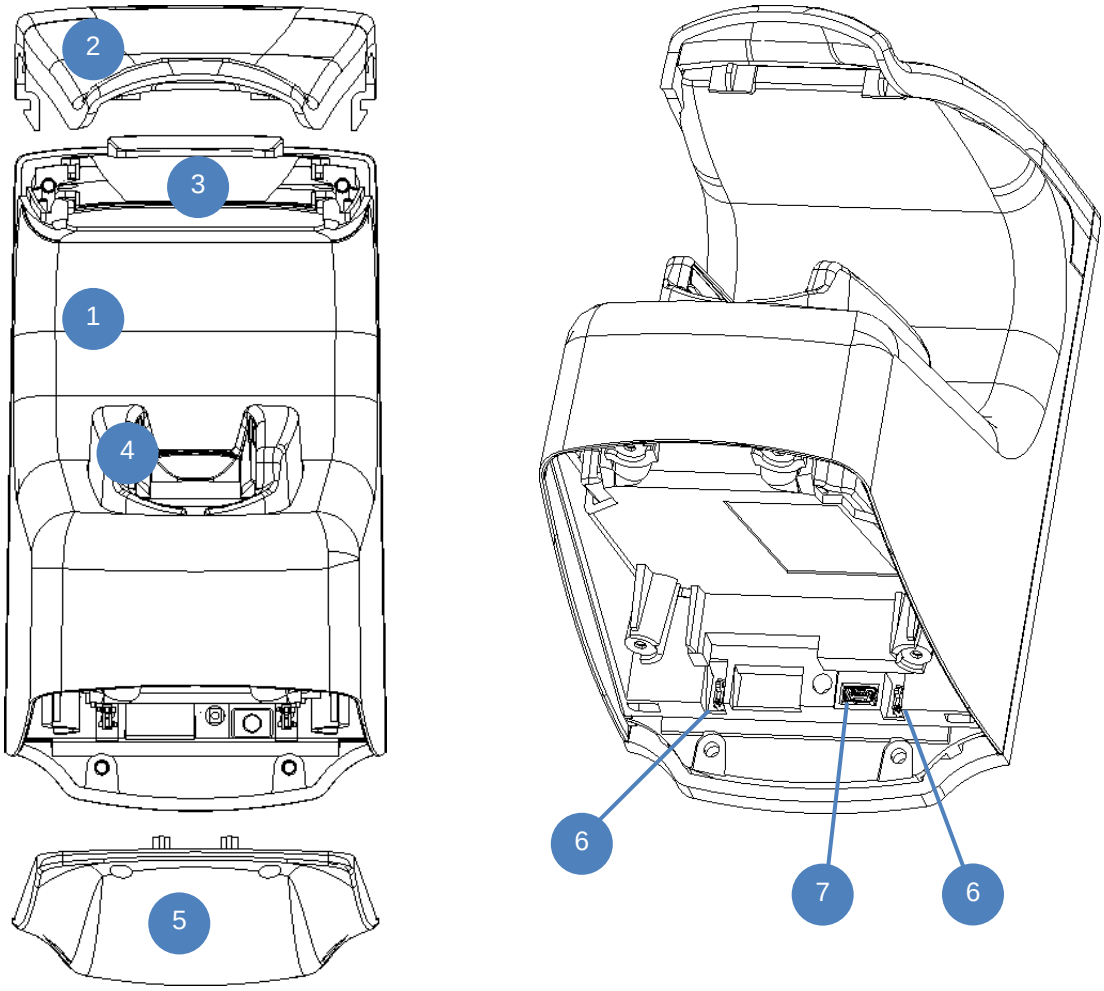


Figure 4: MorphoAccess® VP MD terminal front view

1. Terminal's body
2. Top cover
3. Contactless card reader
4. Multimodal biometric sensor (optical)
5. Bottom cover
6. Anti-tamper switches
7. USB port (for configuration and settings with a USB mass storage key, or for installation of a Wi-Fi™ USB dongle)

Terminal's rear view description

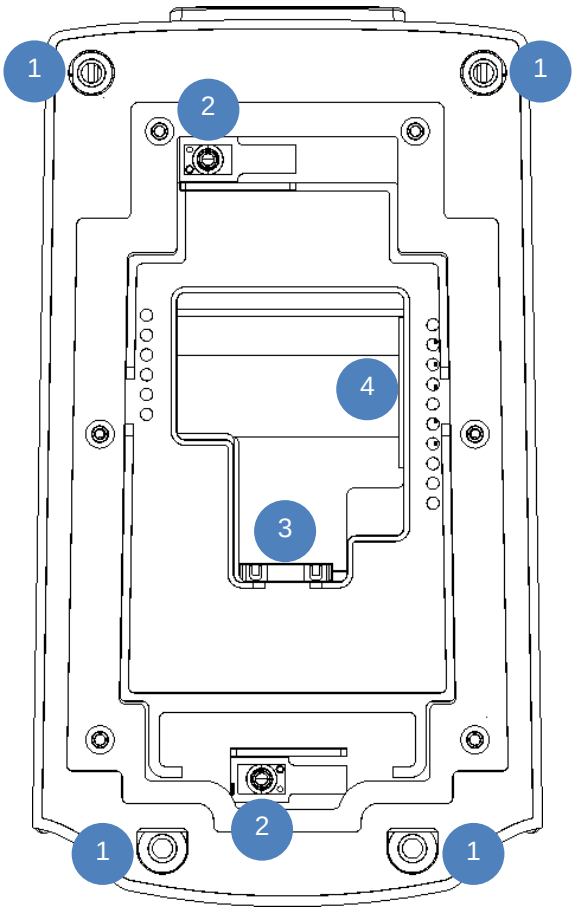


Figure 5: MorphoAccess® VP MD terminal rear view

1. Mounting holes (4)
2. Anti-pulling switches (2)
3. RJ45 (Ethernet and Power Over Ethernet)
4. Terminal blocks

MorphoAccess® VP MD Technical Characteristics

Item	Description
Access control modes	Identification (search for multimodal biometric data in a local database)
	Authentication with contactless card, with or without multimodal biometric data check (only if terminal equipped with a smartcard reader)
	Multi-factor: identification or authentication
	Proxy: the access control check is fully driven by a remote system
Man Machine Interface	Multi color LED
	Multi tone Buzzer
Biometrics	MorphoSmart™ FINGER VP Biometric module inside for multimodal biometric comparison. With 500dpi, 256 gray levels optical sensor, PIV IQS certified by the FBI
	False Acceptance Rate (FAR) adjustable from 10^{-2} down to 10^{-8}
	Database capacity: 5000 users (standard) or 10 000 users (with specific license).
Log capacity	100 000 records (standard) and up to 1 000 000 (with specific license)
LAN/WLAN connection	For terminal configuration and data transfer: Ethernet 10/100 Base T (MDI, MDI-X) Or Wi-Fi™ Wireless LAN (option), WEP, WPA (PSK) and WPA2 (PSK) encryption available Either TCP, TLS or SSL protocol
RFID cards (depending on product version)	MIFARE® 1k, 4k MIFARE® PLUS S (SL1, SL3) 2k, 4k
	DESFire® 2k, 4k, 8k
Serial port	The serial port supports WIEGAND, DATACLOCK (ISO2) and RS485 protocols

Output relay switches	Access granted: 1 switch two outputs (normally “open” and normally “closed”) 30V DC – 1A max (Resistive/inductive loads)
USB host port	Front port for terminal configuration through a USB mass storage key or for Wi-Fi™ USB dongle.
Input signals	LED1/LED2 to activate the access granted relay
Power supply	12 to 24 V DC power supply (1A min @12V) Or by Power Over Ethernet through RJ-45 connector
Security of the terminal	Anti-tamper-pulling switches. Tamper-pulling detection: one relay switch.
Size and weight	W x H x D: 90 mm x 160 mm x 125 mm (3.54” x 6,3” x 4,92”) 675g with wall plate 515g without wall plate
Environmental conditions	Operating temperature -10 °C to + 50 °C (14°F to 122°F)
	Operating humidity 10 % < RH < 80 % (non condensing)
	Storage temperature -20 °C to + 70 °C (-4°F to 158°F)
	Storage humidity 5% < RH < 95 %
	IP55 rated for outdoor use (once wall-mounted)
	The terminal should be installed in controlled lighting conditions. Avoid direct exposure to sunlight or to UV lights.
Certifications	CE, IEC 60950-1, FCC Part 15, RSS210 - Issue 8 : 2010, RSS-102 - Issue 5 : 2015, RSS-Gen – Issue : 2014, RoHS, WEEE

Section 3 : Installation Procedure

Before proceeding to the installation

- Make sure that you have all the components described in “Components of the initial package” section at your disposal.
- Remove the bottom cover from the terminal (with its gasket), the top cover (see Figure 6: Removing the top cover for how to unclip it) and the wall plate. Keep these elements at hand.

