



Sagem Sécurité
SAFRAN Group

MorphoAccess™ 500 Series

User Guide

Preliminary

Produced by SAGEM Sécurité

Copyright ©2007 SAGEM Sécurité

www.sagem-securite.com

MorphoAccess™ 500 Series User Guide

July 2007

SK-60806

Table of content

| | |
|--|-----------------------------|
| INTRODUCTION | 552 |
| CAUTION | 662 |
| MORPHOACCESS™ PRESENTATION | 882 |
| INTERFACES PRESENTATION | 992 |
| SYSTEM SYNOPTIC | 1112 |
| TERMINAL PRESENTATION | 1312 |
| ACCESS CONTROL PRESENTATION | 1512 |
| SENDING THE ID TO THE CENTRAL SECURITY CONTROLLER | 1912 |
| TERMINAL CONFIGURATION | 2122 |
| EASY SETUP ASSISTANT | 2222 |
| ADMINISTRATION MENU | 2622 |
| UNDERSTANDING MORPHOACCESS™ CONFIGURATION | 2922 |
| MODIFYING A PARAMETER USING THE CONFIGURATION APPLICATION | 3132 |
| CONFIGURING A NETWORKED MORPHOACCESS™ | 3432 |
| UPGRADING THE FIRMWARE | 3632 |
| DOWNLOADING A LICENCE | 3732 |
| STAND ALONE MODES (NETWORKED OR NOT CONNECTED) | 4142 |
| PRELIMINARY: ADDING A BIOMETRIC TEMPLATE IN LOCAL DATABASE | 4242 |
| MACCESS APPLICATION: ACCESS CONTROL OR TIME & ATTENDANCE | 4342 |
| ACCESS CONTROL BY IDENTIFICATION | 4542 |
| ACCESS CONTROL BY IDENTIFICATION (MA-XTENDED LICENCE LOADED) | 4742 |
| INTRODUCTION TO CONTACTLESS AUTHENTICATION | 5052 |
| AUTHENTICATION WITH BIOMETRIC TEMPLATES ON CARD | 5252 |
| PIN VERIFICATION – PIN STORED ON CARD | 5352 |
| BIOPIN VERIFICATION - BIOPIN STORED ON CARD | 5452 |
| AUTHENTICATION WITH BIOMETRIC TEMPLATES IN LOCAL DATABASE | 5552 |
| AUTHENTICATION BASED ON CARD MODE | 5752 |
| MULTI-FACTOR MODE | 5952 |
| AUTHENTICATION WITH LOCAL DATABASE: ID ENTERED FROM KEYBOARD | 6062 |
| AUTHENTICATION WITH LOCAL DATABASE: ID INPUT FROM WIEGAND OR DATACLOCK | 6262 |
| BYPASSING THE BIOMETRIC CONTROL IN AUTHENTICATION | 6562 |
| RECOGNITION MODE SYNTHESIS | 6762 |
| SETTING UP RECOGNITION STRATEGY | 6862 |
| SETTING UP MATCHING PARAMETERS | 6962 |

PROXY MODE [72722](#)

PROXY MODE (OR SLAVE) PRESENTATION [73732](#)
PROXY MODE ACTIVATION [74742](#)

APPLICATION CUSTOMIZATION [75752](#)

SETTING UP TIME MASK [76762](#)
MULTILINGUAL APPLICATION [77772](#)

RESULT EXPORTATION [78782](#)

REMOTE MESSAGES: SENDING THE ID TO THE CENTRAL SECURITY CONTROLLER [79792](#)
RELAY ACTIVATION [80802](#)
LOG FILE [81812](#)
LED IN ACTIVATION [82822](#)

SECURITY FEATURES [83832](#)

TAMPER SWITCH MANAGEMENT [84842](#)
PASSWORDS [86862](#)

ANNEX [87872](#)

MORPHOACCESS™ 220 320 COMPATIBILITY [88882](#)
CONTACTLESS MODES TABLE [90902](#)
REQUIRED TAGS ON CONTACTLESS CARD [91912](#)
FAQ [92922](#)
RELATED DOCUMENTS [93932](#)

INTRODUCTION

Congratulations for choosing the SAGEM MorphoAccess™ 500 Automatic Fingerprint Recognition Terminal.

MorphoAccess™ 500 Series provides an innovative and effective solution for access control applications using Fingerprint Verification or/ and Identification.

Among a range of alternative biometric techniques, the use of finger imaging has significant advantages: each finger constitutes an unalterable physical signature, which develops before birth and is preserved until death. Unlike DNA, a finger image is unique to each individual - even identical twins.

The MorphoAccess™ terminal integrates SAGEM image processing and feature matching algorithms. This technology is based acquired knowledge during 20 years of experience in the field of biometric identification and the creation of literally millions of individual fingerprint identification records.

We believe you will find the SAGEM MorphoAccess™ fast, accurate, easy to use and suitable for physical access control or time and attendance.

To ensure the most effective use of your SAGEM MorphoAccess™, we recommend that you read this User Guide entirely.

CAUTION

Europe information:

SAGEM hereby declares that the SAGEM MorphoAccess™ has been tested and found compliant with the following listed standards as required by the EMC Directive 89/336/EEC: EN55022 (1994) / EN55024 (1998), EN300-330 (1999) and by the low voltage Directive 73/23/EEC amended by 93/68/EEC: EN60950 (2000).

Caution: The MA500 terminal is a Class A device. In a residential environment, this device may cause interference. In this case, the user is encouraged to try to correct the interference with appropriated measures such as :

- 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.

USA information:

NOTE: FCC part 15 certificates are pending.

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: Sagem Morpho Inc, 1145 Broadway Plaza, Suite 200, Tacoma, Washington (USA), 98402, (800) 346-2674.

Note: This equipment has been tested and found to comply with the limits for a Class B (MA520, MA521, OMA520, OMA521) or Class A (MA500) 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 or more 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.

Canadian information:

NOTE : Industrial Canadian certificates are pending.

This Class B (MA520, MA521, OMA520, OMA521) or Class A (MA500) digital apparatus complies with Canadian ICES-003.

Ces appareils numériques de Classe B (MA520, MA521, OMA520, OMA521) ou Classe A (MA500) sont conformes à la norme NMB-003 du Canada.

MORPHOACCESS™ PRESENTATION

MorphoAccess™ is a fingerprint identification device for physical access control, time and attendance offering both multi-factor verification and identification capabilities with unequaled level of performance.

INTERFACES PRESENTATION

Man-machine interface

The MorphoAccess™ 500 offers a simple and ergonomic man-machine interface dedicated to access control based on fingerprint recognition:

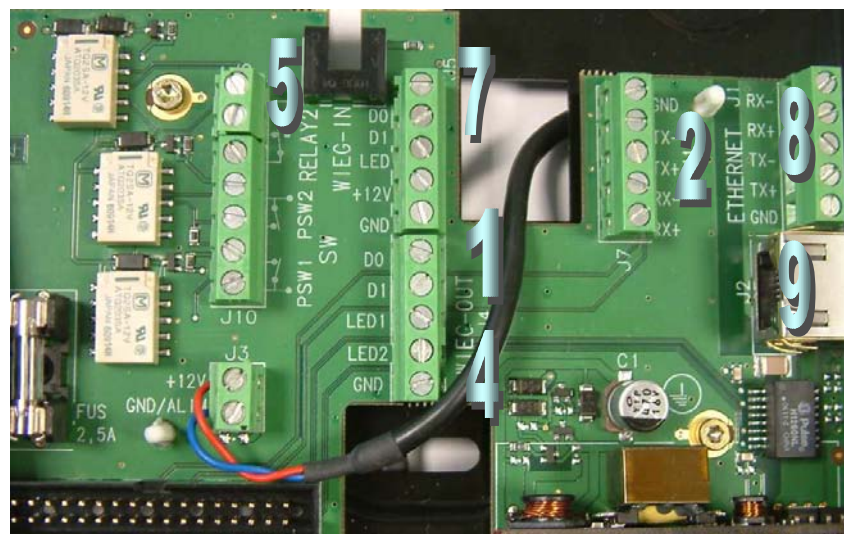
- A high quality optical scanner to capture fingerprints (1),
- A multicolor led (2),
- A multi-toned buzzer,
- A Mifare™ contactless reader on 520 families terminal to read reference templates from a contactless card (3),
- A keyboard for time and attendance purpose, configuration and PIN code (4),
- A 128x64 display (5).



Electrical interfaces

The terminal offers multiple interfaces dedicated to administration and control information:

- A multiplexed Wiegand / DataClock output to export user identifier to a controller (1),
- A RS422 or RS485 output (2),
- A LED signal output (3),
- Two LED IN inputs to improve integration in an Central Security Controller (4),
- A relay to directly command an access (door lock) (5),
- A tamper switch to detect that the back cover has been removed (6),
- A multiplexed Wiegand / DataClock input to receive user identifier from an external badge reader (7),
- An Ethernet interface (LAN 10/100 Mbps) allowing remote management through TCP (8),
- A Power Over Ethernet Interface (LAN 10/100 Mbps) allowing remote management and supplying power through TCP (9).



The *MA500 Series Installation Guide* describes precisely each interface and connection procedure.

SYSTEM SYNOPTIC

Typical architecture including a MorphoAccess™, a Host System and a Central Security Controller



MorphoAccess™ biometric database management

The management of the MorphoAccess™ internal biometric database can be done either locally (through the terminal Man Machine Interface), or remotely by a Host System (typically MEMS™). These two exclusive management modes are defined as the:

- Local management mode
- Remote management mode

MorphoAccess™ operating mode

The MorphoAccess™ works according two exclusive operating modes.

- In *Stand Alone Mode* (terminal networked or not connected) the terminal can operate two applications: *Access Control* or *Time & Attendance*. When the terminal is networked the biometric database can be managed by a Host System and downloaded to the MorphoAccess™. When the terminal is not networked the database is managed locally.

- Unlike the *Stand Alone Mode* in *Proxy Mode* the terminal is remotely operated by a host application that sends individual commands to the MorphoAccess™.



MorphoAccess™ result sending



When the biometric identification is positive, the person ID can be sent to a Central Security Controller, for further action such as opening doors.

MorphoAccess™ keyboard short cut

The keyboard short cuts are:

Key  and  activates LLT mode

Key  and  increases the screen contrast

Key  and  reduces the screen contrast

Key  and  reboots the terminal.

TERMINAL PRESENTATION

A MorphoAccess™ 500 is running with 4 applications dedicated to a given need.

MACCESS

This is the main application, dedicated to biometric control.

It is possible to leave this application to launch other application.

The current *User Guide* details the application features.

ENROLMENT

This application allows enrolling users in the terminal when MorphoAccess™ is not connected to an external network (Local management mode).

The created database can be saved ciphered on a USB key and exported to other stand alone MorphoAccess™.

The *User Management Password* protects this application.

Please refer to *Enrolment Application User Guide* for more information about this application.

CONFIGURATION

This application allows modifying the main application parameters.

Parameters are divided into files, sections and keys.

The *Terminal Configuration Password* protects this application.

Please refer to *Configuration Application User Guide* for more information about this application.

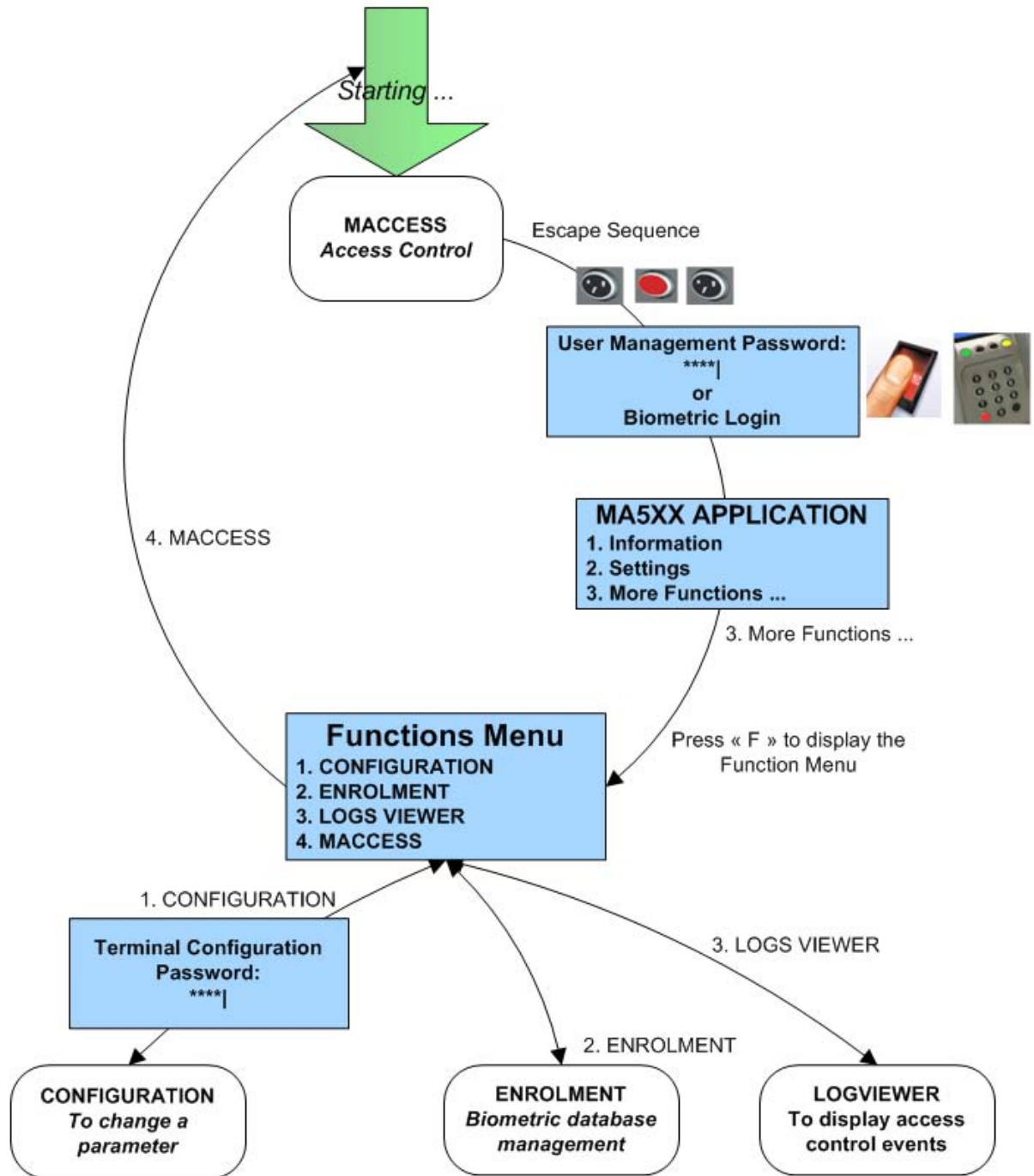
LOGS VIEWER

This application allows consulting the local event diary stored by the MorphoAccess™.

