

# MORPHOACCESS™

## *Installation Guide*





## CONTENTS

<b>INTRODUCTION</b>	<b>9</b>
<b>SAFETY INSTRUCTIONS</b>	<b>10</b>
<b>REPLACEMENT OF THE BATTERY LOCATED ON THE MOTHERBOARD</b>	<b>11</b>
<b>GENERAL DESCRIPTION</b>	<b>12</b>
<b>INSTALLATION PROCEDURE</b>	<b>13</b>
STAGE 1: DRILLING THE MOUNTING HOLES	13
STAGE 2: MOUNTING THE METAL CHASSIS ASSEMBLY	14
STAGE 3: CONNECTING THE CHASSIS ASSEMBLY TO THE COVER ASSEMBLY	15
STAGE 4: CLOSING MORPHOACCESS™	16
<b>HOW TO UPGRADE MORPHOACCESS™ 200 TO 300</b>	<b>17</b>
<b>ELECTRICAL INTERFACE</b>	<b>18</b>
TERMINAL BLOCK BOARD	18
POWER SUPPLY CABLE	19
COM1 RS422 SERIAL PORT WIRING	19
COM1 DEISTER WIRING (OPTIONAL)	20
ETHERNET WIRING	20
COM2 RS232 WIRING	21
WIEGAND OUTPUT WIRING	21
WIEGAND INPUT WIRING	22
DATA CLOCK OUTPUT WIRING	22
DATA CLOCK INPUT WIRING	23
OUTPUT RELAYS AND TAMPER SWITCHES	24
<b>WIEGAND / DATALOCK: MOTHERBOARD CONFIGURATION</b>	<b>25</b>
<b>USER INTERFACE</b>	<b>27</b>
<b>ACCESS CONTROL BY IDENTIFICATION (MORPHOACCESS™ 200)</b>	<b>28</b>
<b>ACCESS CONTROL BY IDENTIFICATION (MORPHOACCESS™ 300)</b>	<b>29</b>

<b><u>ACCESS CONTROL BY AUTHENTICATION – ID SENT ON WIEGAND OR DATACLOCK</u></b>	<b>31</b>
<b><u>CONTACTLESS AUTHENTICATION WITHOUT DATABASE</u></b>	<b>33</b>
ID ONLY MODE	34
TEMPLATES OR BIOPIN CODE MODE	35
PIN CODE MODE	36
PIN CODE THEN TEMPLATES OR BIOPIN CODE MODE	37
CARD DEFINED MODE	39
<b><u>CONTACTLESS AUTHENTICATION WITH : STANDARD CARD</u></b>	<b>40</b>
<b><u>CONTACTLESS AUTHENTICATION WITH DATABASE: BINARY ID</u></b>	<b>42</b>
<b><u>PROXY MODE</u></b>	<b>45</b>
<b><u>MERGED MODE</u></b>	<b>46</b>
<b><u>AUTHENTICATION MODE WITH DATABASE: USING KEYBOARD ID</u></b>	<b>47</b>
<b><u>SOFTWARE ADMINISTRATOR INTERFACE</u></b>	<b>48</b>
<b><u>BIOMETRIC MANAGEMENT OPERATIONS</u></b>	<b>49</b>
BIOMETRIC MANAGEMENT BETWEEN TERMINAL AND MORPHOACCESS™ MANAGEMENT SYSTEM (MMS)	49
BIOMETRIC MANAGEMENT IN STAND-ALONE MODE	50
INSERT TEMPLATE/ID IN DATABASE	51
REMOVE TEMPLATE/ID FROM DATABASE	51
REMOVE ALL TEMPLATE/ID FROM DATABASE	52
RESET CONFIGURATION TO FACTORY SETTINGS	52
WARM-UP RESET	52
<b><u>ACCESS THE SET UP FUNCTIONS OF THE SYSTEM</u></b>	<b>54</b>
<b><u>CONFIGURATION MENU</u></b>	<b>56</b>
<b><u>HOW TO EDIT PARAMETERS? NETWORK PARAMETERS EXAMPLE</u></b>	<b>57</b>
<b><u>SYSTEM AND ADMIN PASSWORDS</u></b>	<b>59</b>
MORPHOACCESS™ SYSTEM ADMINISTRATOR PIN	59
MORPHOACCESS™ ADMINISTRATOR PIN	59