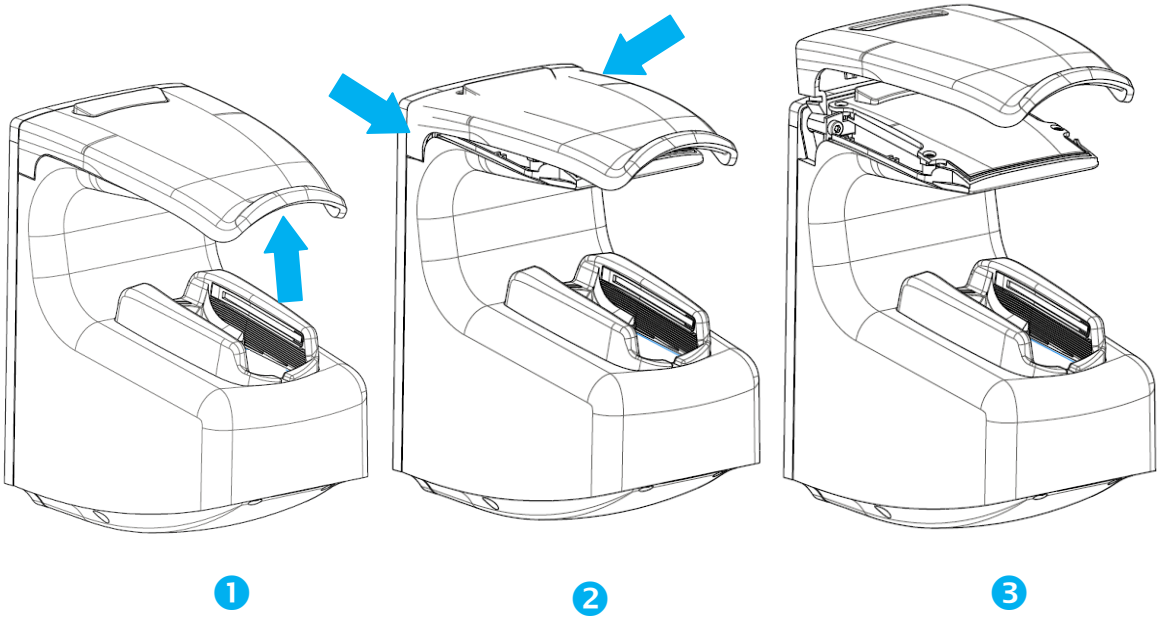


Figure 6: Removing the top cover

It is then possible to fix the terminal:

- either directly on a wall,
- or using a standard electric case (not provided).

The recommended height for fixing of the terminal lies between 1m and 1.20m.

For an optimal use the terminal must be installed in an area where the lighting conditions are controlled. Avoid direct exposure of the sensor to the sun light and to the ultraviolet rays (UV).

Installation

Required tools (not supplied)

- Two (2) rawplugs + two (2) ø 3.5mm max and length 30mm screws.
- One (1) screwdriver adapted to screws above.
- One (1) Drill (with a drill bit diameter adapted to rawplugs above).
- One (1) hole saw ø 67mm.
- One (1) Flat tip screwdriver (2,5mm) for block connector screws.
- A (1) Torx T10 screwdriver or a (1) regular 4 mm screwdriver.
- A (1) Torx T8 screwdriver.

- Deadbolt/door strike
- Snubber diode required to protect regulated DC power supply from inductive kickback (1N4007 diode or equivalent recommended)
- Separate power supply for the deadbolt/door strike based on supplier's recommendations.
- External relay (if required)
- Networking cable

Equipment from the initial package to use

- One (1) Terminal’s body.
- One (1) wall plate.
- Four (4) M3x25 screws.
- One (1) bottom cover.
- Four (4) K2.5x8 screws.
- Two (2) Block connectors.
- One (1) top cover.

Step by step procedure

The recommended height for fixing of the terminal lies between 1m and 1.20m.

For an optimal use the terminal must be installed in an area where the lighting conditions are controlled. Avoid direct exposure of the sensor to the sun light.

Power supply from electrical source shall be switched off before starting the installation.

The strength of the attachment depends on the solidity of the wall on which the terminal is mounted.

The adhesive foam joint at the back of the wall plate is required for sealing purposes (watertightness). If walls have a rough or uneven surface, a silicon bead may be required between the wall plate and the wall to ensure sealing.

Drilling the mounting holes

If not present, drill in the wall a hole with a diameter adapted to the width of the terminal and the cable to be hosted in (see Figure 7: Drilling template This template at scale 1:1 can be found in the Quick Installation Guide).

Confirm the presence inside the hole of all the cables needed for the electrical installation (see Electrical Interface)

Drill in the wall 2 holes with a diameter adapted to screws and fit them with the raw plugs (see Figure 7: Drilling template and Figure 8: Wall plate fixing).

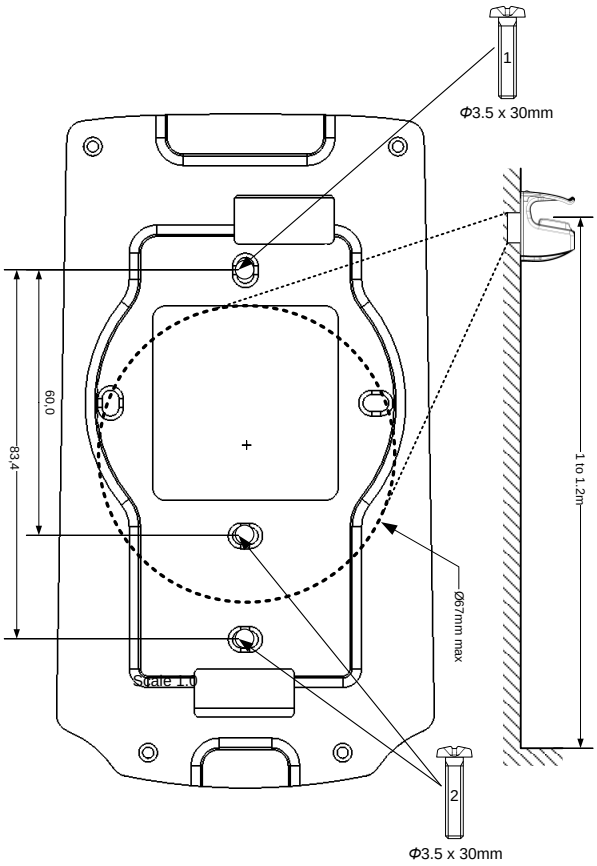


Figure 7: Drilling template

Fixing

Be sure that a sufficient space is reserved in the wall for the passage of cables, in particular for Ethernet cable and plug, and also for the Wi-Fi dongle (if applicable).

Place the wall plate against the wall, opposite the four holes pierced in the wall (see Figure 8: Wall plate fixing).