The *User Management Password* protects this application.

Please refer to *Logs Viewer Application User Guide* for more information about this application.

Multi-applicative architecture synthesis



ACCESS CONTROL PRESENTATION

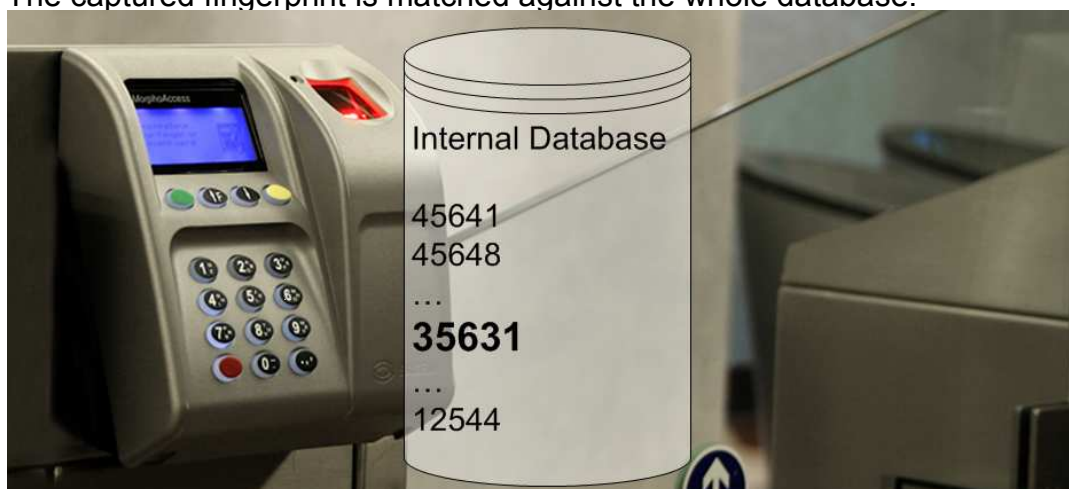
The MorphoAccess™ works according two biometric recognition modes: identification or authentication. Identification and authentication can be activated at the same time (multi-factor mode).

Identification (1 vs. N)

The captured fingerprint is matched against a database – 1 vs. N.

Biometric templates are stored in terminal local database. Depending on the installed licence, the terminal can store 3000 users (2 fingers per user) in its local database or 50 000 users divided in 5 bases of 10000 users each.

In this mode the sensor will be always switched on, waiting for a finger. The captured fingerprint is matched against the whole database.

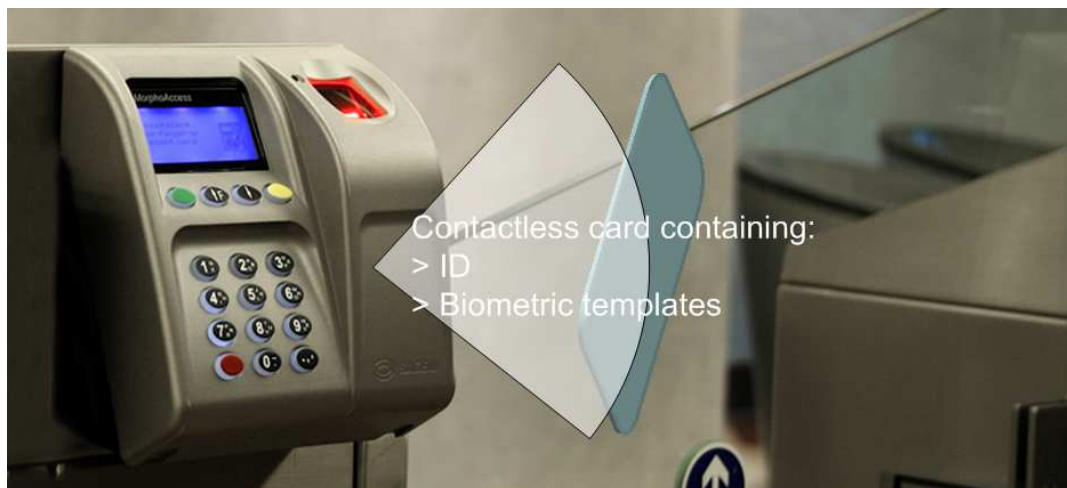


If the user is not recognized a no-match message is sent to the Central Security Controller.

See section [Access Control By Identification](#).

Authentication with reference templates in card (1 vs. 1)

The captured fingerprint is matched against a reference template – 1 vs. 1.
User biometric templates are stored on a contactless card.



If the user is matched the ID is returned to the Central Security Controller.

If the user is not recognized a no-match message is sent to the Central Security Controller.

See section [Access Control By Authentication](#).

Authentication with reference templates in terminal (1 vs. 1)

The captured fingerprint is matched against a reference template – 1 vs. 1.

User minutiae are stored into the local database. In this case the user identifier is used as a key to find the minutiae. The user identifier can be sent through Wiegand, DataClock, typed on keyboard or stored on a contactless card.

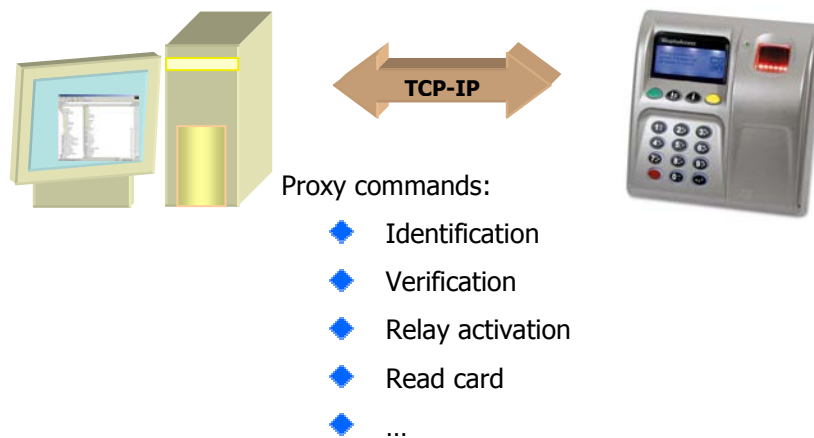
Multi-Factor recognition

It is possible to combine multifactor such as, what I have (a contactless smart card), what I know (PIN code), and what I am (biometric templates).

Proxy mode

Proxy Mode is not strictly speaking a recognition mode. In this mode, the MorphoAccess™ works as a slave waiting for external commands such as:

- Identification,
- Verification,
- Relay activation,
- Read data on a contactless card,
- ...



Chapter [Proxy mode](#) gives more information about remote management.

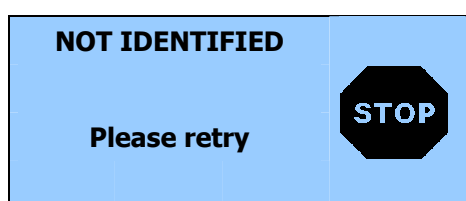
Please refer to *MorphoAccess™ Host System Interface Specification* for a complete description of command.

SENDING THE ID TO THE CENTRAL SECURITY CONTROLLER

If the user has been recognized, the terminal may trigger the access or returns the corresponding ID to the Central Security Controller.



If the user has *not* been recognized, the terminal can return the failure to Central Security Controller.



Various messages or interfaces can be activated to send or store the control result.

Relay

After a successful control the MorphoAccess™ relay may be activated during a given period.

Wiegand Id Emission

The ID of the recognized user can be sent through the Wiegand output. The format of the frame may be defined.

DataClock Id Emission

The ID of the recognized user can be sent through the DataClock output.

Ethernet Id Emission

The ID of the recognized user can be sent through the Ethernet link. The administrator may set the port and defined the protocol.

RS485/422

Control information can be sent through RS485/422 link.

Local Diary (log)

A local file will store logs.

This diary can be downloaded by the Host System or consulted on the terminal.

TERMINAL CONFIGURATION

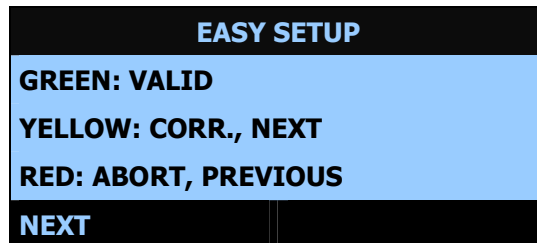
This chapter details how to configure the MorphoAccess™. A parameter can be changed directly on the terminal or remotely through a network.


A “first start assistant” named “Easy Setup” helps the administrator to define quickly a configuration “plug’n play” with an existing physical Access Control System.


EASY SETUP ASSISTANT


Assistant initialization

When the MorphoAccess™ starts for the first time an “assistant” helps the administrator to configure easily the main functions.



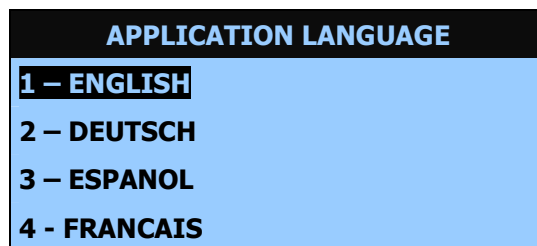
Key  validates the choice.

Key  goes to next step.

Key  returns to previous step.

Language selection

It is possible to choose the language of the application among installed languages.




Date and time configuration

Date and time can be configured.

Date format is **MM/DD/YYYY**.

Key  deletes a character.

Key  validates the selection.



Network settings

Static or dynamic configuration

It is possible to choose between static or dynamic network configurations.

| DHCP | |
|--------------------|----------------------------------|
| 1 – Enable | <input checked="" type="radio"/> |
| 2 – Disable | <input type="radio"/> |

DHCP disabled

If DHCP is disabled following parameters must be set:

- IP address,
- Network mask,
- Default gateway.

| ENTER IP ADDRESS | |
|------------------|--|
| 10.10.161.3_ | |
| VALID | |

DHCP enabled

With DHCP only the terminal hostname on the network is required.

| ENTER HOSTNAME | |
|----------------|--|
| MA0789652_ | |
| VALID | |

Recognition mode

Once IP parameters are defined next step is to define the recognition mode.

| RECOGNITION MODE | |
|---------------------------|----------------------------------|
| 1 – Identification | <input checked="" type="radio"/> |
| 2 – Contactless | <input type="radio"/> |
| 3 – MultiFactor | <input type="radio"/> |

MorphoAccess™ 500 can only be configured in identification mode (other modes could be configured later).

MorphoAccess™ 520 can be configured in identification mode, contactless authentication or multi-factor mode (identification and contactless authentication modes are merged).

Output interface

Last step allows defining the interface required to export the control result.

| INTERFACE PARAMETERS | |
|----------------------|---------|
| 1 – Wiegand | [OFF] |
| 2 – DataClock | [OFF] |
| 3 – ID on UDP | [OFF] |
| 4 – Next | |

Each interface can be configured and activated independently.

Select **4 – Next** to go to next step.

Wiegand configuration

Three protocols are available 26, 32 and 34 bits.

For other Wiegand configurations, please refer to chapter [Authentication: ID input from Wiegand](#).

| WIEGAND | |
|-------------|-------|
| 1 – 26 bits | [•] |
| 2 – 34 bits | [] |
| 3 – 32 bits | [] |
| 4 – OFF | [] |

DataClock configuration

DataClock interface can be activated – but is multiplexed with Wiegand output.