<b>SETTING UP HOST COMMUNICATION.</b>	<b>60</b>
<b>SETTING UP MATCHING PARAMETERS</b>	<b>61</b>
SETTING UP JUVENILE RECOGNITION	61
SETTING UP ANTI-LATENCY	61
SETTING UP RECOGNITION MODE	62
MATCHING THRESHOLD	64
<b>USER INTERFACE SETTINGS</b>	<b>66</b>
MULTILINGUAL APPLICATION	66
IDENTIFICATION INFORMATION	67
CLOCK	68
IDLE MODE	68
<b>DISPLAY PERSONALIZATION</b>	<b>69</b>
<b>SETTING UP CONTACTLESS READER PARAMETERS</b>	<b>70</b>
<b>LOG FILE</b>	<b>72</b>
<b>SETTING UP TIME MASK</b>	<b>73</b>
<b>SETTING UP DOWNLOAD AGENT - (SDL)</b>	<b>74</b>
<b>WIEGAND / DATACLOCK CONFIGURATION</b>	<b>75</b>
NOTE	75
WIEGAND / DATACLOCK : ID SENDING	75
WIEGAND / DATACLOCK : ADVANCED INFORMATIONS	76
WIEGAND : FACILITY CODE	76
WIEGAND : FACILITY CODE VERIFICATION	77
DATACLOCK : DATA AND STROBE LEVELS	77
WIEGAND / DATACLOCK : LED OUT – CARD PRESENT SIGNALS	77
WIEGAND / DATACLOCK : LED IN SIGNAL	79
SETTING UP WIEGAND INTERFACE	80
<b>ID SENDING ON UDP</b>	<b>82</b>
<b>ID SENDING ON RS232 OR RS422</b>	<b>83</b>
ID SENDING ON « COM1 »	83
ID SENDING ON « COM2 »	83

<b>SERIAL PORT PARAMETERS</b>	<b>85</b>
COM1 PORT (SER0)	85
USING A DEISTER CONTACTLESS READER ON COM1	86
COM2 PORT (SER1)	86
<b>RELAY ACTIVATION</b>	<b>87</b>
<b>TIME AND ATTENDANCE</b>	<b>88</b>
<b>THE VERSION MENU</b>	<b>91</b>
<b>THE SERIAL NUMBER MENU</b>	<b>92</b>
<b>THE SETTING MENU</b>	<b>93</b>
<b>ACCESS THE MIFARE KEYS UPDATE MENU (MORPHOACCESS 220)</b>	<b>95</b>
<b>CONTACTLESS CARD DATA STRUCTURE (MORPHOACCESS 220 ONLY)</b>	<b>97</b>
DATA STRUCTURE	97
MORPHOACCESS™ TAGS	97
<b>ADMIN CARD FORMAT (MORPHOACCESS 220 ONLY)</b>	<b>99</b>
SAGEM KEYS	99
MAPPING	100
<b>COMMUNICATION PROTOCOL</b>	<b>101</b>
<b>MORPHOACCESS-TECHNICAL CHARACTERISTICS</b>	<b>102</b>
DISPLAY	102
KEYBOARD	102
FUSE	102
MEMORY	102
PERIPHERALS INTERFACES	102
POWER SUPPLY	102
SIZE AND WEIGHT	103
ENVIRONMENTAL CONDITIONS	103
STORAGE CONDITIONS	103
CLEANING PRECAUTIONS	103
<b>RECOMMENDATIONS</b>	<b>104</b>