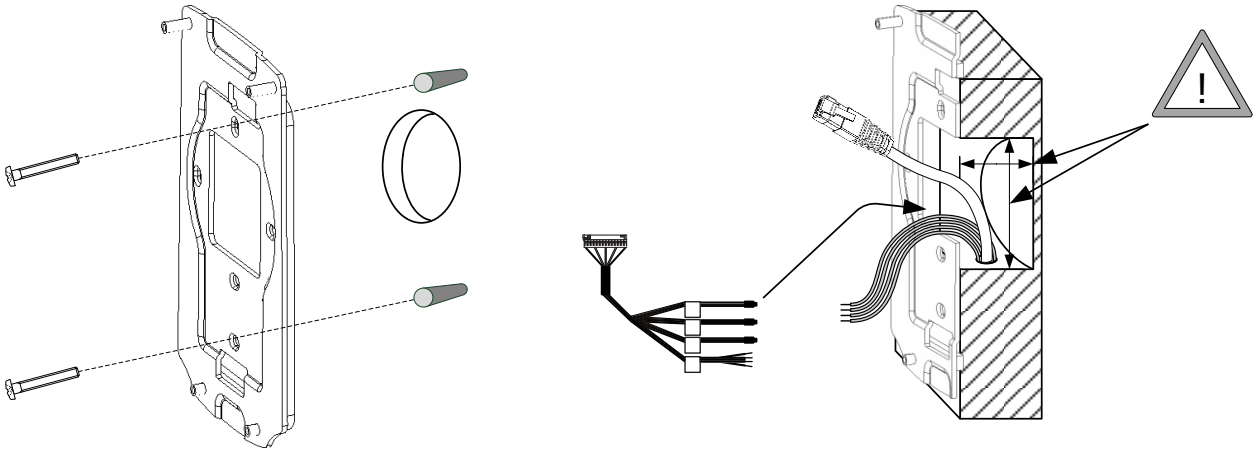


Figure 8: Wall plate fixing

Fix the wall plate using the two screws that fit the rawplugs (Max diameter: 3.5 mm, length 30 mm) (see Figure 7: Drilling template and Figure 8: Wall plate fixing). Use the 2 upper screw shanks to make sure that the wall plate is mounted horizontally.

Cabling

Cable for wiring shall be AWG 20 to 24, length shall be adapted to the size of the hole in the wall, to terminal connections, and to the distance between the electric source and the terminal itself.

Plug Ethernet cable (if present) into the RJ45 connector (see Figure 5: MorphoAccess® VP MD terminal rear view).

Terminal body mounting

Fix Terminal's body with four (4) M3x8 screws (see Figure 9: Terminal's Body fixation)

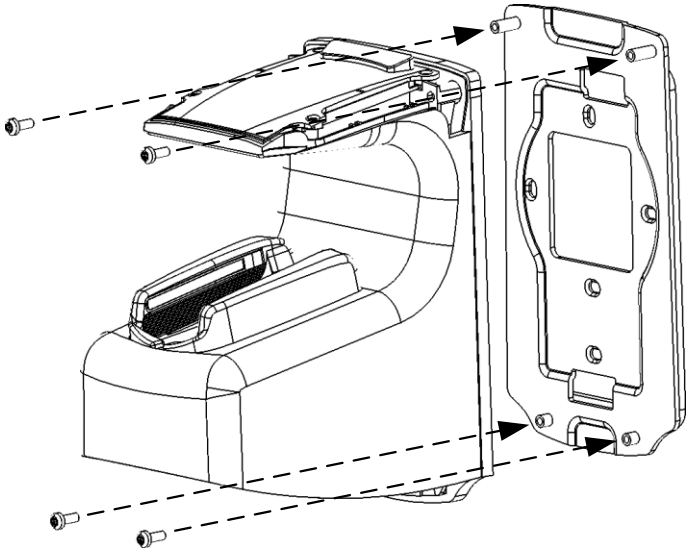


Figure 9: Terminal's Body fixation

Closing

Clip the top cover (see Figure 6: Removing the top cover, following steps 1 to 3 in reverse, and Figure 10: Assembling top and bottom covers).

Screw on the bottom cover (see Figure 10: Assembling top and bottom covers1), using the four K2.5 x 8 screws.

Power has to be set up just after closing it. If product has to be stored for a long time (more than 48 hours), don't forget to restore its configuration before use.

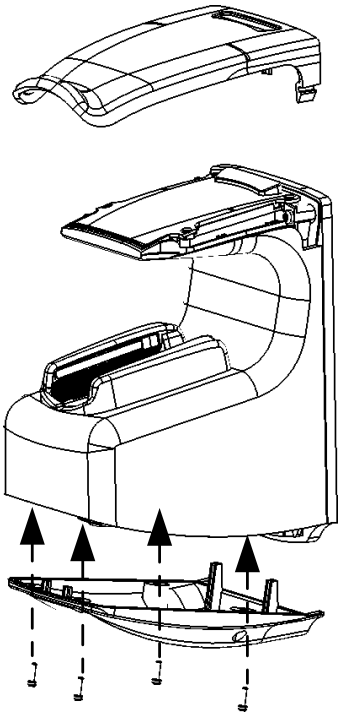


Figure 10: Assembling top and bottom covers

Section 4 : Electrical Interface

Wiring overview

Before proceeding, make sure that the person in charge of installation and connections is properly connected to earth, in order to prevent Electrostatic Discharges (ESD).

Power supply ground shall not be used for peripheral ground. All other grounds can be used indifferently.

Note that all connections of the MorphoAccess® VP MD terminal described hereafter are of SELV (Safety Electrical Low Voltage) type.

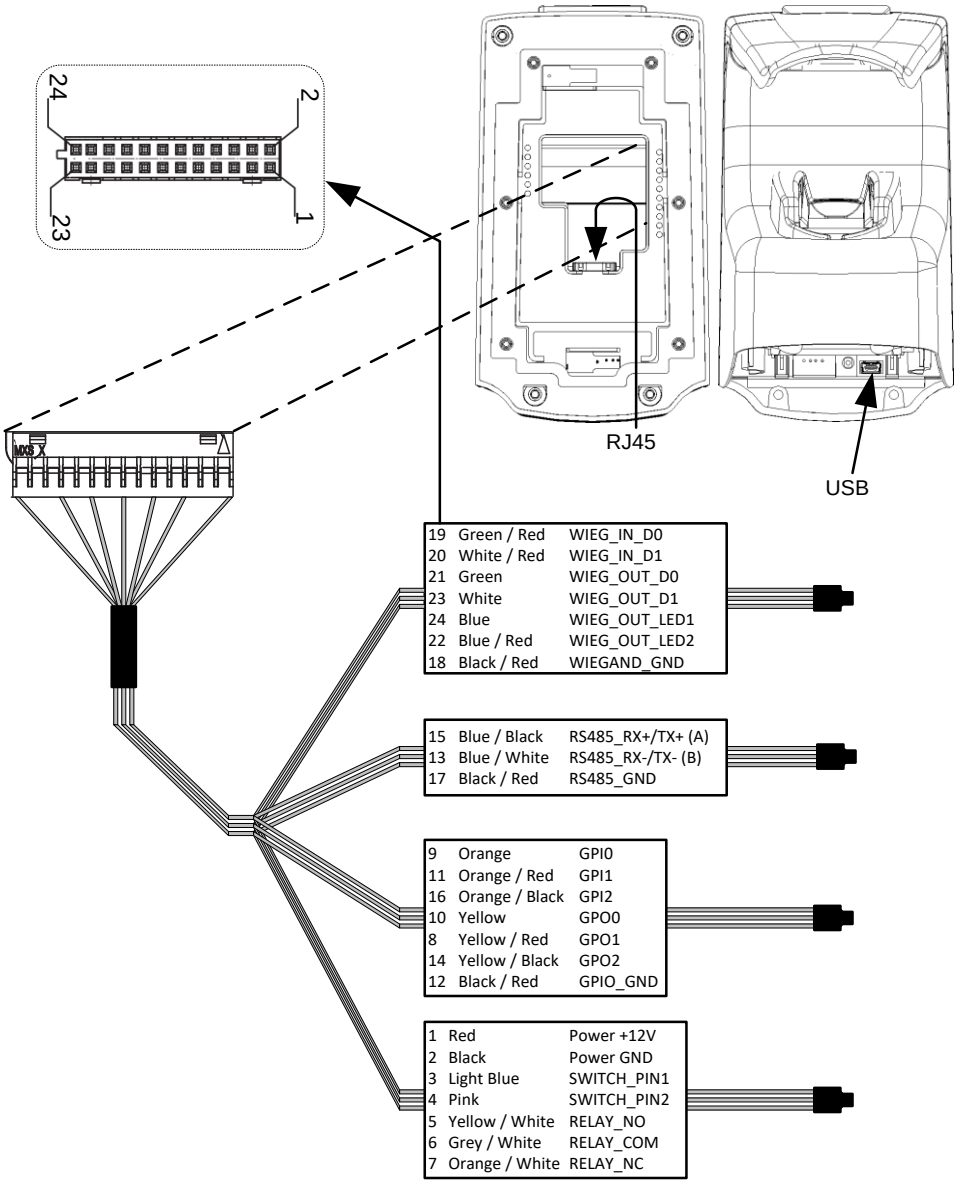


Figure 11: Cabling layout

Power Supply

POE and external power supply can be used simultaneously, but when both power supplies are available, priority is given to external power supply. If the external power supply fails or is shut down, the terminal will go off and then restart using POE.