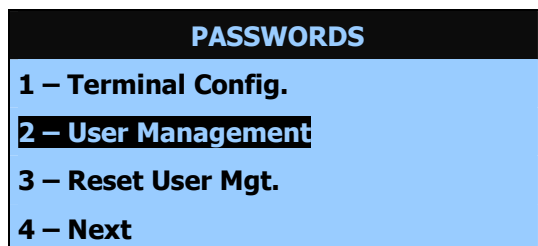
UDP activation

UDP remote messages can also be activated. The server IP address must be specified.

| SERVER IP ADDRESS | |
|-------------------|--|
| 10.10.161.7_ | |
| VALID | |

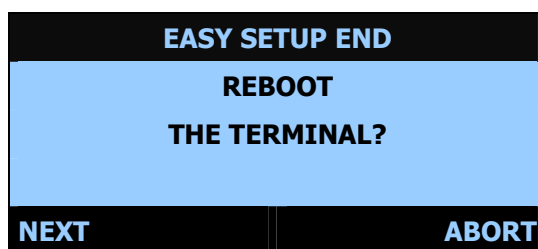
Password configuration

Last step consists in changing the passwords.



Select **4 – Next** to leave the assistant.

The terminal must reboot to apply the changes.



Press **NEXT** to reboot the terminal.

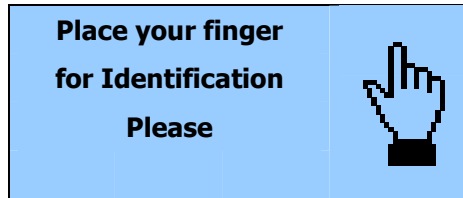
Press **ABORT** to return to password management.

Restarting “Easy Setup”

MorphoAccess™ “Easy Setup” can be restarted using the End Menu.

ADMINISTRATION MENU

Access to Administration Menu

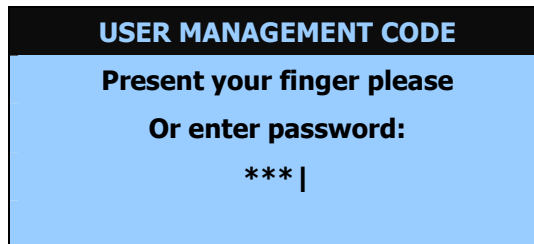


The main application can be interrupted using the escape sequence. Hit the following keys in sequence:

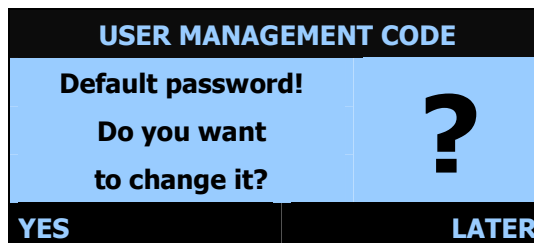



If the biometric database is not empty, the terminal accepts a finger registered as administrator instead of the valid *User Management Password Code*.

By default *User Management Password* is "12345".



If the Administrator uses the default password it is possible to change it immediately.



 For security, we strongly recommend you to change the terminal default password.

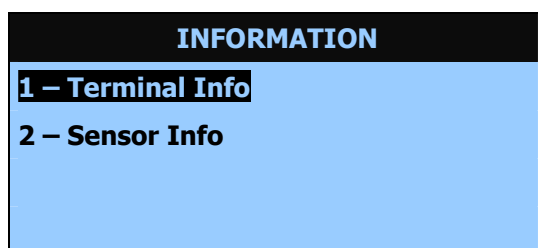
Administration Menu features



Information Menu



Select **Information** to access to terminal and sensor information:



Terminal information

Select **Terminal Info** to access to the following information:

| Terminal information | Description | Example |
|----------------------|--|-------------------|
| 1 – Type | Terminal type | 520 |
| 2 – Serial Number | Terminal serial number | 053535353A |
| 3 – Soft. Version | Terminal main software version (MACCESS) | V01.20.04 |
| 4 – IP Address | Terminal IP address | 134.1.32.214 |
| 5 – MAC Address | Terminal MAC address | 00:60:4C:69:53:53 |

Sensor information

Select **Sensor Info** to access to the following information:

| Sensor information | Description | Example |
|--------------------|--|---|
| 1 – Product Info | MSO Biometric product information (type, licence, serial number, ID) | MSO300 MSO_MA_IDENTLITE OEM SN: 0709F151008 OEM ID: 25194664 |
| 2 – Sensor Info | Sensor information (flash size, serial number, ID) | Flash: 4096 Ko SN: 0710A010026 ID: 25115841-4 |
| 3 – Soft. Info | Sensor software version | MSO V08.01.d-C |

UNDERSTANDING MORPHOACCESS™ CONFIGURATION

Presentation

MorphoAccess™ parameters are stored into files organized in sections and values.

For example a file named “app.cfg” contains all the parameters defining the main application settings.

```
[bio ctrl]
identification=1
nb attempts=2
...
[log file]
enabled=1
...
```

Configuration organization

The application creates several files:

- app.cfg,
- adm.cfg,
- bio.cfg,
- net.cfg,
- fac.cfg,

The *app.cfg* file contains the application settings, *adm.cfg* contains administration parameters, *bio.cfg* the biometric sensor settings, *net.cfg* Ethernet parameters, *fac.cfg* the factory parameters.

Two files are reserved by the system to store factory settings and network parameters:

- fac.cfg,
- net.cfg.

Modifying a parameter

There are two ways to modify a parameter:

- Directly on the terminal using the *Configuration Application*,
- Remotely through Ethernet or Serial link with a client application running on the Host System.

Notation

In this manual a parameter is presented using this formality:

| "Short parameter description" | |
|-------------------------------|-------|
| <i>file/section/parameter</i> | Value |

For example to activate recognition mode based on identification this key must be set to 1:

| Access control by identification | |
|------------------------------------|---|
| <i>app/bio ctrl/identification</i> | 1 |

MODIFYING A PARAMETER USING THE CONFIGURATION APPLICATION

The *Configuration Application* allows changing a parameter directly on the terminal.


You must exit a possible running application to display the *application selection* menu.

If the main application is running, it must be quit using the escape sequence:



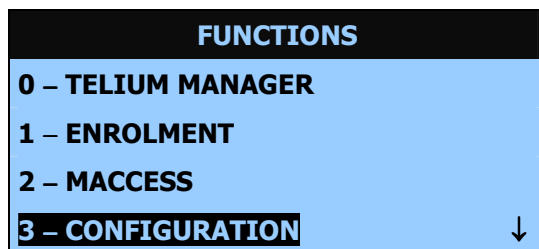
Then enter the *Terminal Configuration Password* to access to the *Administration Menu*.

Select “Quit” to exit the *Access Control* application.

Press  to display the functions menu.


Select **3 – CONFIGURATION** to launch the *Configuration Application*.

The *Configuration Application* is fully detailed in the *Configuration Application User Guide*. This chapter only offers a brief description.




Keys role

Keys  and  change the current selection.

Key  deletes a character or goes to previous screen.

Key  confirms the change.

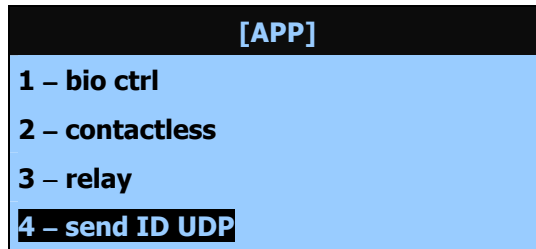
Key  quits the application.

Changing a parameter

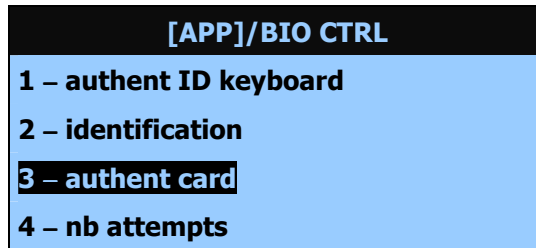
A main menu allows selecting the file to modify.



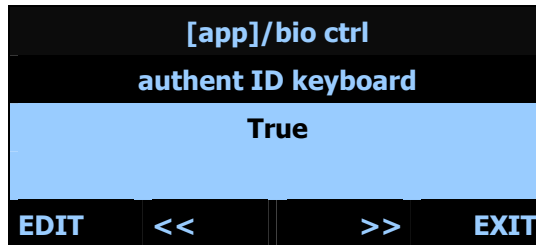
When a file has been selected it is possible to choose a section.



The parameter list contains all parameters available in a section.



It is possible to display parameter one by one in a given section.



The edition menu will depend on the parameter type.

Binary choice

| [app]/bio ctrl | |
|----------------------------|------------|
| authent ID keyboard | |
| True | [•] |
| False | [] |

IP address

| [app]/send ID udp | | | |
|--------------------------|-----------|------------|-------------|
| host address | | | |
| 134. | .1 | .32 | .214 |

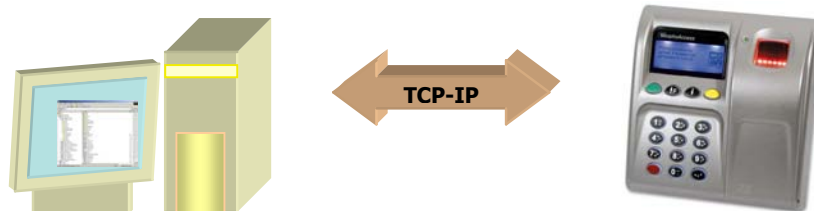
CONFIGURING A NETWORKED MORPHOACCESS™

Introduction

A PC (running with MEMS™ for example) connected to a MorphoAccess™ can manage the terminal. Available remote operations are:

- Biometric template addition,
- Control settings modification,
- Configuration reading,
- Local database deletion,
- Record deletion,
- Control diary downloading,
- Firmware upgrade.

The PC acts as a client for the MorphoAccess™.



Remote management:

- ◆ Change mode
- ◆ Add template
- ◆ Get configuration
- ◆ ...

The MorphoAccess™ works as a server waiting for request from a client.

The client will send biometric templates to the terminal and manage the local database.

Please refer to *MorphoAccess™ Host System Interface Specification* for a complete description of TCP administration. This document explains how to create a database and store biometric records in this base.

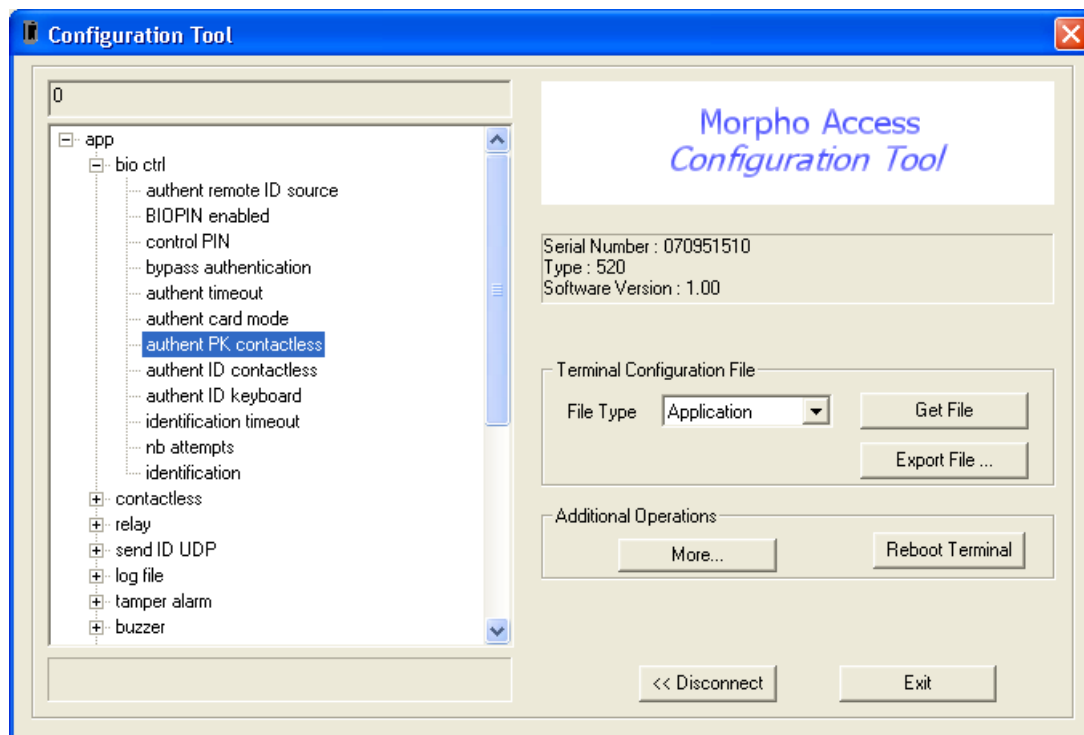
Network factory settings

By default the terminal IP address is 134.1.32.214. This address can be changed through Ethernet or with the *Configuration Application*.

The default server port is 11010.

Modifying a key using “configuration tool”

Configuration Tool allows changing parameters. This program is an illustration of utilization of the TCP API. Please refer to *Configuration Tool User Guide* for more information about this program.