AREAS CONTAINING COMBUSTIBLES	104
GENERAL PRECAUTIONS	104
ETHERNET CONNECTION	104
DATE / TIME SYNCHRONISATION	105
WARNING	105
<b><u>APPENDIX 1 - ETHERNET COLOR STANDARD</u></b>	<b>106</b>
RJ45 PINOUT	106
<b><u>APPENDIX 2 - WIEGAND DATA FORMAT</u></b>	<b>107</b>
EXAMPLES	108
<b><u>APPENDIX 3 - ISO 7811/2-1995 - TRACK 2 DATACLOCK FORMAT</u></b>	<b>109</b>
DATA ENCODING TABLE	109
DATACLOCK LEVELS	111
<b><u>APPENDIX 4 - RESERVED CONFIGURATION</u></b>	<b>112</b>
<b><u>APPENDIX 5 - FINGERPRINT PLACEMENT RULES</u></b>	<b>113</b>
<b><u>APPENDIX 6 – RECOGNITION MODES</u></b>	<b>114</b>
<b><u>BIBLIOGRAPHY</u></b>	<b>115</b>
<b><u>DRILLING TEMPLATE</u></b>	<b>116</b>



## INTRODUCTION

Congratulations for choosing the SAGEM MorphoAccess™<sup>1</sup> Automatic Fingerprint Recognition Terminal. MorphoAccess™ provides an innovative and effective solution for access control or time and attendance 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 (MorphoSoft™ and MorphoImaging™). This technology is based on lessons learned during 18 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.

The SAGEM MorphoAccess™ offers the following advantages:

- High quality optical scanner.
- Supports multiple input/output interfaces used in the physical access control industry.
- Local area network interface for easy interaction with other host systems.
- Compact size for easy installation and integration into your available office space.
- Intuitive interface that is easy to use in both setup and operational modes.
- Extensive, flexible flash memory for data storage (user data, biometric templates, etc.).

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

---

<sup>1</sup> The SAGEM logo and trademark are the property of *SAGEM Défense Sécurité*.

All other trademarks or product names are trademarks or product names of the respective title holders.

## SAFETY INSTRUCTIONS

The installation of this product should be made by a qualified service Person and should conform to all local codes.

It is strongly recommended to use a class II power supply at 12 V  $\pm$ 5% and 2.5 A/min according with Safety Electrical Low Voltage (SELV). The 12 V power supply cable length should not exceed 3 meters.

This product is intended to be installed in accordance with the NEC Class 2 requirements; or supplied by a listed external Power Unit marked Class 2, Limited Power source, or LPS and rated 12 V DC, 2.5 A minimum.

In case of building to building connection it is recommended to connect 0V to ground. Ground cable must be connected with the terminal block board fixation screw marked with universal ground symbol.



**Warning::** The user could connect the MorphoAccess™ 0V to Ground only if the MorphoAccess™ was before connected and tested in working.

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

**USA:** This equipment has been tested and found compliant with Class B digital device requirements, pursuant to part 15 of the FCC Rules. These requirements are designed to ensure reasonable protection against harmful RF 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 interfere with radio communications. If this equipment interferes with radio or television reception - which can be determined by disconnecting and re-connecting the unit – 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.