External Power supply

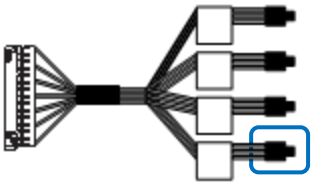


Figure 12: Power supply wiring

1	Red	Power Supply 12V	In	Positive 12 Volts, power supply
2	Black	Power ground	In	Ground power supply

External power supply

- Must comply with CEE/IEC EN60950 standard.
- 12V to 24V DC (regulated) 1 Amp min at 12V.
- Could be provided by a 12 Volts Wiegand power supply, which complies with the Security Industry Association's Wiegand standard March 1995.)

POE (Power Over Ethernet)

MorphoAccess® VP MD terminal's power supply can also be provided by the Ethernet using RJ45 connection (Power Over Ethernet mode - IEEE802.3af or IEEE802.3at type 1 compliant).

Output Relay

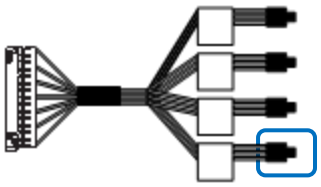
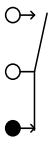


Figure 13: Output relay wiring

5	Yellow / White	Relay NO		Contact relay (normally open)
6	Grey / White	Relay COM		Contact relay common
7	Orange / White	Relay NC		Contact relay (normally closed)

Nominal characteristics of relay

Load characteristics:

- 1 A max @ 30 VDC (according to the safety extra low voltage requirements independently of the power supply),
- Resistive load or inductive load; see warning information hereafter for inductive load.
- The internal relay is designed for at least 100 000 cycles.

Inductive load management requires a parallel diode for a better contact lifetime.

Example of connection for electrical door locks

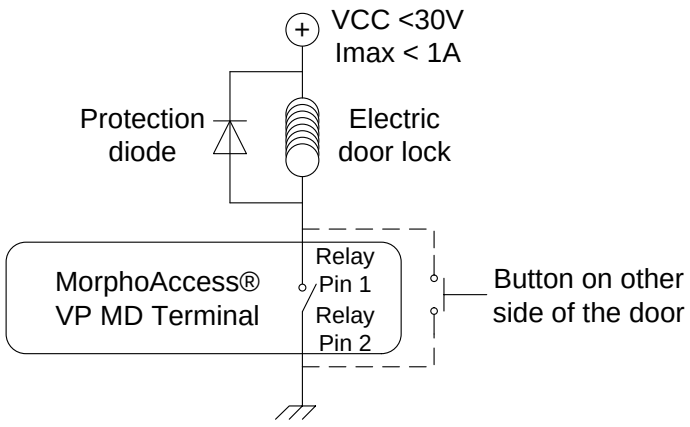


Figure 14: Example of electric door strike connection

Tamper Switch

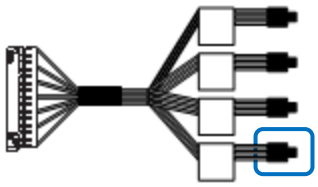


Figure 15: Tamper switch wiring

3	Light Blue	Switch 1		Tamper switch contact
4	Pink	Switch 2		Strip on tamper switch

Operating principle for the switch

- Product installed on the wall plate: switch enabled (contact closed).
- Product opened (rear connectors accessible): switch disabled (contact open).

Nominal characteristics of switch block

Electrical characteristics: 100 mA at 30 VDC max (Resistive load) according to the safety extra low voltage standard.

This MorphoAccess® VP MD terminal is part of security system; it is customer's responsibility to connect the tamper switch (contact) to physical access controller, in order to detect unauthorized access to the connector blocks.

Wiegand port wiring

Wiegand input wiring

The following figure shows how to cable the wires of the “Wiegand In” port of the terminal for Wiegand protocol. This is used, for instance, to connect an external card stripe reader to the MorphoAccess® VP MD terminal.

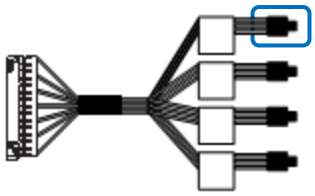


Figure 16: Wiegand input wiring

18	Black / Red	Digital ground		Ground for Wiegand
19	Green / Red	WIEG_IN_D0	In	Wiegand IN D0 (Output type required: Open drain or 5V+/-5%)
20	White / Red	WIEG_IN_D1	In	Wiegand IN D1 (Output type required: Open drain or 5V+/-5%)

If pull-up’s to 12V have been added on D0_IN and D1_IN inputs on a previous installation with a MorphoAccess® 500 Series terminal, these resistors must be removed to avoid any damage to the MorphoAccess® VP MD terminal.

Wiegand output wiring

The following figure shows how to cable the wires of the Wiegand OUT port of the terminal for Wiegand protocol. This is used, for instance, to connect the MorphoAccess® VP MD terminal to an Access Control Panel (ACP).

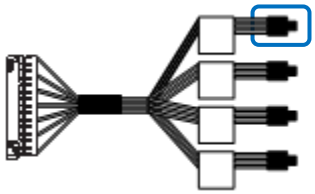


Figure 17: Wiegand output wiring

18	Black / Red	Digital ground		Ground for Wiegand
21	Green	WIEG_OUT_D0	Out	Wiegand OUT D0 (5V TTL)
23	White	WIEG_OUT_D1	Out	Wiegand OUT D1 (5V TTL)
24	Blue	WIEG_OUT_LED1	In	Wiegand LED IN 1 (option) : panel feedback (Output type required: Open drain or 5V+/-5%)
22	Blue / Red	WIEG_OUT_LED2	In	Wiegand LED IN 2 (option) : panel feedback (Output type required: Open drain or 5V+/-5%)

The use of LED IN 1 and LED IN 2 wires is described in the paragraphs below.

The controller supports neither LED1 nor LED2 signals

When the access controller has no relay contact to provide an answer to the MorphoAccess® terminal, then the decision to emit either the “access granted” signal or the “access denied” signal is taken by another way. It is either the MorphoAccess® terminal itself that decide, or it waits for the access controller answer through the local area network (TCP), or on the RS-485 serial port.

It is strongly recommended to disable the LED IN feature, to avoid any interference on MorphoAccess terminal behavior.

The controller supports only LED1 signal

When the access controller has only one relay contact which is dedicated to the “access granted” answer, this one must be connected between the LED1 and GND wires. The LED1 wire is set to the low level by closing the contact between the LED1 and the GND wires, and it means “access granted”.

The MorphoAccess® terminal uses the timeout of the wait for a low level on the on LED1 wire or LED2 wire as “access denied” answer.

To minimize at most the waiting time of the user, the MorphoAccess® VP MD terminal timeout value, must be adjusted to a value a little bit higher than the maximal value of the controller response time.

Warning: if the LED2 wire is connected, it must be constantly maintained in the high state.

The controller supports LED1 and LED2 signals

When the controller supports one relay contact for each of the possible answers then:

- The « access granted » contact must be connected between the LED1 and the GND wires of the terminal
- The « access denied » contact must be connected between the LED2 and the GND wires of the terminal.