UPGRADING THE FIRMWARE

It is possible to upgrade your MorphoAccess™ firmware through Ethernet. Two package types are available. One dedicated to terminal system, another one dedicated to biometric library.

Use the *Downloader* to upgrade your terminal system.

Use the *BioLoader* to upgrade your terminal biometric library.

Please refer to the *MA500 Series Upgrade Tools User Guide* for more information about upgrade procedures.

DOWNLOADING A LICENCE

By default the MorphoAccess™ can match a fingerprint against 3000 users database. This database configuration corresponds to a basic licence (*MSO_MA_IDENTLITE*).

MA-Xtended licence (*MSO_MA_IDENTPLUS*) allows to extend MorphoAccess™ recognition capabilities to 5 databases of 10 000 users (2 fingers per user).

Checking the licence installed in the MorphoAccess™

To display the licence installed in the MorphoAccess™, display the [Administration Menu](#), select “Information”, “Sensor Info” then “Product Info”.

| PRODUCT INFO | |
|---|--|
| MSO 300 MSO_MA_IDENTPLUS OEM SN: 0725F152306 OEM ID: 251946640 | |
| VALID | |

Available licences

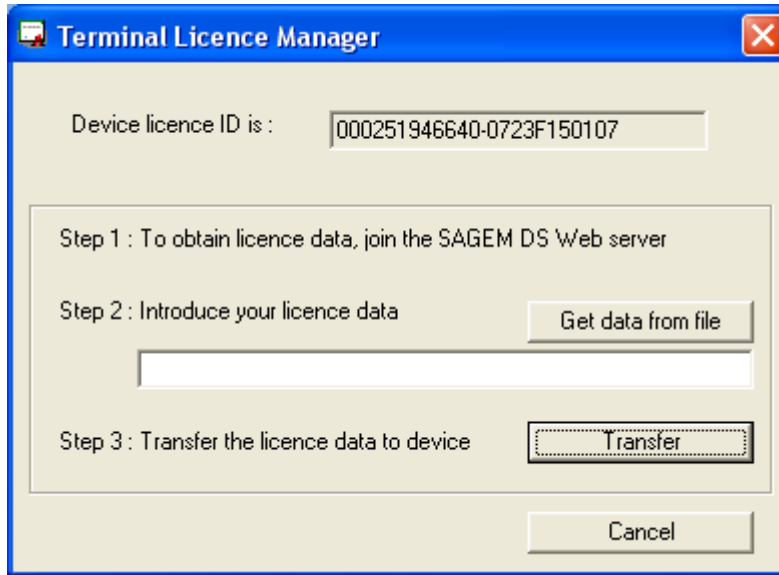
| Licence | |
|--|----------------------------------|
| Default (<i>MSO_MA_IDENTLITE</i>) | 1 database of 3000 users |
| MA-Xtended (<i>MSO_MA_IDENTPLUS</i>) | 5 databases of 10 000 users |
| (UNKNOWN LICENCE) | <i>contact the SAGEM support</i> |

MSO_MA_IDENTPLUS licence can be loaded in the MorphoAccess™.

Upgrade to MA-Xtended licence (1/2): obtaining device serial number

The MorphoAccess™ 500 must be connected to a LAN.

Launch the Terminal Licence Manager tool, connect to the MorphoAccess™ and retrieve the terminal *device serial number*.



Device serial number has the following format “*OEM ID-OEM SN*”.

Copy this string to the “clipboard”.

Upgrade to MA-Xtended licence (2/2): downloading a MA-Xtended licence
 Connect to our customer support web site: <https://www.sagem-ds.com/biometrics-customersupport>.



In the *licence generator* section enter your customer login and password.
Xtended licence corresponds to *MSO_MA_IDENTPLUS* licence.
 Select this licence and copy the *device serial number*.

You ~~will receive~~ ~~obtain~~ your *licence number* by email:-

You have to introduce the licence data send by the web server in the dialog box (Step 2). You can use the *Get data from file* button to copy the data from a file.

If you received the licence by the Hotline then introduce it in the dialog box formatted *MSO MA IDENTPLUS licence*

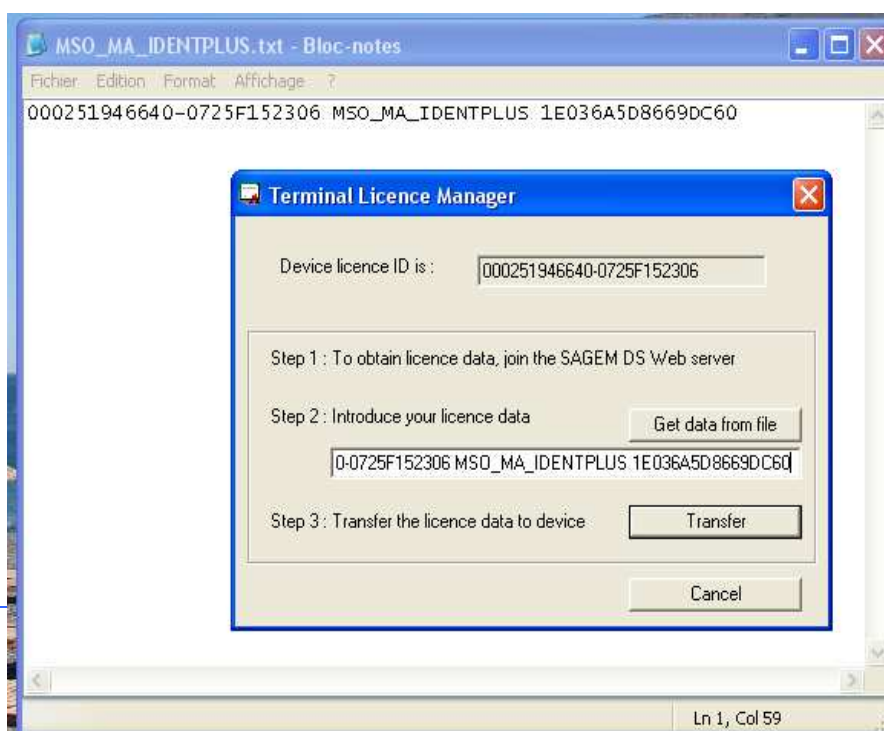
Then, use the *Transfer* button to really process the loading of the device (Step 3).

At any time, you can stop the procedure by using the *Cancel* button

~~Copy the complete string in *Licence Manager* tool.~~

~~If you receive your licence by email, select *Get data from file*.~~

~~Load the licence in the *MorphoAccess*.~~



The software confirms the operation with the following dialog box (the license is now loaded in your MorphoAccess™ device)



or signals a problem with a dialog box.

The display of the base number '00' ~~display~~ on the MorphoAccess™ screen means the license "MSO_MA_IDENTPLUS" has been correctly set.

STAND ALONE MODES (NETWORKED OR NOT CONNECTED)

The MorphoAccess™ works according two biometric recognition modes: identification or authentication. Identification and authentication can be activated at the same time (multi-factor mode).

In Stand Alone Mode the terminal can operate two applications: Access Control or Time & Attendance.

PRELIMINARY: ADDING A BIOMETRIC TEMPLATE IN LOCAL DATABASE

The management of the MorphoAccess™ internal biometric database can be done either locally (through the terminal Man Machine Interface), or remotely by a Host System. These two exclusive management modes are defined as the:

- Local management mode
- Remote management mode

Local enrolment



The local database can be exported ciphered to other MA5xx devices using a USB key.

The *Enrolment Application* is dedicated to this function.

Please refer to *Enrolment Application User Guide* for a complete description of local enrolment facilities.

Remote management

The user is enrolled on an Enrolment Station (typically a station with MEMS™) and biometrics templates are exported to the MorphoAccess™ via Ethernet network or USB key.



This architecture allows managing many MorphoAccess™ databases from one PC client station.

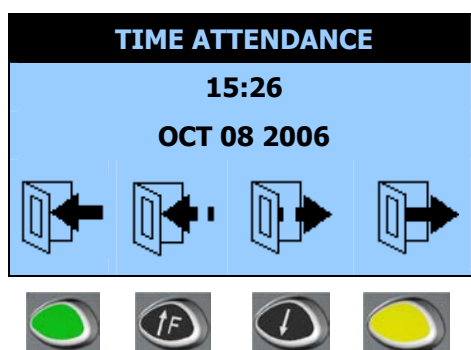
MACCESS APPLICATION: ACCESS CONTROL OR TIME & ATTENDANCE

MorphoAccess™ application can be configured to work in physical access control mode or in time and attendance mode. In this configuration, MorphoAccess™ events logged can be enriched with some attendance information (entry, exit...).

When the time attendance feature is activated the main screen may display 2 or 4 functions.

Four functions mode:

| | |
|--------------------------------------|---|
| Time Attendance (4 functions) | |
| <i>app/modes/time and attendance</i> | 2 |




Two functions mode:

| | |
|--------------------------------------|---|
| Time Attendance (2 functions) | |
| <i>app/modes/time and attendance</i> | 1 |




When entering, the user has to press key  to log his entry time.

When exiting, the user has to press key  to log his exit time.

For particular uses such as temporary absences, two additional functions corresponding to function keys 2 and 3 can be displayed.

After selection, the MorphoAccess™ switches in biometric mode (identification or authentication).

The selected function is written in the log file and sent to the host.

If the user has selected the wrong operation (IN/OUT...), key  can be pressed at any moment during biometric invitation to abort the verification. In this case, nothing is logged or sent to the controller.

After 10 seconds of inactivity on identification mode (no finger detected on the sensor), the terminal switches back to the selection screen. In this case the operation result is logged and/or sent to the controller (time-out).

To disable *Time Attendance* mode set *app/modes/time and attendance* to 0.

Note about terminal clock deviation

The terminal clock has a +/- 4 sec per day typical time deviation at +25°C. At 50°C, the time deviation may be up to -8 sec per day.

For application requiring time precision, MorphoAccess™ clock must be synchronised regularly with an external clock.

ACCESS CONTROL BY IDENTIFICATION

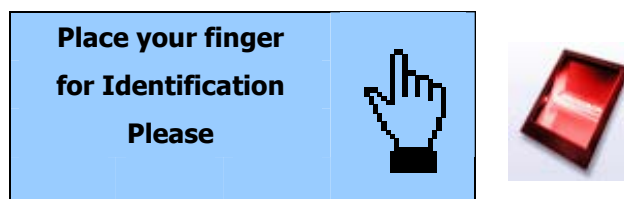
Access control by identification

app/bio ctrl/identification

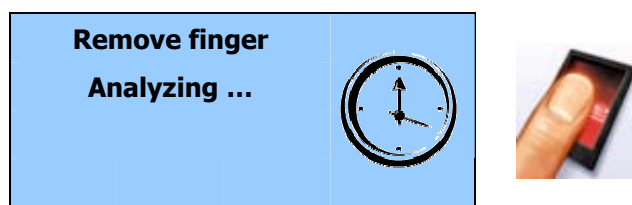
1

To configure MorphoAccess™ terminal in this mode, set the parameter *app/bio ctrl/identification* to 1.

After starting the MorphoAccess™ terminal waits for fingerprint detection in identification mode. The sensor is lighted on.



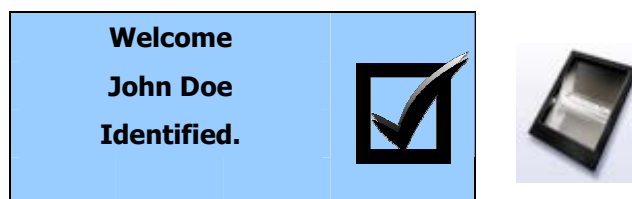
The user can present a finger to launch identification process.



If the identification is successful, the terminal triggers the access or returns the corresponding ID to central security controller.

The ID can be sent through various interfaces. Please refer to *MorphoAccess™ Remote Messages Specification* for a complete description of "hit" and "no hit" messages.

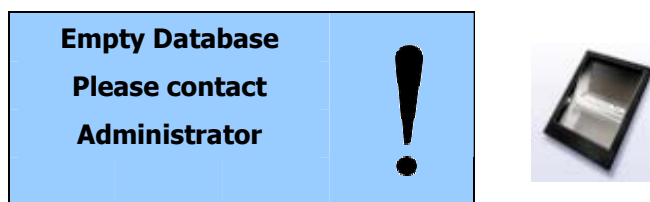
Result is displayed on terminal screen.



Once the user identification is done, the terminal automatically loops back and waits for a new finger.

At least one user (biometric template) must be stored in the local database. In this configuration up to 3000 users with 2 biometric templates each can be stored.

If the terminal is running in identification mode with an empty database, the sensor is off and the following screen is displayed.



Disabling identification

Set *app/bio ctrl/identification* to 0 to disable identification (Proxy Mode).

ACCESS CONTROL BY IDENTIFICATION (MA-XTENDED LICENCE LOADED)

It is possible to increase MorphoAccess™ 500 biometric database size thanks to a licence (*MA-Xtended licence*): the MorphoAccess™ then manages 5 bases of 10 000 users.

Access control by identification with MA-Xtended licence

app/bio ctrl/identification

1

To configure MorphoAccess™ terminal in this mode, set the parameter *app/bio ctrl/identification* to 1 and verify that *MA-Xtended licence* has been loaded.