## REPLACEMENT OF THE BATTERY LOCATED ON THE MOTHERBOARD

### **CAUTION**

**Danger of explosion if battery is incorrectly replaced.**

**Replace only with the same or equivalent type recommended by the manufacturer.**

**Must be disposed of properly.**

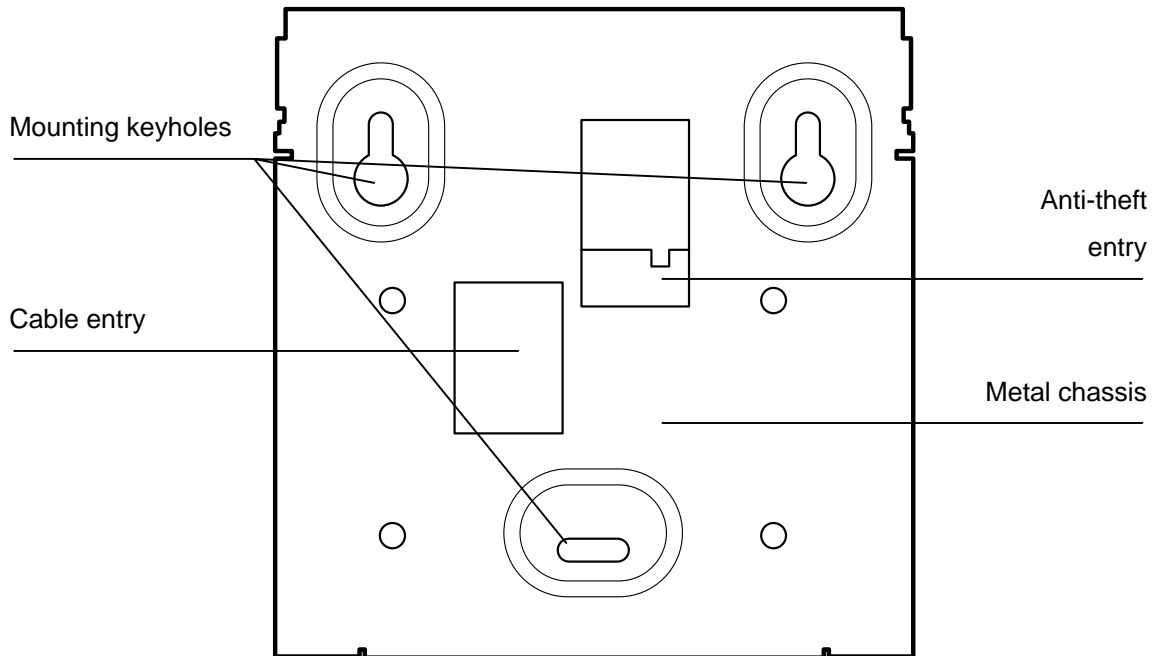
### **ATTENTION**

**Il y a danger d'explosion s'il y a remplacement incorrect de la batterie.**

**Remplacer uniquement avec une batterie du même type ou d'un type équivalent recommandé par le constructeur.**

**Éliminer de façon appropriée.**

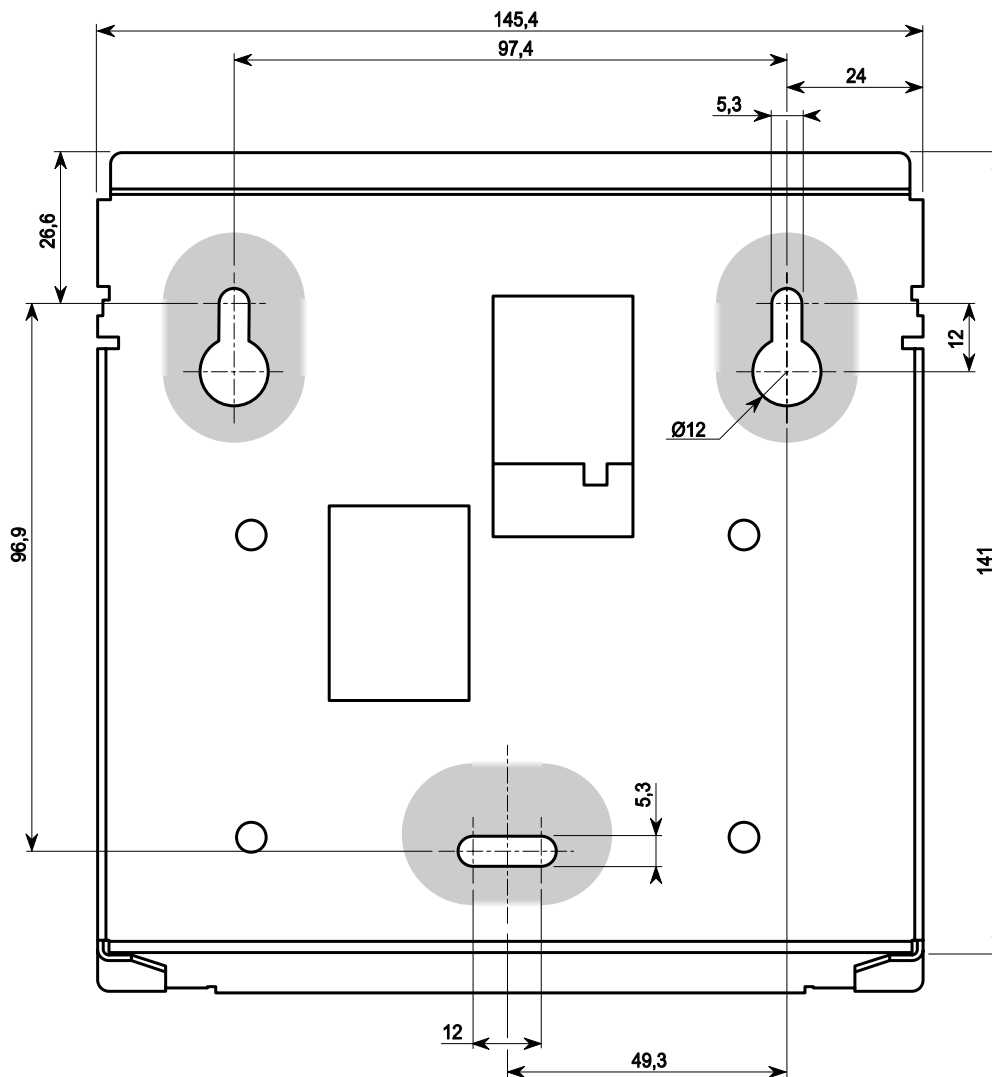