The MorphoAccess® terminal considers that:

- The answer of the controller is "access granted", when the controller puts the LED1 wire to the low state (by closing a contact between the LED1 and the GND wires), **and leaves the LED2 wire to the high state.**
- The answer of the controller is "access denied", when the controller puts the LED2 wire to the low state (by closing a contact between the LED2 and the GND wires), **whatever is the state of the LED1 wire.**

The MorphoAccess® terminal also considers that the answer of the controller is "access denied" in case of time-out while expecting for a closure between LED1 and GND wires, or between LED2 and GND wires.

Data Clock Input

The following figure shows how to cable the wires of the "Wiegand In" port of the terminal for Data Clock protocol. This is used, for instance, to connect an external card stripe reader to the MorphoAccess® VP MD terminal.

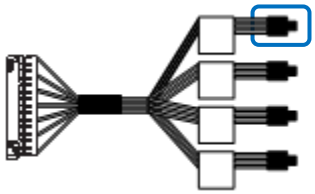


Figure 18: Wiegand port wiring – DataClock

18	Black / Red	Digital ground		Ground for Wiegand
19	Green / Red	D0_IN	In	Data (Output type required: Open drain or 5V+/-5%)
20	White / Red	D1_IN	In	Clock (Output type required: Open drain or 5V+/-5%)

Data Clock Output

The following figure shows how to cable the wires of the Wiegand OUT port of the terminal for Data Clock protocol. This is used, for instance, to connect the MorphoAccess® VP MD terminal to an Access Control Panel (ACP).

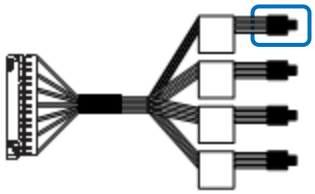


Figure 19: Wiegand port wiring – Data Clock

18	Black / Red	Digital ground		Ground for Wiegand
21	Green	D0_OUT	Out	Data (5V TTL)
23	White	D1_OUT	Out	Clock (5V TTL)

RS-485 port wiring

The following figure shows how to cable the wires of the RS-485 OUT port of the terminal (RS-485 protocol). This is used, for instance, to connect the MorphoAccess® VP MD terminal to an Access Control Panel (ACP).

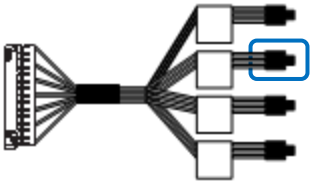


Figure 20: RS-485 port wiring – RS485

15	Blue / Black	RS485_RX+/TX+ (A)	In/Out	RS485 Rx/Tx non inverting signal
13	Blue / White	RS485_RX-/TX- (B)	In/Out	RS485 Rx/Tx inverting signal
17	Black / Red	RS485_GND		Ground

RS485 implementation is limited to half-duplex communication. So only Tx+, Tx- and ground reference signals are necessary.

Depending on the RS485 network, an impedance adaptation may be required.

For farthest terminal, a 120-Ohms resistor termination may be added outside the terminal between Tx+ and Tx-.

GPIO wiring

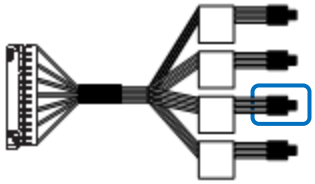


Figure 21: GPIO wiring

12	Black / Red	Digital ground		Ground
9	Orange	Digital Input 0	In	Digital Input (1.8V to 5V)
11	Orange / Red	Digital Input 1	In	Digital Input (1.8V to 5 V)
16	Orange / Black	Digital Input 2	In	Digital Input (1.8V to 5 V)
10	Yellow	Digital Output 0	Out	Digital Output (5V – 5mA max)
8	Yellow / Red	Digital Output 1	Out	Digital Output (5V – 5mA max)
14	Yellow / Black	Digital Output 2	Out	Digital Output (5V – 5mA max)

Single Door Access Control (SDAC) implementation

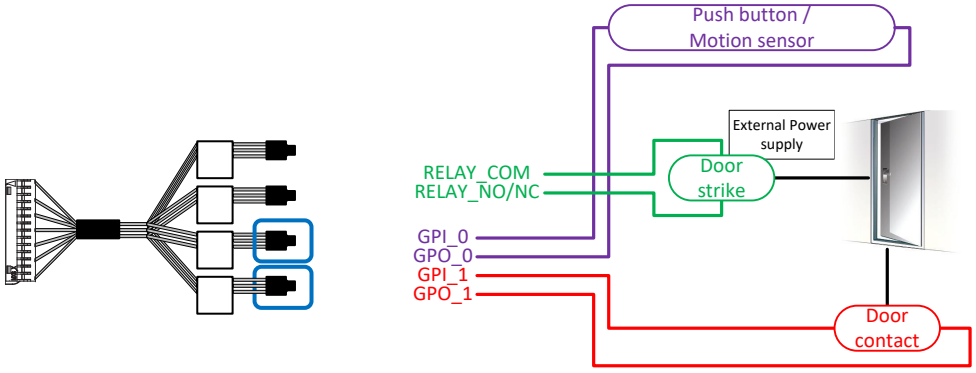


Figure 22: SDAC wiring

If door contact is not used, GPI1 and GPO1 shall be connected together

Ethernet connection

Ethernet interface can be used to power the MorphoAccess® VP MD terminal through POE (Power Over Ethernet - IEEE802.3af or IEEE802.3at type 1 mode). According to the POE standard two modes are available: power on data pins and power on dedicated pins.

Use either one of these modes depending on POE implementation on your local Ethernet network.

Wi-Fi™ dongle must not be used with POE power supply. The POE doesn't provide enough power for both the terminal and the Wi-Fi USB dongle.

Ethernet cable shall be shielded

Default Ethernet configuration

By default, MorphoAccess® VP MD terminal is configured in Static mode

IP address Mode	Parameter	Factory value
Static	Terminal IP address	192.168.1.10
	Gateway IP address	192.168.1.254
	Sub network mask	255.255.254.0
	Host name	MA-VP

Connecting MorphoAccess® VP MD terminal with default Ethernet configuration

Administrator must change the default Ethernet configuration before deploying terminal on site. This can be achieved by several ways as mention below.

- MBTB > Quick Configuration > Communication Configuration > IPv4 Address Settings
- MBTB > USB Script > Set IP configuration
- Webserver > Terminal Settings > Communication > IPv4 Network

Prior to connecting through MBTB or Webserver, please check if terminal is accessible from Host system/PC or not. To access terminal which is having default network parameter, the administrator may need to modify the network parameters of the Host PC.

Please refer to following example to connect terminal which is having default network parameter.

Figure 23: Direct Point to Point Ethernet Connection

1. Connect terminal directly to PC with Point to Point Ethernet connection.
2. Change the Host PC IP address to 192.168.1.11 (or any IP address within 192.168.x.x range excluding 192.168.1.10)
3. Connect terminal with its default IP address i.e. 192.168.1.10 either from MBTB or Webserver.
4. Change the Terminal network parameter from MBTB or Webserver.

NOTE: For connecting terminal directly to a PC (Point to Point connection) by an Ethernet cable, the Ethernet port of the PC must support the Auto-MDIX feature, otherwise a crossover Ethernet cable is mandatory. If no crossover Ethernet cable is available, then a dedicated switch can be used for the connection.

Recommendations for RJ45 wiring

Pin	1	2	3	4	5	6	7	8
Signals	Data pair 1	Data pair 1	Data pair 2	NC/POE pin dedicated (+)	NC/POE pin dedicated (+)	Data pair 2	Ground/ pin dedicated (-)	NC/POE pin dedicated (-)
EIA / TIA T568B Colors	White orange	Orange	White green	Blue	White blue	Green	White brown	Brown
EIA / TIA T568A Colors	White green	White green	White green	White green	White green	White green	White green	White green
Corel L120 Colors	Grey	White	Pink	Orange	Yellow	Blue	Purple	Brown

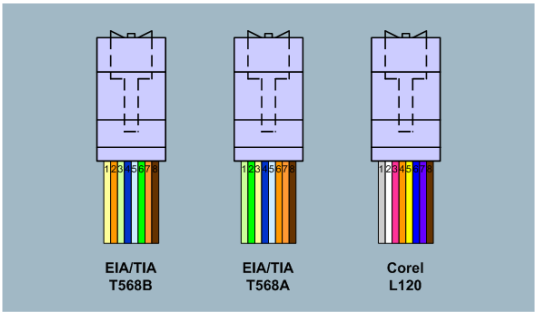


Figure 24: RJ45 wiring

RJ45 plug pinout is compliant with 10/100 base T, IEEE802.3 Specification. Product is compliant also with MDI or MDI-X.