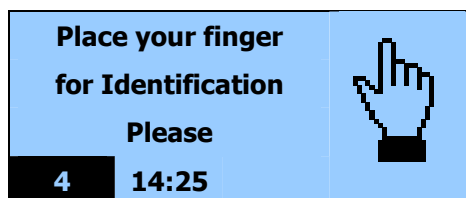
Please refer to chapter [Downloading a licence](#) to know how to upgrade the MorphoAccess™ with MA-Xtended licence.

After starting the MorphoAccess™ terminal waits for fingerprint detection in identification mode. The sensor is lighted on.

If an MA-Xtended licence is loaded it is possible to choose the active database.

To select a user database, just press a key number to toggle the database number. By default, databases 0 to 4 can be selected and used.

Database 0 is the default database.



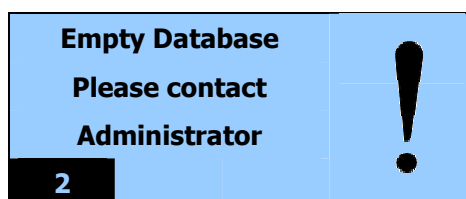
The user can present a finger to launch identification process.

If the identification is successful, the terminal triggers the access or returns the corresponding ID to Central Security Controller.

Once the user identification is done, the terminal automatically loops back to database 0 and waits for a new finger.

At least one fingerprint must be stored in the local database.

If the selected database is empty or does not exist, the sensor is off and the following screen is displayed.



Set *app/bio ctrl/identification* to 0 to disable identification (Proxy Mode).

Database numeration




MA-Xtended licence extends biometric database capacity from 1 base of 3000 users to 5 bases of 10000 users. In this configuration the user must select his database number (from 0 to 4) before presenting a finger to launch identification process.

For user convenience MorphoAccess™ 300 series it is also possible to activate a “16 databases mode”. In this mode the user selects a database number between 0 and 15, and presents a finger to launch identification process. Database selection

The base identification is a two digit number, with a leading zero when required. The default selected base is the base with the identification is “00”.

Pressing a decimal key changes the base to use by modifying the current identification number: the higher digit is replaced by the unit digit and the unit number is replaced by the entered digit. It means that is the “x” key is pressed while the selected base number is “yz”, then the new selected base will be “zx”, if it exists.

Valid base numbers are from 00 to 15, then if the selected base number is higher than “15”, then the number of the default base (00) is automatically forced.

Key  allows to select a database from 10 to 15. For To select database 13 press  then , just press a key number to toggle the database number. By default, databases 0 to 4 can be selected and used.

Access control by identification with MA-Xtended licence

app/bio ctrl/identification

1

From the terminal point of there is still 5 biometric databases.

| MorphoAccess™ 300 series Or MorphoAccess™ 500 series | MorphoAccess™ 500 series (<i>MA-Xtended licence</i>) |
|--|---|
| Database | |
| 0,1,2 | 0 |
| 3,4,5 | 1 |
| 6,7,8 | 2 |
| 9,10,11 | 3 |
| 12,13,14,15 | 4 |

MEMS™ will automatically associates the user to the right base. For example a user stored into database 4 on a MorphoAccess™ 300 will be stored into database 1 on a MorphoAccess™ 500.

INTRODUCTION TO CONTACTLESS AUTHENTICATION

Various recognition modes can be applied depending on the templates location (card or terminal database) and the required security level.

This mode supposes that the user swipes a Mifare™ card containing some structured data (**identifier**, **biometric templates**, **PIN code**)...

Data are localized on the card by a block (“B” parameter) and are protected by a key (defined by “C” parameter). The “C” parameter defines which key is used during the authentication with the card.

For a complete description of card structure and access mode, please refer to *MorphoAccess™ Contactless Card Specification*.

| | |
|--------------------------|---------|
| First bloc to read | |
| <i>app/contactless/B</i> | 1-215 |
| Key number to present | |
| <i>app/contactless/C</i> | 1, 2, 3 |

Following recognition modes are available:

Authentication with biometric templates on card:

Captured fingerprints are matched against templates *read on the card (PK)*. **Identifier** and **biometric templates** must be stored on the card.

In this mode it is also possible to check a **PIN** code before the authentication and to replace the biometric authentication by a **BIOPIN** code check. The BIOPIN code is used when user’s biometric templates are not available (a visitor for example).

Authentication with biometric templates on local database:

Captured fingerprints are matched against templates *read from the local database*. Only the **identifier** is required on the card.

Authentication based on “tag” card mode:

Depending on the **card mode** either templates are read on the card or the control can be bypassed (visitor mode). The **card mode** tag must be stored on the card.

It is possible to check **PIN** code before the authentication and to replace the biometric authentication by a **BIOPIN** check.

It is also possible to skip the biometric control: in this case the terminal acts as a contactless card reader.

Contactless authentication can be combined with a local identification (multi-factor mode).

AUTHENTICATION WITH BIOMETRIC TEMPLATES ON CARD

Authentication with biometric templates on contactless card

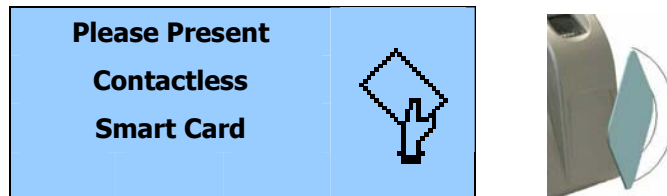
app/bio ctrl/authent PK contactless

1

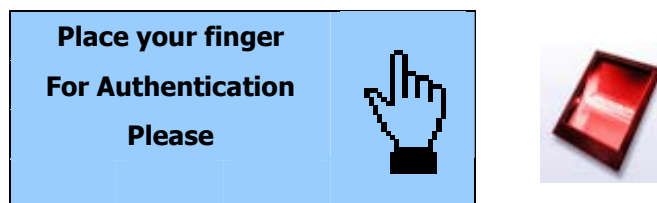
MorphoAccess™ 520 can work in *contactless authentication mode*: the user presents its card, the terminal reads the reference biometric templates on the card and launches a biometric control based on the read templates.

In this case the card will contain the user identifier and biometric templates: no local database is required.

To trigger authentication, user should present his card to the terminal.



If card contains user templates, user is invited to present his finger for biometric authentication.



If the authentication is successful, the terminal triggers the access or returns the corresponding ID to central security controller.

Once the user authentication is finished, the terminal automatically loops back and waits for a new card presentation.

Required tags on card

| ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|----|-----------|-----|-----|-----|--------|
|----|-----------|-----|-----|-----|--------|

Contactless authentication Yes No Yes Yes No No

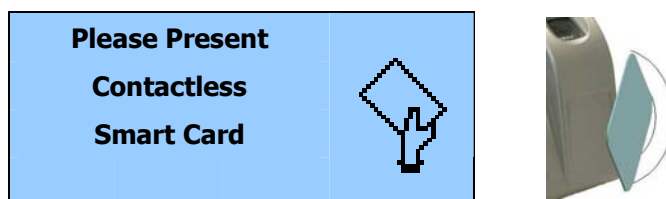
Card structure is described in *MorphoAccess™ Contactless Card Specification*.

PIN VERIFICATION – PIN STORED ON CARD

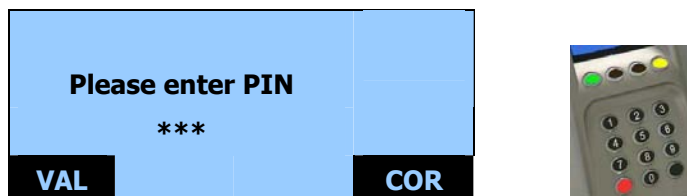
If a reference PIN code is stored on the card it is possible to check this code before controlling the fingerprints.

| | |
|---------------------------------|---|
| PIN code verification | |
| <i>app/bio ctrl/control PIN</i> | 1 |

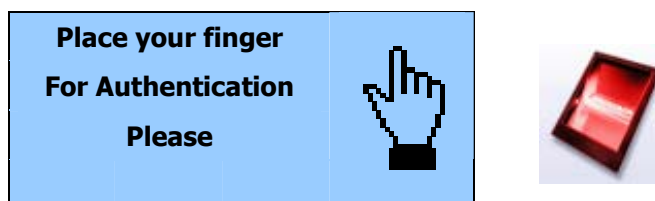
To trigger authentication, user should present his card to the terminal.



If card contains a PIN code, user is invited to enter his PIN code.



If the PIN code is correct, user is invited to presents his finger for biometric authentication.



If the authentication is successful, the terminal triggers the access or returns the corresponding ID to central security controller.

It is also possible to activate this mode independently of biometric authentication. In this case, only the PIN code is checked.

Required tags on card

| | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|-------------------------|-----|-----------|-----|-----|-----|--------|
| PIN code verification | Yes | No | No | No | Yes | No |
| PIN then authentication | Yes | No | Yes | Yes | Yes | No |

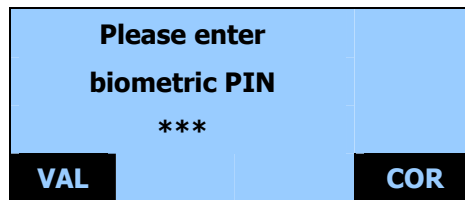
BIOPIN VERIFICATION - BIOPIN STORED ON CARD

In this mode the card should contain a BIOPIN code. The goal of this code is to replace fingerprints authentication by BIOPIN code verification.

| | |
|------------------------------------|---|
| BIOPIN code verification | |
| <i>app/bio ctrl/control BIOPIN</i> | 1 |

To trigger the BIOPIN code verification, user should present his card to the terminal.

If card contains user BIOPIN, user is invited to enter it.



If the BIOPIN is correct, the terminal triggers the access or returns the user ID to the central security controller.

BIOPIN control replaces fingerprint authentication.

This mode can be combined with a preliminary PIN code verification.

It is also possible to activate the fingerprint control (configuration key *"authent PK contactless"* set to 1): in this case the terminal will control fingerprint if templates are stored on the card or BIOPIN if only a BIOPIN is stored on the card.

Required tags on card

| | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|--------------------------|-----|-----------|-----|-----|-----|--------|
| BIOPIN code verification | Yes | No | No | No | No | Yes |

AUTHENTICATION WITH BIOMETRIC TEMPLATES IN LOCAL DATABASE

In this mode only the ID is read on the card. If the ID exists in the biometric database, the MorphoAccess™ performs an authentication using the biometric templates associated to this ID.

The ID can be stored into a TLV structure (typically a card encoded by MEMS™) or directly read at a given offset of the card (binary ID).

ASCII ID, structured data

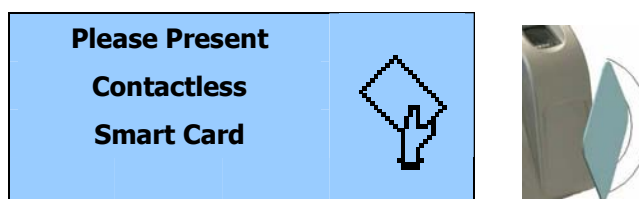
| Contactless authentication with templates on local database | |
|---|---|
| <i>app/bio ctrl/authent ID contactless</i> | 1 |

The identifier must be stored into a TLV structure.

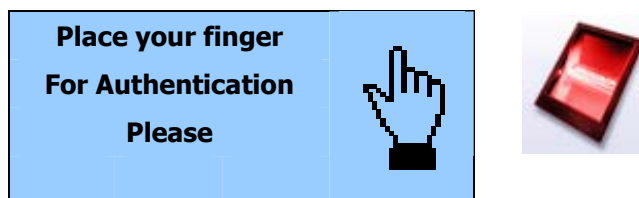
| ASCII identifier in tagged structure. | |
|---------------------------------------|---|
| <i>app/contactless/data format</i> | 0 |
| <i>app/contactless/data length</i> | 0 |
| <i>app/contactless/data offset</i> | 0 |

The user identifier is used as an index in the local database of the MorphoAccess™: reference biometric templates are stored in the local database.

To trigger authentication, user should present his card to the terminal.



If the corresponding ID exists in the terminal database, user is invited to place his finger for biometric authentication.



If the authentication is successful, the terminal triggers the access or returns the corresponding ID to Central Security Controller.

Once the user authentication is done, the terminal automatically loops back and waits for a new card presentation.

Required tags on card

| | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|------------------------|-----|-----------|-----|-----|-----|--------|
| authent ID contactless | Yes | No | No | No | No | No |

Note: a database must exist in the terminal.

Binary identifier, non-structured data

| Contactless authentication with templates on local database | |
|---|---|
| <i>app/bio ctrl/authent ID contactless</i> | 1 |

In this mode the identifier is read at a given offset on the card and is supposed to be binary. No TLV structure is required on the card.

This mode is useful for using the card serial number as an identifier.

| ASCII identifier in tagged structure. | |
|---------------------------------------|-------------------------------------|
| <i>app/contactless/data format</i> | 1 |
| <i>app/contactless/data length</i> | [1-8]: ID size in bytes |
| <i>app/contactless/data offset</i> | [0-15]: ID offset in the read block |

The user identifier is used as an index in the local database of the MorphoAccess™: in this case reference biometric templates are stored in the local database.

Authentication progress is exactly the same as presented above.