## GENERAL DESCRIPTION



## INSTALLATION PROCEDURE

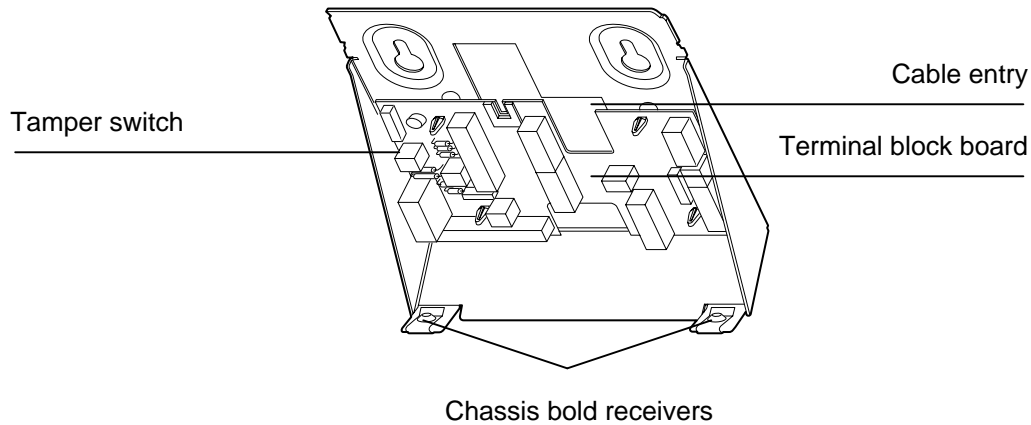
### Stage 1: Drilling the mounting holes

#### Mounting and cable entry hole location (rear view)



- Drill the 2 holes for the screws for the mounting keyholes so that the cable entry is in a suitable position for your cabling, using the dimensional drawing above.
- Drill the hole for the third screw in the centre of the slot so that it is possible to correct the position later, if necessary.
- The mounting screws must be 5 mm diameter maximum.