External USB connection

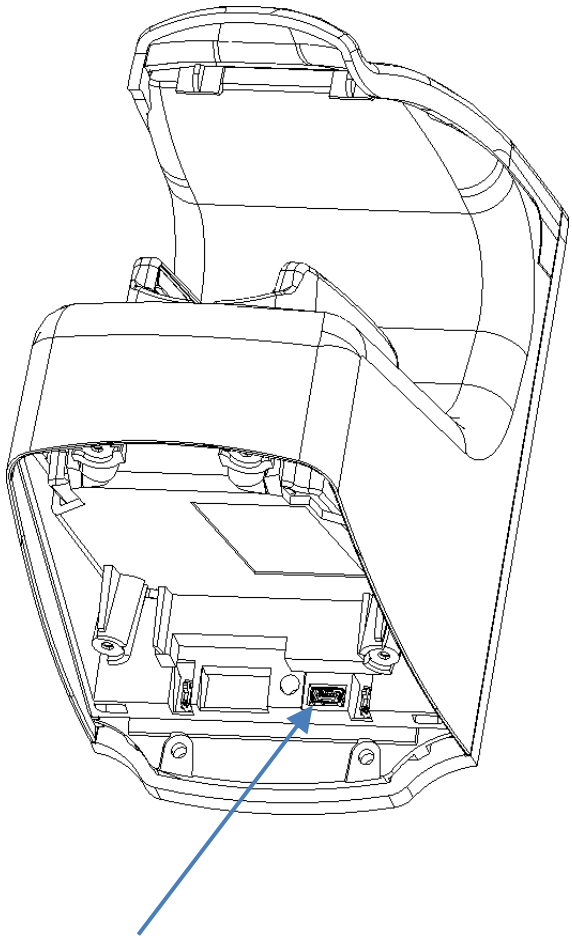


Figure 25: External USB connection

The external Micro USB port can be used to connect a mass storage USB key for administration only. This requires a standard Mini USB-type B / USB-type A female adapter or cable (which can be found in Morpho catalogue with ref 29XXXXXX).

Please report to MorphoAccess® VP MD Administration Guide for more information.

USB connection is limited to USB mass storage key connection (power consumption shall not exceed 200mA)

Wi-Fi™ dongle installation

Wi-Fi™ dongle shall be preferably installed outside the product (separate area shall be reserved in the wall) and connected to the internal USB Mini B (at the rear of the terminal) using Morpho cable provided in the kit.

Wi-Fi™ dongle shall not be exposed to temperature exceeding 50°C (don't forget to count the thermal dissipation of the product and of the Wi-Fi™ dongle).

Wi-Fi™ feature requires the product to be powered from an external DC 12V to 24V power supply (the POE doesn't provides enough power for both the terminal and the Wi-Fi™ dongle)

Only Wi-Fi™ dongle delivered by IDEMIA (kit reference 293686787) may be installed with the terminal for WLAN (Wireless Local Area Network) operation.

Cable has to be plugged on the upward USB connector of the rear panel, as on the following image:

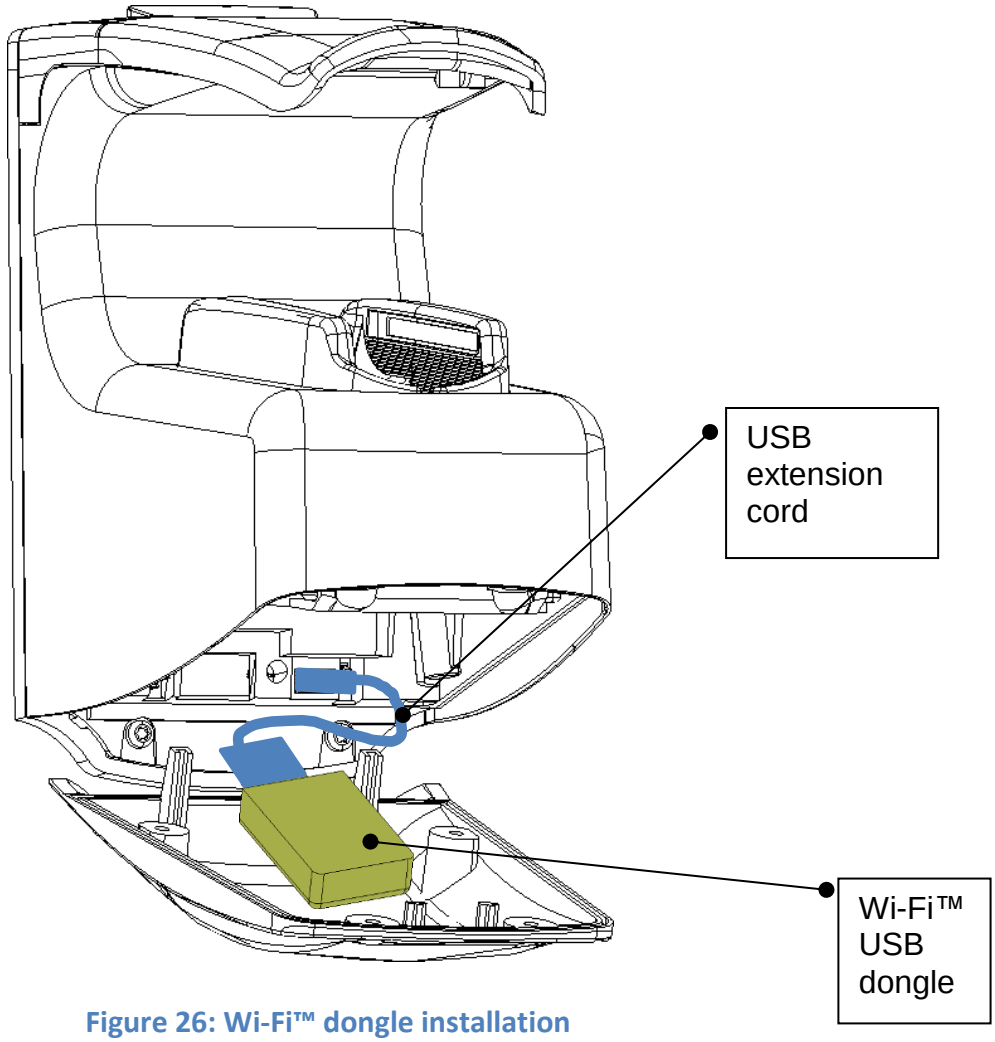


Figure 26: Wi-Fi™ dongle installation

Section 5 : User Interface

Modes for controlling access rights

Introduction

The MorphoAccess® VP MD terminal offers several methods for controlling access rights: it needs to be configured in one of the following four modes:

- Identification mode,
- Authentication mode (requires a contactless smartcard reader in the terminal),
- Multi-factor mode (requires a contactless smartcard reader in the terminal),
- Proxy mode

Refer to MorphoAccess® VP MD Administration Guide for more information on Access Control.

Identification mode

The Identification process of the MorphoAccess® VP MD terminal proceeds by comparison of the biometric data of the finger placed on the biometric sensor, with all the biometric data stored in the database.

It means that the biometric data of the allowed users must be stored in the internal database before they can request the access on the terminal. This biometric data is acquired either directly on the terminal (using the embedded webserver application and the biometric sensor of the terminal), or on an enrolment system using a biometric sensor compatible with the terminal (such as MorphoSmart™ sensors).

The access control by identification process is started when a finger is detected on the biometric sensor

When the user requests the access, his identity is unknown, and it is the terminal that searches for his identity. The terminal grants the access if a match is found (the user is identified); otherwise the access is denied (the user remains unknown).