Example – 4 bytes identifier.

The terminal is configured to read 4 bytes.

Read bytes are F4 E1 65 34.

Corresponding user identifier in the local database is “4108412212” (ASCII).

Example – reading Mifare card Serial Number (little endian format).

app/contactless/data format = 1

app/contactless/data length = 4

app/contactless/data offset = 0

AUTHENTICATION BASED ON CARD MODE

Contactless authentication with card mode

app/bio ctrl/authent card mode 1

In this mode the card decides on the control progress.

The CARD MODE tag is required. This tag can take several values:

- **PKS** [0x02]: user identifier, template 1 and template 2 are required on the card. Biometric authentication is triggered with biometric templates. If a BIOPIN is present instead of templates, BIOPIN is controlled.
- **ID_ONLY** [0x01]: only the user identifier is required. There is **no biometric** control, the control is immediately positive. This feature is useful for visitor requiring an access without enrolment. But it is still possible to store templates on the card.
- **PIN_CODE** [0x10]: only PIN code is controlled.
- **PIN_THEN_PKS** [0x12]: PIN code is controlled then templates or BIOPIN.

To enable this mode set *app/bio ctrl/authent card mode* to 1.

To disable this mode set *app/bio ctrl/authent card mode* to 0.

Required tags on card if CARD MODE tag value is PKS.

| | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|----------------------------------|-----|-----------|-----|-----|-----|--------|
| authent card mode (PKS) | Yes | Yes | Yes | Yes | No | No |
| authent card mode (PKS) (BIOPIN) | Yes | Yes | No | No | No | Yes |

Required tags on card if CARD MODE tag value is ID_ONLY.

| | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|-----------------------------|-----|-----------|-----|-----|-----|--------|
| authent card mode (ID_ONLY) | Yes | Yes | No | No | No | No |

Required tags on card if CARD MODE tag value is PIN_CODE.

| | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|------------------------------|-----|-----------|-----|-----|-----|--------|
| authent card mode (PIN_CODE) | Yes | Yes | No | No | Yes | No |

Required tags on card if CARD MODE tag value is PIN_THEN_PKS.

| | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|---|-----|-----------|-----|-----|-----|--------|
| authent card mode (PIN_THEN_PKS) | Yes | Yes | Yes | Yes | Yes | No |
| authent card mode (PIN_THEN_PKS) (BIOPIN) | Yes | Yes | No | No | Yes | Yes |

Card structure is described in *MorphoAccess™ Contactless Card Specification*.

Note about “bypass” option combined with “card mode”

When the *bypass authentication* configuration key is activated (see [Bypassing the biometric control in authentication](#)), the global control is bypassed and “card mode” is ignored.

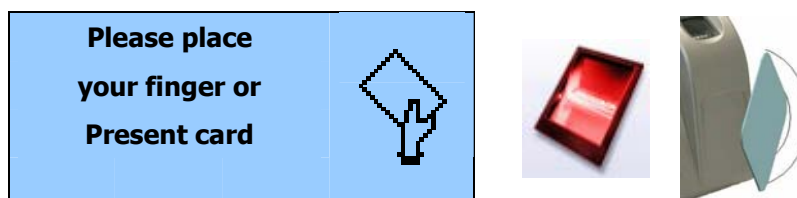
MULTI-FACTOR MODE

This mode is the fusion of identification mode and contactless authentication without database mode.

This mode allows:

- Performing an identification when user places his finger (operation identical to identification mode).
- Performing a contactless authentication when user swipes his contactless card (operation identical to contactless authentication without database mode).

To trigger authentication, user should present his card to the terminal or place his finger on the sensor.



If the authentication or the identification is successful, the terminal triggers the access or returns the corresponding ID to central security controller.

If there is no database contactless card presentation is still possible.

Enabling one contactless mode and identification activate this mode.

| Merged mode | |
|--|--------|
| <i>app/bio ctrl/identification</i> | 1 |
| <i>And</i> | |
| <i>app/bio ctrl/authent PK contactless</i> | 0 or 1 |
| <i>app/bio ctrl/authent card mode</i> | 0 or 1 |
| <i>app/bio ctrl/control BIOPIN</i> | 0 or 1 |
| <i>app/bio ctrl/control PIN</i> | 0 or 1 |

Required tags on card

Required tag on card depends on the authentication mode, but at least an ID is necessary.

| | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|-----------------------|-----|-----------|-----|-----|-----|--------|
| bypass authentication | Yes | No | No | No | No | No |

AUTHENTICATION WITH LOCAL DATABASE: ID ENTERED FROM KEYBOARD

Biometric authentication with ID entered from keyboard

app/bio ctrl/authent ID keyboard

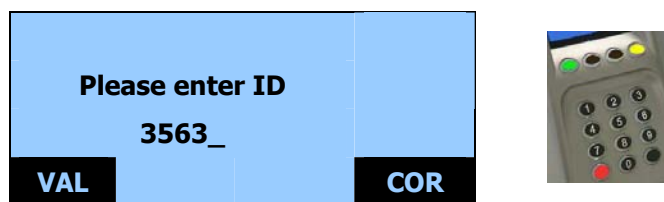
1

In this mode the ID of the user is entered on the MorphoAccess™ keyboard. If the ID exists in the database (or in one of the five databases), the MorphoAccess™ performs an authentication using the biometric templates associated to this ID.

ID is entered using the keypad and the authentication starts



The default screen invites the user to enter his numerical identifier.

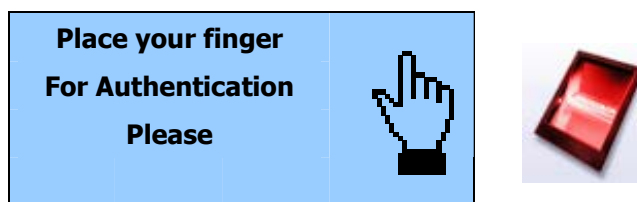


Note: ID length is limited to 24 characters.

Key deletes one character.

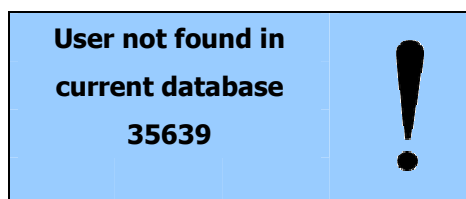
Once the ID is entered, the user confirms with green key .

If the corresponding ID exists in the terminal database, user is invited to place his finger for biometric authentication.



If the authentication is successful, the terminal triggers the access or returns the corresponding ID to Central Security Controller.

If the identifier is not present in the local database authentication is not launched.



Once the user identification is done, the MorphoAccess™ automatically loops back and waits for a new ID.

Remark about MorphoAccess™ with MA-Xtended licence loaded

A MorphoAccess™ with MA-Xtended licence loaded will scan the five biometric database to find the biometric templates associated to the ID.

Note about “bypass” option

When the *bypass authentication* configuration key is activated (see [Bypassing the biometric control in authentication](#)), the MorphoAccess™ verifies that the ID is present on the local database before granting the access.

AUTHENTICATION WITH LOCAL DATABASE: ID INPUT FROM WIEGAND OR DATALOCK

Biometric authentication: ID input from Wiegand or DataClock

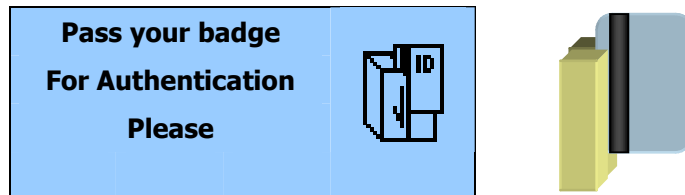
app/bio ctrl/authent remote ID source

1 for Wiegand
2 for DataClock

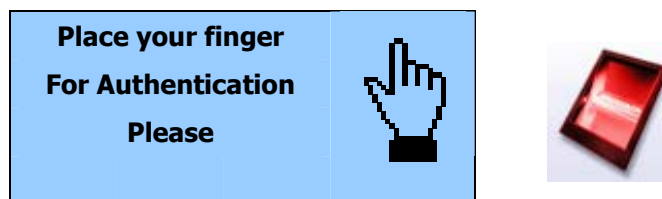
This mode requires an external card reader that will send the ID of the user to authenticate to the MorphoAccess™ Wiegand or DataClock input.



The default screen invites the user to pass his badge so the external reader sends the user ID on MorphoAccess™ Wiegand or Dataclock input.



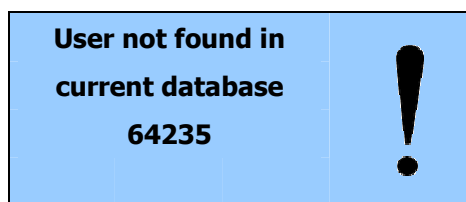
If the ID exists in the database, the MorphoAccess™ performs an authentication using the biometric templates associated to this ID.



If the authentication is successful, the terminal triggers the access or returns the user ID to Central Security Controller.

Once the user authentication is done, the MorphoAccess™ automatically loops back and waits for a new input ID.

If the identifier sent by the reader is not present in the local database authentication is not launched.



Remark about MorphoAccess™ with MA-Xtended licence loaded

A MorphoAccess™ with MA-Xtended licence loaded will scan the five biometric database to find the biometric templates associated to the ID.

Note about "bypass" option

When the *bypass authentication* configuration key is activated (see [Bypassing the biometric control in authentication](#)), the MorphoAccess™ verifies that the ID sent on Wiegand or DataClock input is present on the local database before granting the access.

Wiegand frame configuration

It is possible to define the format of the Wiegand input and thus of the read identifier.

Frame description is based on frame length (in bits), ID, site code position and size and party policy.

RemarkNote: Since the software version 2.00.00 the configuration key name has been modified. The previous set key value is ~~saved~~preserved.

| Wiegand input parameters | | |
|---|---------------------------------|--|
| <i>app/wiegand in/</i> | | |
| <i>frame length</i> (before v2.00 : <i>length</i>) | 1-128 | Defines the number of bits of the frame. |
| <i>start format</i> (before v2.00 : <i>start</i>) | 0.0 1.0 2.n 3.n 4.0 | Defines the start control bit: Reset to 0. Set to 1. Even parity calculated over the n first bits. Odd parity calculated over the n first bits. No start bit. |
| <i>stop format</i> (before v2.00 : <i>stop</i>) | 0.0 1.0 2.n 3.n 4.0 | Defines the stop control bit: Reset to 0. Set to 1. Even parity calculated over the n last bits. Odd parity calculated over the n last bits. No stop bit. |
| <i>site format</i> (before v2.00 : <i>site</i>) | n.m | Insert m bits of site value at offset n. |
| <i>ID format</i> (before v2.00 : <i>Id</i>) | n.m | Insert m bits of ID value at offset n. |
| <i>Custom format</i> (before v2.00: <i>Custom</i>) | n.m | RFU. |

Wiegand frame example (26 bits)

| | | | | | | | | | | | | | |
|-----------------------------|--------|---|---|-----|---|---------|----|----|----|----------------------------|----|------|----|
| 0 | 1 | 2 | 3 | ... | 8 | 9 | 10 | 11 | 12 | ... | 23 | 24 | 25 |
| START | SITE | | | | | ID | | | | | | STOP | |
| 1 | 8 bits | | | | | 16 bits | | | | | | 1 | |
| START bit calculation range | | | | | | | | | | STOP bit calculation range | | | |

BYPASSING THE BIOMETRIC CONTROL IN AUTHENTICATION

This mode requires only a user ID. This ID can be read on a smart card, entered on the keyboard or sent on Wiegand or DataClock input.

The *bypass authentication* configuration key must be combined with an authentication mode. Activating this flag means that the biometric verification is bypassed.

The terminal controls that the user ID exists in the database

When combined with an authentication mode with templates on local database, the MorphoAccess™ verifies that the ID is present on the local database before granting the access.

ID on a contactless card

| Disabling biometric control, but ID must be present in the local database | |
|---|----------|
| <i>app/bio ctrl/bypass authentication</i> | 1 |
| <i>app/bio ctrl/authent ID contactless</i> | 1 |

Required tags on card

| | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|-----------------------|-----|-----------|-----|-----|-----|--------|
| bypass authentication | Yes | No | No | No | No | No |

ID entered on the keyboard

| Disabling biometric control, but ID must be present in the local database | |
|---|----------|
| <i>app/bio ctrl/bypass authentication</i> | 1 |
| <i>app/bio ctrl/authent ID keyboard</i> | 1 |

ID sent on Wiegand or DataClock input

| Disabling biometric control, but ID must be present in the local database | |
|---|----------------------------------|
| <i>app/bio ctrl/bypass authentication</i> | 1 |
| <i>app/bio ctrl/authent remote ID source</i> | 1 for Wiegand 2 for DataClock |

The terminal works as a smart card reader.