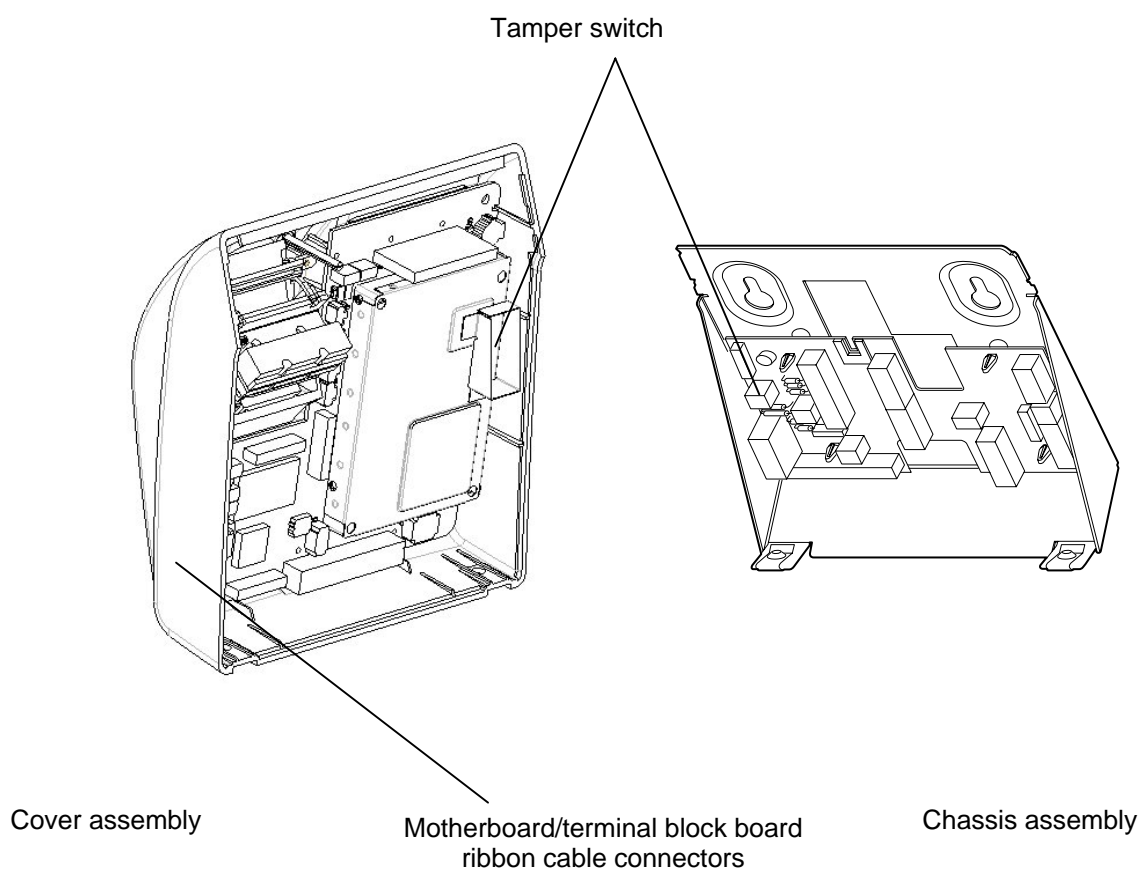
## Stage 2: Mounting the metal chassis assembly