For further information, please see the "Identification mode" section in the MorphoAccess® VP MD Administration Guide.

Authentication (verification) mode

Unlike the "identification" mode, the user identity must be known in order to execute the authentication process.

Indeed, authentication is an identity verification process: the user provides his identity and the terminal checks it with the relevant process.

This mode doesn’t compare the user’s data to the data of several users: it compares the data provided by the user with the reference data provided by the same user during enrollment phase. The data can be on a card presented to the terminal or in a database and ID is provided by the user.

Access is authorized if the terminal finds a correspondence.

For further information, please see the "Authentication mode" section in the MorphoAccess® VP MD Administration Guide.

Multi-factor mode

In this mode, the "identification" and "authentication" modes are available simultaneously; the user decides which control method will be used:

- by placing his finger on the sensor, thereby triggering the identification process,
- by placing his contactless card on the reader, thereby triggering the authentication process,

This is the default mode for terminals fitted with a contactless smartcard reader.

For further information, please see the "Multi-factors method" section in the MorphoAccess® VP MD Administration Guide.

Proxy mode

The Proxy mode is an operating mode where the access control main application is located in a distant system. This is not a standalone mode like Identification and Authentication modes.

It means that the terminal becomes a slave of the host system application. The access control application is running on the host system and uses MorphoAccess® VP MD terminal high level functions:

- Identification function
- Authentication function
- Read data on a contactless card
- Access control result signal command

The MorphoAccess® VP MD terminal is driven through an Ethernet (or Wi-Fi™) link using TCP, SSL or TLS protocol.

The MorphoAccess® VP MD terminal acts as a server: it is either waiting for a command or executing a command.

The commands allowed by the MorphoAccess® VP MD terminal are described in the MorphoAccess® VP MD Host System Interface Specification document.

For further details about SSL or TLS on the MorphoAccess® VP MD terminal, please refer to the MorphoAccess® VP MD Administration Guide.

External database mode (also called polling mode)

The reference biometric templates of the users are stored in external database, instead of terminal local database or user's RF card.

When authentication is initiated on the terminal, the terminal will poll the user ID to external controller. On polling out the ID, the corresponding template (if exists) is fetched from the external database and is authenticated against user's biometric on the terminal. Once the template request is posted to the external database, the

terminal shall wait for the finger template from the external database to start authentication. Further process shall be same as authentication.

Polling Process using buffer:

- The user's input ID will be queued in the terminal's queue, which is polled by external application.
- External application waits for the User ID by polling the buffer. After getting a user ID, it will search the template in database and send template to terminal for further authentication.
- The user is authenticated by the external device and granted access accordingly.

MorphoAccess® VP MD terminal also has distant commands to retrieve polling buffer status and polling buffer data. Refer to the MorphoAccess® VP MD Host System Interface Specification document.

How to Activate?

External database mode can be activated through Webserver > Complete Configuration, by setting "ucc.enable_external_database" parameter to 1. You can refer to the MorphoAccess® VP MD Host System Interface Specification document to know how to set this parameter.

Configuring the terminal

The following methods can be used to configure the terminal:

- through the Ethernet interface (remote management)
- through a Wi-Fi™ connection (license and dongle required)

Configuration procedures are described inside the MorphoAccess® SIGMA Series Administration Guide as follows:

- Section 4: Terminal Configuration And Administration

These Anti-tamper / anti-pulling switches

Please refer also to “Tamper Switch” section.

These switches are activated as soon as there is enough pressure applied on the terminal against the wall. They are deactivated as soon as this pressure is not big enough, e.g. when the terminal is pulled out of the wall.

When the switches are deactivated, the MorphoAccess® VP MD terminal acts as required by the related configuration key (see MorphoAccess® VP MD Administrator / User Guide for key configuration description):

- Ignore the event (default): useful during normal maintenance operations.
- Send an alarm message to the Central Access Controller, through the usual channel of the access control result messages (Wiegand, DataClock, RS485, Ethernet or Wi-Fi™). An alarm switch (relay contact) is directly available on block terminal «tamper switch pins». Please refer to “Wiring overview” and to “Tamper Switch” sections.
- Generate an audible alarm signal with the buzzer and a visual alarm signal with the status LED.

Section 6 : Accessories, Software Licenses and PC Applications

Compatible Accessories, Licenses and Software

The following items can be ordered directly to IDEMIA or to an official distributor, so as to enjoy all the features of your MorphoAccess® VP MD terminal:

- **Power supply units**,
- **Contactless smartcards**: MIFARE® 1k, 4k; DESFire® 2k, 4k, 8k,
- **MA WI-FI PACK**: containing a Wi-Fi™ USB dongle to activate Wi-Fi™ capability on your terminal,
- **User database size license (MA_10K_USERS)**: enabling database size upgrade from 5000 to 10,000 users capacity (max 3 fingers per record) at creation of the database.

Compatible PC applications

MorphoAccess® VP MD terminals are fully compatible with:

- MorphoManager (version 13.1.9 or higher),
- Morpho Integrator's Kit (MIK) software development kit (version 6 or later),
- MorphoBioToolBox (version 4.1.2 or later).

Section 7 : Recommendations

Global warning

The manufacturer cannot be held responsible in case of non-compliance with the following recommendations or incorrect use of the terminal.

General precautions

- Do not attempt to repair your terminal yourself. The manufacturer cannot be held responsible for any damage/accident that may result from attempts to repair components. Any work carried out by non-authorized personnel will invalidate your warranty.
- Do not expose your terminal to extreme temperatures.
- Use your terminal with original accessories. Attempts to integrate unapproved accessories to the terminal will void your warranty.
- Due to electrostatic discharge, and depending on the environment, synthetic carpet should be avoided in areas where the terminal has been installed.

Areas containing combustibles

It is strongly recommended that you do not install your terminal in the vicinity of gas stations, petroleum processing facilities or any other facility containing flammable or combustible gasses or materials.

Specific precautions for terminals equipped with a contactless smartcard reader

It is recommended to install terminals equipped with a contactless smartcard reader at a certain distance (> 30cm) from metallic elements such as iron fixations or lift gates or radio product (such as contactless smartcard reader). Performances in terms of contactless badge reading distance will decrease when metallic elements are closer.

Ethernet connection

It is recommended to use a category 6 shielding cable (120 Ohms). It is also strongly recommended to insert a repeater unit every 90m.

Extreme care must be taken while connecting Ethernet wire to the terminal block board since low quality connection may strongly impact Ethernet signal sensibility.

It is recommended to connect Rx+ and Rx- with the same twisted-pair wire (and to do the same with Tx+/Tx- and the other twisted-pair wire).

Date / Time synchronization

The terminal clock has a +/-10 ppm typical time deviation at +25°C (roughly around +/-6 sec per 48 hours). At lower and higher temperature (but within normal operating

temperatures), deviation may be more important (worst case: - 14 seconds per 48 hours).

If the terminal is used in an application requiring high time precision, we recommend synchronizing regularly your terminal time with an external clock (using NTP). Every 24 hours is usually enough for most applications.

Please note that the date/time of the terminal is protected from power failure during at least 24 hours. If the duration of the power failure or power down is longer, the date/time of the terminal will be lost.

Cleaning precautions

The use of a dry cloth is recommended to clean the terminal, especially the biometric sensor. Acid liquids, alcohol or abrasive materials are prohibited.

Annex 1 : Finger Placement Recommendations

Main principles

Acquisition needs to be done with extreme care, in order to:

- get the best image quality
- increase recognition performance
- reduce recognition time

Then, it is highly recommended to:

- Maximize the contact between the fingerprint and the sensor
- Exert firm, but not excessive, finger pressure on the surface of the sensor
- Do not press too hard
- Do not slide nor roll the finger across the sensor
- Do not move the finger during acquisition
- Wait for the extinction of sensor backlight before removing the finger

Most useful areas for biometric data

Areas with the most useful biometric data are different according to the type of biometric data:

- **Fingerprint**: the most useful zone is around the centre of the first phalanx of the finger.
- **Vein network**: the useful zone is between the first and third phalanx of the finger.