When combined *authent PK contactless* the MorphoAccess™ always authorizes the access: the MorphoAccess™ works as a simple Mifare™ card reader.

| Disabling biometric control, access is always granted | |
|---|----------|
| <i>app/bio ctrl/bypass authentication</i> | 1 |
| <i>app/bio ctrl/authent PK contactless</i> | 1 |

Required tags on card

| | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|-----------------------|-----|-----------|-----|-----|-----|--------|
| bypass authentication | Yes | No | No | No | No | No |

RECOGNITION MODE SYNTHESIS

The MorphoAccess™ operating mode is driven by:

- The authentication or identification mode required: Card Only, Card + Biometric, Biometric only.
- Who defined the operating mode: Card or Terminal.

| | Mode defined by Card <i>app/bio ctrl/authent card mode</i> 1 | Mode defined by Terminal <i>app/bio ctrl/authent card mode</i> 0 |
|--|--|---|
| Operating mode | | |
| Authentication Card only | ID in card Card Mode Tag = ID_ONLY | ID in card bypass authentication 1 <i>authent ID contactless 1</i> Check ID on terminal |
| | | ID in card bypass authentication 1 <i>authent PK contactless 1</i> No ID check on terminal |
| Authentication Card + Biometric | ID and BIO in Card Card Mode Tag = PKS | ID and BIO in card bypass authentication 0 <i>authent PK contactless 1</i> |
| | | ID on card and BIO in terminal bypass authentication 0 <i>authent ID contactless 1</i> |
| Identification Biometric only | | ID and BIO in terminal identification 1 |

SETTING UP RECOGNITION STRATEGY

Two attempts mode

If the recognition fails, it is possible to give a “second chance” to the user.

In identification mode if a bad finger is presented the user has 5 seconds to present a finger again. The result is sent if this period expires or if the user presents a finger again.

In authentication mode, if the user presents a bad finger, he can replace his finger without presenting his card again. The result is sent only after this second attempt.

It is possible to set the finger presentation timeout and to deactivate this “two attempts mode”.

If the user is not identified, a second step follows immediately using a smarter coding method. This coding allows recognizing users with dry fingers or fingers with a bad placement on the sensor. However this coding is slower than the light one.

Parameters

This mode can be configured using the *Configuration Tool* for example.

By default the two attempts mode is activated.

Setting up the number of attempts

| | |
|---------------------------------|--|
| <i>app/bio ctrl/nb attempts</i> | 1 (only one attempts) 2 (two attempts mode) |
|---------------------------------|--|

The period between two attempts in identification (two attempts mode) can be modified.

Setting up the identification timeout

| | |
|--|----------|
| <i>app/bio ctrl/identification timeout</i> | 5 (1-60) |
|--|----------|

In authentication mode a finger presentation period can be defined.

Setting up the authentication timeout

| | |
|-------------------------------------|-----------|
| <i>app/bio ctrl/authent timeout</i> | 10 (1-60) |
|-------------------------------------|-----------|

SETTING UP MATCHING PARAMETERS

Setting up matching threshold

bio/bio ctrl/matching th 3 (1-10)

The performances of a biometric system are characterized by two quantities, the False Non Match Rate - FNMR - (also called False Reject Rate) and the False Match Rate - FMR - (also called False Acceptance Rate). Different trade-off are possible between FNMR and FMR depending on the security level targeted by the Central Security Controller. When convenience is the most important factor the FNMR must be low and conversely if security is more important then the FMR has to be minimized.

Different tunings are proposed in the MorphoAccess terminal depending on the security level targeted by the system. The table below details the different possibilities.

This parameter can be set to values from 1 to 10. This parameter specifies how tight the matching threshold is. Threshold scoring values are identified hereafter

| | | |
|----|---|---|
| 1 | Very few persons rejected | FAR < 1% |
| 2 | | FAR < 0.3% |
| 3 | Recommended value | FAR < 0.1% |
| 4 | | FAR < 0.03% |
| 5 | Intermediate threshold | FAR < 0.01% |
| 6 | | FAR < 0.001% |
| 7 | | FAR < 0.0001% |
| 8 | | FAR < 0.00001% |
| 9 | Very high threshold (few false acceptances). Secure application | FAR < 0.0000001% |
| 10 | High threshold for test purpose only | There are very little false recognition, and many rejections. |

FAKE FINGER DETECTION

MA2x1 – MA3x1 compatibility

- Password

Default password is “12345”. (On MA2x1 and MA3x1 terminals, default specific password was “131664”.) **SAGEM recommends strongly** to the administrator to **configure it with a different value**, and specific at each customer.

- Delay after fake finger detection

The function associated to MA2x1 and MA3x1 */cfg/Maccess/Security Policy/Delay in 10ms* configuration key is no more supported.

- FFD security level

The function associated to *app/bio ctrl/FFD security level* is only for stand alone mode. (On MA2x1 and MA3x1 terminals, this parameter applied to standalone mode **and** ILV.) ILV has to set this parameter to have a security level different from default security level.

FFD security level

The fake finger detection is characterized by a false reject rate (percentage of live fingers detected as fake fingers) and a false acceptance rate (percentage of fake finger detected as real ones). This FRR (resp. FAR) is called FFD-FRR (resp. FFD-FAR). The overall reject rate of MAxx1 models is in fact : standard MA FRR + FFD-FRR.

Three security levels are proposed and provide different trade-off between FFD-FAR and FFD-FRR.

| | |
|-------------|---|
| 0 | Low fake finger detection security level |
| 1 (default) | Medium fake finger detection security level |
| 2 | High fake finger detection security level |

Setting up FFD security level

| | |
|--|---------|
| <i>app/bio ctrl/FFD security level</i> | 1 (0-2) |
|--|---------|

Presence detection

Terminals with fake finger detection option allow another presence detection mode.

| | |
|-------------|--|
| 0 (default) | Standard presence detection in identification mode. |
| 1 | In identification mode, sensor is in standby (LEDs are off) while no finger is detected. |

Setting up presence detection

app/bio ctrl/presence detection

0 (0-1)

Failure ID

The administrator may chose the specific ID sent on Wiegand and DataClock interfaces when a fake finger is detected.

Setting up FFD failure ID

app/failure ID/FFD ID

65535 (0-65535)

PROXY MODE

In Proxy mode is an operating mode where the Host System performs the access control remotely.

PROXY MODE (OR SLAVE) PRESENTATION

This operating mode allows to control the MorphoAccess™ remotely (the link is Ethernet or RS422) using a set of biometric and databases management commands.

In Proxy mode the access control is performed remotely by the Host System: MorphoAccess™ works as a slave waiting for external commands such as:

- User identification.
- User verification.
- Relay activation.
- Read data on a contactless smart card.
- Biometric database management.
- Terminal configuration changes.
- Read an entry from the keyboard.
- Display a message.
- Read a contactless smart card.



MorphoAccess™



Host System

Please refer to refer to *MorphoAccess™ Host System Interface Specification*: this document explains how to manage a terminal on a TCP network.

PROXY MODE ACTIVATION

Identification and authentication must be disabled. It means that all controls must be turned off: the terminal becomes a slave.

| Proxy mode | |
|--|----------|
| <i>app/bio ctrl/identification</i> | 0 |
| <i>app/bio ctrl/authent card mode</i> | 0 |
| <i>app/bio ctrl/authent PK contactless</i> | 0 |
| <i>app/bio ctrl/authent ID contactless</i> | 0 |
| <i>app/bio ctrl/authent ID keyboard</i> | 0 |
| <i>app/bio ctrl/authent remote ID source</i> | 0 |
| <i>app/bio ctrl/ BIOPIN enabled</i> | 0 |
| <i>app/bio ctrl/control PIN</i> | 0 |
| <i>app/bio ctrl/bypass authentication</i> | 0 |

APPLICATION CUSTOMIZATION

SETTING UP TIME MASK

When using MEMS™, a time mask feature is available. This mode enables the access according to its time mask. Time mask is defined by slots of 15 minutes over a week.

Note: Since software version 2.00.00 the configuration key path has been modified. The previous set key value is ~~preserved~~**saved**.

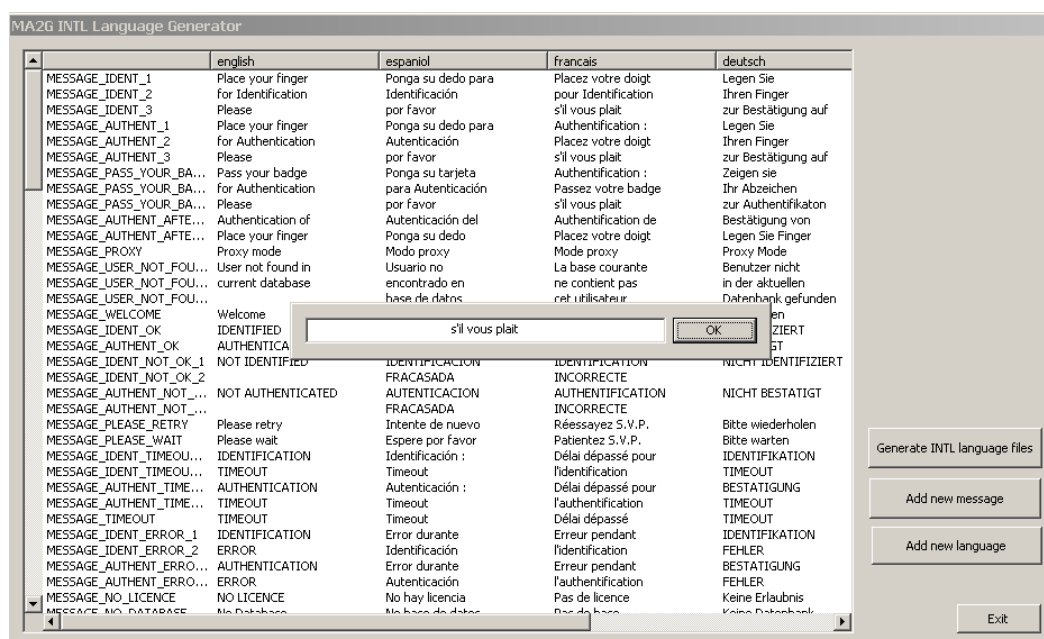
| Time mask activation | |
|--|---|
| <i>Since v2.00 : app/modes/time mask</i> | 1 |
| <i>Before v2.00 :</i> | |
| <i>app/time mask/enabled</i> | |

MULTILINGUAL APPLICATION

The MorphoAccess™ can display texts in six languages (including French, Spanish, German, Italian). It is possible to download a user defined string table. For more information about this feature, refer to the *MorphoAccess™ Host System Interface Specifications*.

| Default language | |
|--|---|
| <code>app/G.U./default language</code> | 0 English (default) 1 Spanish 2 French 3 German 4 Italian 5 Portuguese |

INTL Language Generator allows defining the whole table.



RESULT EXPORTATION

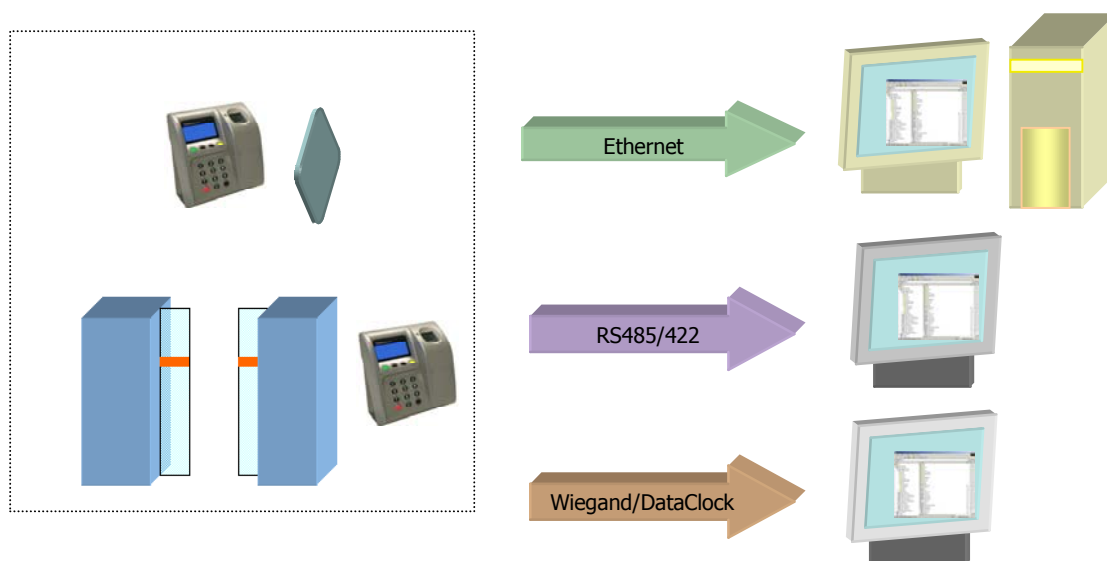
The MorphoAccess™ can export the result of the control to an Central Security Controller, and can log the result in a local diary or directly command an access.

This section is only an introduction about the MorphoAccess™ interface. Please refer to MorphoAccess™ Remote Messages Specification for complete details of each interface.

REMOTE MESSAGES: SENDING THE ID TO THE CENTRAL SECURITY CONTROLLER

Presentation

The MorphoAccess™ terminal can send status messages in real time to an Central Security Controller by different means and through different protocols. This information, called *Remote Messages* can be used, for instance to display on an external screen the result of a biometric operation, the name or the ID of the person identified... depending on the role of the controller in the system.