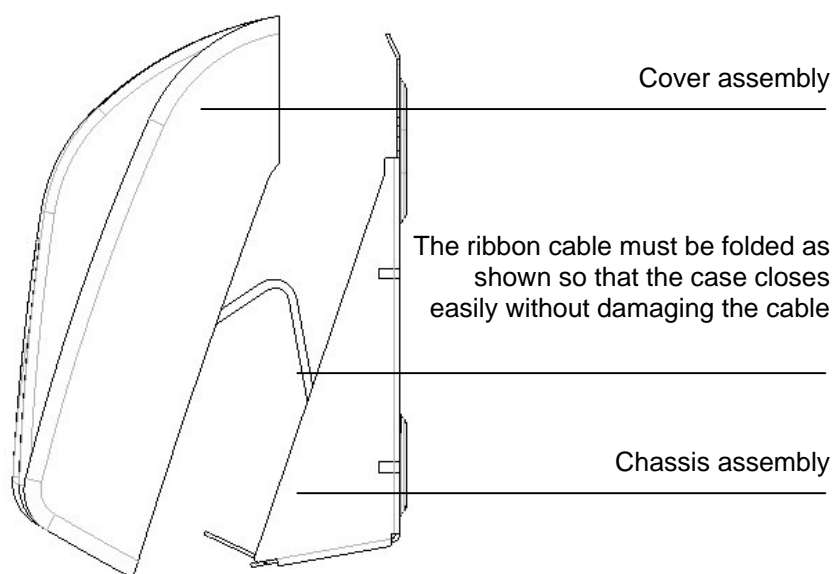
- a) Disconnect the ribbon cable between the motherboard and the terminal block board so that the assembly shown above can be detached from the rest of MorphoAccess™.
- b) Pass the connecting cables through the cable entry.
- c) Position the chassis assembly against the wall using the two screws in the mounting keyholes.
- d) Hold the chassis in place with a screw through the mounting slot.
- e) Adjust the position, and fix in place by tightening all three screws.
- f) Connect cables to terminal blocks (see the detailed instructions in the following sections).

## Stage 3: Connecting the chassis assembly to the cover assembly

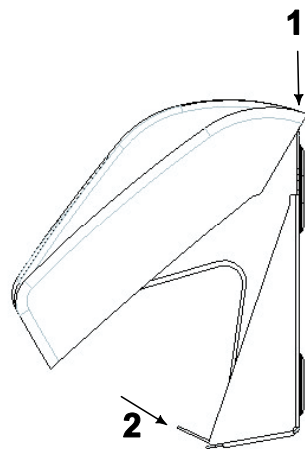
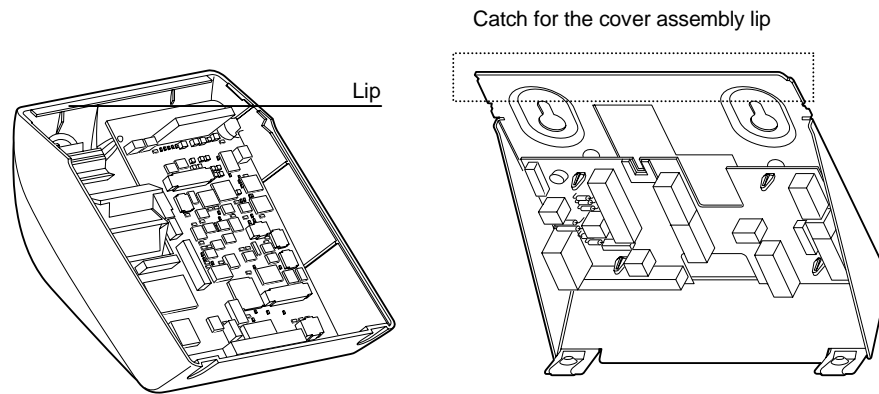
### Ribbon cable connector location