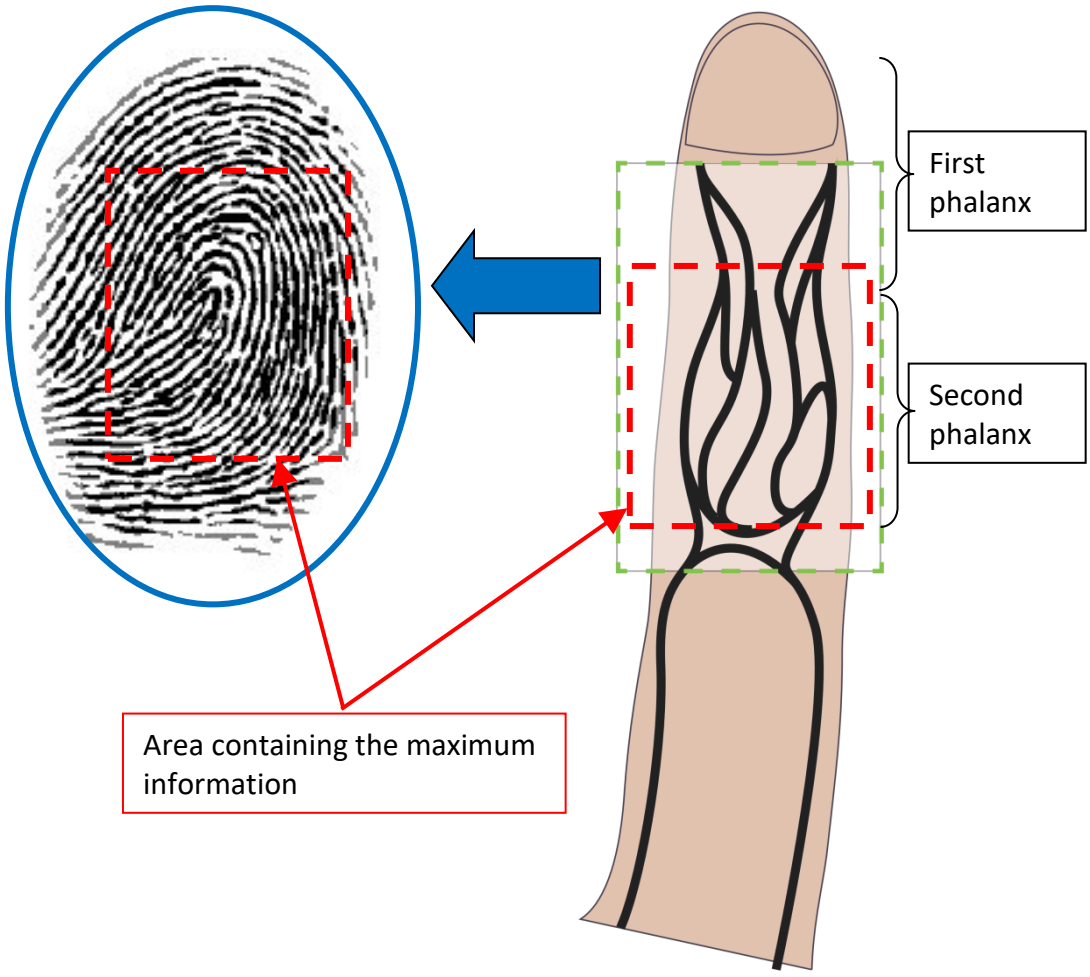


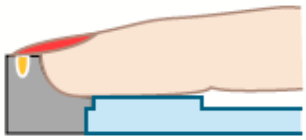
Figure 27: Most useful areas for biometric data

The sensor is designed so that when the fingertip is in contact with the rounded hollow guide:

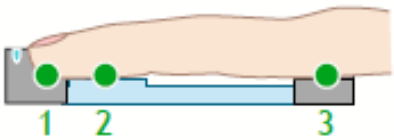
- the central zone of the first phalanx is aligned with that of the section dedicated to the fingerprint capture,
- the second phalanx is positioned inside the section dedicated to capturing the finger vein network.

Position of finger

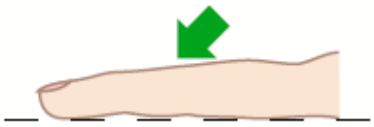
Correct position



- Place the fingertip in contact with the rounded hollow guide (1).
- In case of long nail, pass it over the fingertip guide so that the fingertip is correctly in contact with the hollow guide (1) and not the tip of the nail.



- Keep the fingertip in contact with the rounded hollow guide (1).
- Make sure that the fingerprint is properly in contact with the transparent optical surface (2).
- Place the base of the finger in the position guide on the other side (3).
- Let rest the palm of the hand on the shell of the terminal.



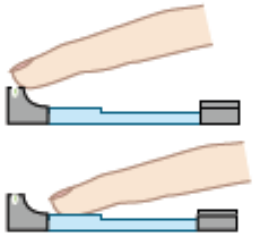
- Keep the finger straight.

Figure 28: Recommended finger positions

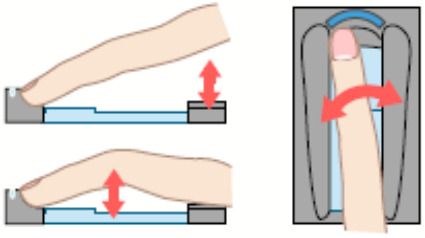
To guarantee good acquisition quality, please leave the finger on the biometric sensor until the backlighting switches off.

Bad finger position

The following figures show incorrect finger positions.



- Do not place the fingertip on the top of the fingertip guide.
- Do not place the fingertip on the surface of the sensor: it must be in contact with the rounded hollow guide.



- Do not leave the finger in the air.
- Do not bend the finger.
- Do not tilt the finger: it must be parallel with the sensor's walls.

- Do not roll the finger.
- Do not bend the finger upwards.
- Do not bend the finger downwards.

Figure 29: Incorrect finger positions

Troubleshooting

Please follow these recommendations to improve acquisition quality:

- wipe the finger if it is too wet,
- warm the finger if cold or dry,
- lightly moisten the finger if dry,
- clean the finger if dirty,
- remove any band aids and adhesive tape if they are obstructing the fingerprint or second phalanx of the finger,
- do not press down too hard and do not contract the finger to avoid constricting blood vessels.

Annex 2 : Bibliography

How to get the latest versions of documents

The last version of the documents can be downloaded from our web site at the address below:

www.biometric-terminals.com

(Login and password required to allow access to the private part).

To request a login, please contact your sales representative.

Documents concerning the MorphoAccess® terminal

Bibliography

MorphoAccess® 5G Series Bibliography,

Ref. 2016_2000022505 - MorphoAccess® 5G Series Bibliography

This document gives document's references for MorphoAccess® 5G Series terminals. This document is in English.

Annex 3 : Support

Troubleshooting

The terminal IP address is unknown or it is not possible to connect to the terminal

Load a valid set of network parameters in your terminal.

The sensor is switched off

Check that the database contains at least one record.

Check that the identification mode is enabled.

The terminal returns erratic responses to Ping commands

Check the subnet mask.

Ask the network administrator for the correct value.

Check that each device connected to the network has a different IP address.

Technical Support and Hotline

North America

Mail: support.bioterminals@idemia.com

Tel: +1 888 940 7477

South America

Mail: support.bioterminals@idemia.com

Tel: +1 714 575 2973

South Africa

Mail: support.bioterminals@idemia.com

Tel: + 27 11 286 5855

India:

Mail: support.bioterminals@idemia.com

Tel: 0120-4699900

Europe and rest of the world:

Mail: support.bioterminals@idemia.com

Tel: +33 1 30 20 30 40

(9H00am to 5H30pm French Time, Monday to Friday)

Web site

For the latest firmware, software, document releases, and news, please check our websites :

- **North and South America** : e-mailing support.bioterminals@idemia.com with your name, phone number, MorphoAccess serial number and “Send Links For MorphoAccess® VP MD Documents” in the subject line
- **Other countries** : please visit our web site www.biometric-terminals.com (To get your log in and password please contact your sales representative).

Head office:

IDEMIA

2, place Samuel de Champlain

92400 Courbevoie – France

www.idemia.com