The *MorphoAccess™ Remote Messages Specification* describes the different solutions offered by the MorphoAccess™ to dialog with a controller, and how to make use of them.

Supported Protocols

The terminal can send messages about the biometric operations performed by the MorphoAccess™ to a controller through the following protocols:

- Wiegand,
- DataClock,
- RS485/422,
- Ethernet (TCP or UDP).

RELAY ACTIVATION

If the control is successful, a relay may be activated to directly control a door. This installation type offers a low security level.

| Relay activation | |
|--------------------------|---|
| <i>app/relay/enabled</i> | 1 |

The relay aperture time can be defined and is set by default to 3 seconds (i.e. 300).

| Relay aperture time in 10 ms | |
|---|----------------------|
| <i>app/relay/aperture time in 10 ms</i> | 300 (50 to 60000) |

LOG FILE

MorphoAccess™ is logging its activities

app/log file/enabled

1

The MorphoAccess™ can log its biometric activities. It stores the result of the command, the possible time and attendance function, date and time, the matching mark, the execution time, and the ID of the user.

It is possible to download the diary file. For more information on this feature, refer to the *MorphoAccess™ Host System Interface Specification*.

It is also possible to display the log file using the *Logs Viewer Application*.

JANUARY 8 2007

15:25,OK,783170

15:28,KO,

15:45,OK,7895641

15:59,KO,783170

LED IN ACTIVATION

Use this signal to wait a controller “ACK” before granting the access.



LED1 to GND: Access authorized.
LED2 to GND: Access refused.

1. If the user is recognized the MorphoAccess™ sends the user identifier to the controller.
2. The MorphoAccess™ waits for a **GND** signal on LED1 or LED2. A timeout can be defined.
3. The controller checks the user rights.
4. The controller sets LED1 to **GND** to authorize the access or sets LED2 to **GND** to forbid the access.

This feature improves integration in an Central Security Controller (ACS). The ACS through LED IN signals validates result of biometric matching.

| LED IN mode activation | |
|---------------------------|---|
| <i>app/led IN/enabled</i> | 1 |

When the ACS validates the control a timeout must be specified: it defines the time during which the MorphoAccess™ will wait for an acknowledgement signal from the ACS through LED IN signals.

| LED IN acknowledgement timeout in 10 ms | |
|--|--------------------|
| <i>app/led IN/controller ack timeout</i> | 300 (0 to 3000) |

If the controller has only one LED signal dedicated to “access authorized”, this signal must be connected to LED1 input. In this case “access forbidden” signal will be based on a timeout. "controller ack timeout" value must be defined as short as possible in a range corresponding to controller reply delay.

A controller with distinct outputs (one for “access forbidden”, one for “access authorized”) will be connected to LED1 and LED2.

SECURITY FEATURES

TAMPER SWITCH MANAGEMENT

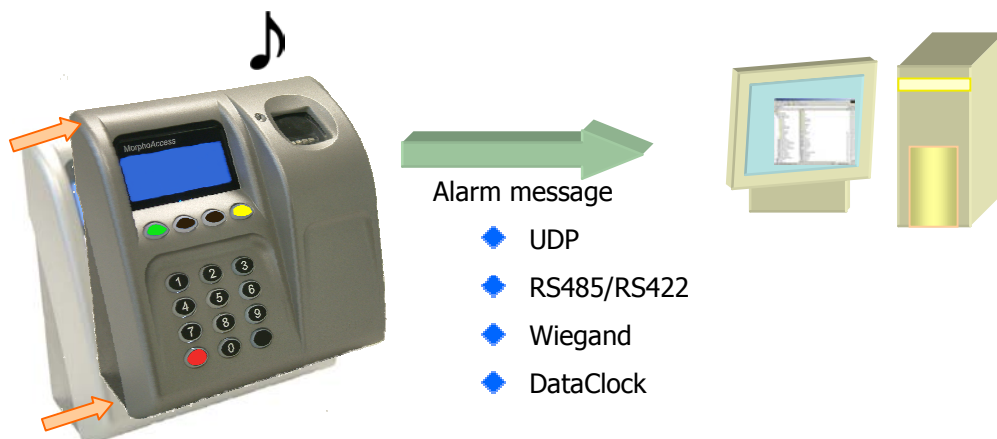
Alarm activation

The MorphoAccess™ can detect two intrusion attempts type:

- Someone tries to steal the complete terminal (opto-sensor is triggered).
- Someone tries to open the terminal (tamper switch is triggered).

The device can send an alarm to the central controller in case of intrusion. It can also play a sound alarm while sending the alarm.

Note: either the tamper switch or the opto-sensor triggers the alarm. Please refer to *MA500 Series Installation Guide* to identify these switches on the terminal.



To send an alarm on an output (UDP, RS485/RS422, Wiegand, DataClock), the corresponding interface must be activated otherwise no alarm will be sent.

Because Wiegand and DataClock are multiplexed on the same lines, only one of these protocols shall be enabled at one time, else priority is given to *Wiegand*, then *DataClock*.

These keys are:

app/send ID wiegand/enabled

app/send ID dataclock/enabled

app/send ID serial/enabled

app/send ID serial/mode (to select RS422 or RS485 link)

app/send ID UDP/enabled

Setting the key *app/tamper alarm/level* to an appropriate value configure tamper switch management feature.

| Tamper Alarm Level | |
|---|-----------|
| <i>app/tamper alarm/level</i> | 0 (0 – 2) |
| 0 No Alarm. 1 Send Alarm (No Sound Alarm). 2 Send Alarm and Activates Buzzer (Sound Alarm) | |

The key *app/failure ID/alarm ID* defines the value of the alarm ID to send in Wiegand or DataClock. This ID permits to distinguish between a user ID and an error ID. To be validated, key *app/failure ID/enabled* must be set to 1.

| Tamper Alarm ID | |
|--------------------------------|-------------------|
| <i>app/failure ID/alarm ID</i> | 65535 (0 – 65535) |
| <i>app/failure ID/enabled</i> | 1 |

In Wiegand and DataClock the alarm ID is sent like other Failure Ids. See the documentation *MorphoAccess™ Remote Messages Specification* for a description of the packet format in UDP and RS485.

Examples

Example 1: Send an alarm ID (62221) in Wiegand, and play sound warning, in case of intrusion detection.

To send an alarm in Wiegand, the key *app/send ID wiegand/enabled* must be set to 1, and the key *app/tamper alarm/level* must be set to 2 (alarm and buzzer.)

The key *app/failure ID/alarm ID* must be set to 62221 to link the intrusion event to this identifier.

Example 2: Send an alarm in UDP quietly in case of intrusion detection.

To send an alarm in UDP, the key *app/send ID UDP/enabled* must be set to 1.

Then the key *app/tamper alarm/level* must be set to 1 (quiet alarm.)

PASSWORDS

Two passwords protect the system:

- The *Terminal Configuration Password* protects MorphoAccess™ local administration and controls devices settings.
- The *User Management Password* is required to access to local database: it protects the *Enrolment Application* and the *Log Viewer Application*.

 Default password value is “12345”.

 **If a password is lost terminal must be returned to SAGEM Sécurité.**

ANNEX

MORPHOACCESS™ 220 320 COMPATIBILITY

These tables present parameters equivalence between MA300/200 family.
[Multi-factor mode](#) (*/cfg/Maccess/Admin/mode 5* on 220 and 320) is activated when *app/bio ctrl/identification* is set to 1.

| MA 200/300 | MA 500 |
|------------|--------|
|------------|--------|

| Identification | |
|----------------------------------|---|
| <i>/cfg/Maccess/Admin/mode 0</i> | <i>app/bio ctrl/identification 1</i> <i>app/bio ctrl/* 0</i> |

| Contactless authentication with ID on card, template in local database | |
|--|--|
| <i>/cfg/Maccess/Admin/mode 4</i> | <i>app/bio ctrl/authent ID contactless 1</i> |

| Contactless authentication: Card mode | |
|--|---|
| <i>/cfg/Maccess/Contactless/without DB mode 0</i> <i>/cfg/Maccess/Admin/mode 3 or</i> | <i>app/bio ctrl/authent card mode 1</i> |
| <i>/cfg/Maccess/Admin/mode 5</i> <i>(mutli-factor mode)</i> | <i>app/bio ctrl/identification 1</i> |

| Contactless authentication: Biometric verification | |
|--|--|
| <i>/cfg/Maccess/Contactless/without DB mode 2</i> <i>/cfg/Maccess/Admin/mode 3 or</i> | <i>app/bio ctrl/authent PK contactless 1</i> |
| <i>/cfg/Maccess/Admin/mode 5</i> <i>(mutli-factor mode)</i> | <i>app/bio ctrl/identification 1</i> |

| Contactless authentication: ID “only”, no biometric verification | |
|--|---|
| <i>/cfg/Maccess/Contactless/without DB mode 1</i> <i>/cfg/Maccess/Admin/mode 3 or</i> | <i>app/bio ctrl/authent PK contactless 1</i> <i>app/bio ctrl/bypass authentication 1</i> |
| <i>/cfg/Maccess/Admin/mode 5</i> <i>(mutli-factor mode)</i> | <i>app/bio ctrl/identification 1</i> |

| Authentication: ID input from Wiegand or DataClock | |
|--|---|
| <i>/cfg/Maccess/Admin/mode 1</i> Jumper configuration defining the ID source (DataClock or Wiegand) | <i>app/bio ctrl/authent remote ID source 1 or 2</i> |

| Proxy mode | |
|----------------------------------|--|
| <i>/cfg/Maccess/Admin/mode 2</i> | <i>app/bio ctrl/identification 0</i> <i>app/bio ctrl/authent card mode 0</i> <i>app/bio ctrl/authent PK contactless 0</i> <i>app/bio ctrl/authent ID contactless 0</i> <i>app/bio ctrl/authent ID keyboard 0</i> <i>app/bio ctrl/authent remote ID source 0</i> |

CONTACTLESS MODES TABLE

| Operation | Authent card mode | Authent PK contactless | Authent ID contactless | Bypass authentication |
|--|-------------------|------------------------|------------------------|-----------------------|
| Authentication with templates in database Read ID on contactless card. Retrieve corresponding templates in database. Biometric authentication using these templates. Send ID if authentication is successful. | 0 | 0 | 1 | 0 |
| Authentication with templates on card Read ID and templates on contactless card. Biometric authentication using these templates. Send ID if authentication is successful. | 0 | 1 | 0 | 0 |
| Card mode authentication Read card mode, ID, templates (if required by card mode) on contactless card. If card mode is « ID only », send ID. If card mode is « Authentication with templates on card », biometric authentication using templates read on card, then send ID if authentication is successful. | 1 | 0 | 0 | 0 |
| Authentication with templates in database – biometric control disabled Read ID on contactless card. Check corresponding templates presence in database. Send ID if templates are present. | 0 | 0 | 1 | 1 |
| Authentication with templates on card – biometric control disabled Read ID on contactless card. Send ID. | 0 | 1 | 0 | 1 |
| Card mode authentication – biometric control disabled Read card mode, ID, templates (if required by card mode) on contactless card. Whatever card mode, send ID. | 1 | 0 | 0 | 1 |

REQUIRED TAGS ON CONTACTLESS CARD

| Operation | ID | CARD MODE | PK1 | PK2 | PIN | BIOPIN |
|--|-----|-----------|-----|-----|-----|--------|
| Authentication with templates in database | Yes | No | No | No | No | No |
| Authentication with templates on card | Yes | No | Yes | Yes | No | No |
| Card mode authentication (ID_ONLY) | Yes | Yes | No | No | No | No |
| Card mode authentication (PKS) | Yes | Yes | Yes | Yes | No | No |
| Authentication with templates in database – biometric control disabled | Yes | No | No | No | No | No |
| Authentication with templates on card – biometric control disabled | Yes | No | No | No | No | No |
| Card mode authentication (ID_ONLY) – biometric control disabled | Yes | Yes | No | No | No | No |
| Card mode authentication (PKS) – biometric control disabled | Yes | Yes | Yes | Yes | No | No |
| BIOPIN check | Yes | No | No | No | No | Yes |
| PIN check | Yes | No | No | No | Yes | No |

FAQ

Sensor is off

Verify that the base contents at least one record.

Check that identification is enabled.

Terminal returns erratic answers to ping requests

Check the subnet mask. Ask to your administrator the right value.

RELATED DOCUMENTS

Administrator Information

MA500 Series Installation Guide

This document describes terminal electrical interfaces and connection procedures.

MA500 Series Parameters Guide

The complete description of terminal configuration files and registry keys. This document gives also parameters default values.

Developer Information

MorphoAccess™ Host Interface Specification

A complete description of remote management commands.

MorphoAccess™ Remote Messages Specification

Details how the MorphoAccess™ sends the access control result to a Central Security Controller.

MorphoAccess™ Contactless Card Specification

This document describes the MorphoAccess™ contactless card feature.

Support Tools

Configuration Tool User Guide

Configuration Tool user guide, via Ethernet.

USB Tool User Guide

Configuration Tool user guide, via USB key.

MA500 Series Upgrade Tools User Guide

Upgrade Tool user guide about firmware upgrading procedures.



Siège social : Le Ponant de Paris
27, rue Leblanc - 75512 PARIS CEDEX 15 - FRANCE