### Position of the ribbon cable as the case is closed



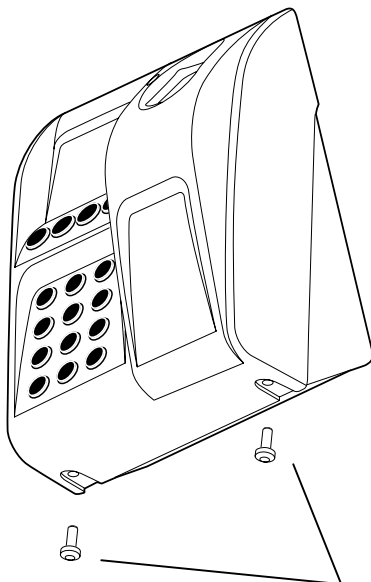
## Stage 4: Closing MorphoAccess™



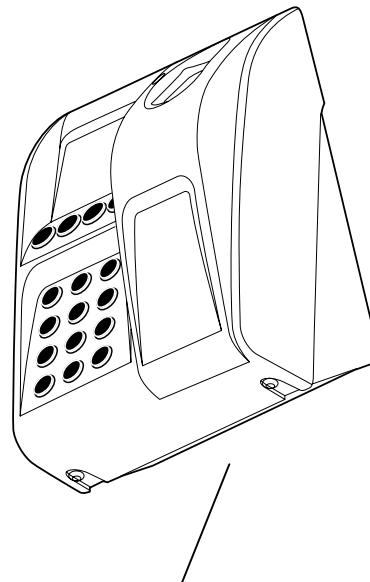
When the ribbon cable has been connected between the two assemblies (see stage 3), the cover assembly is fitted to the chassis assembly.

1 The lip on the cover slides behind the chassis, to fit over the catch shown on the diagram above.

2 The cover is fitted onto the chassis by rotating it.



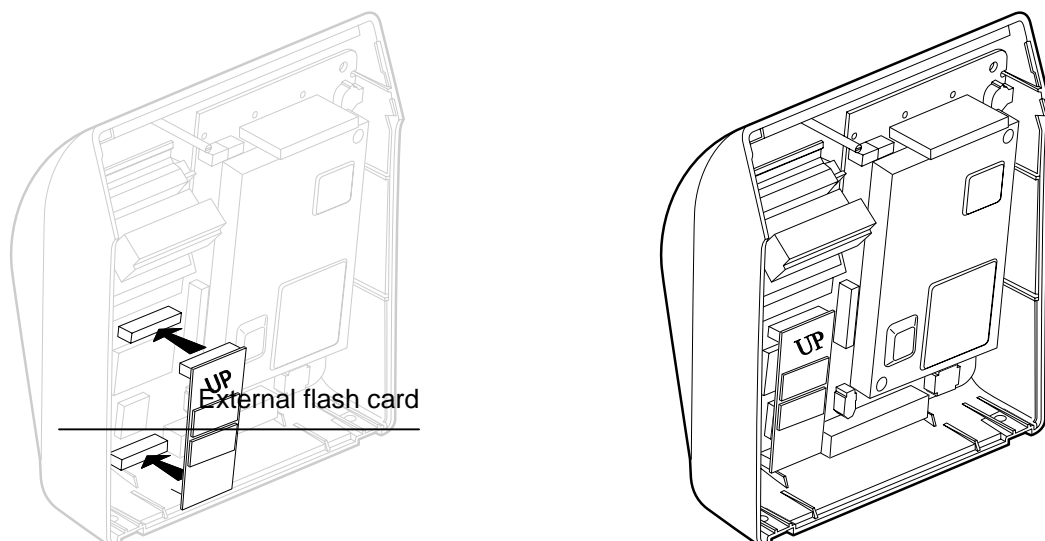
Fit the two M4x10 assembly screws. Use screwdriver TORX 20



Assembled MorphoAccess™


## HOW TO UPGRADE MORPHOACCESS™ 200 TO 300

This operation requires that the MorphoAccess™ is powered off.



When external flash card is inserted, the MorphoAccess™ 200 becomes a MorphoAccess™ 300. From then, all database information will be stored on the new media.

 **Warning:** All database information of the MorphoAccess™ 200 is lost.

 **Warning:** 12 pin card flash must be connected on the most right position on the 13 pin motherboard connector. One pin of the motherboard connector must be visible on the left side of the external card flash while connected.

Bad positioning may damage the external card flash.

For more information, refer to the *MorphoAccess Host System Interface Specifications*.

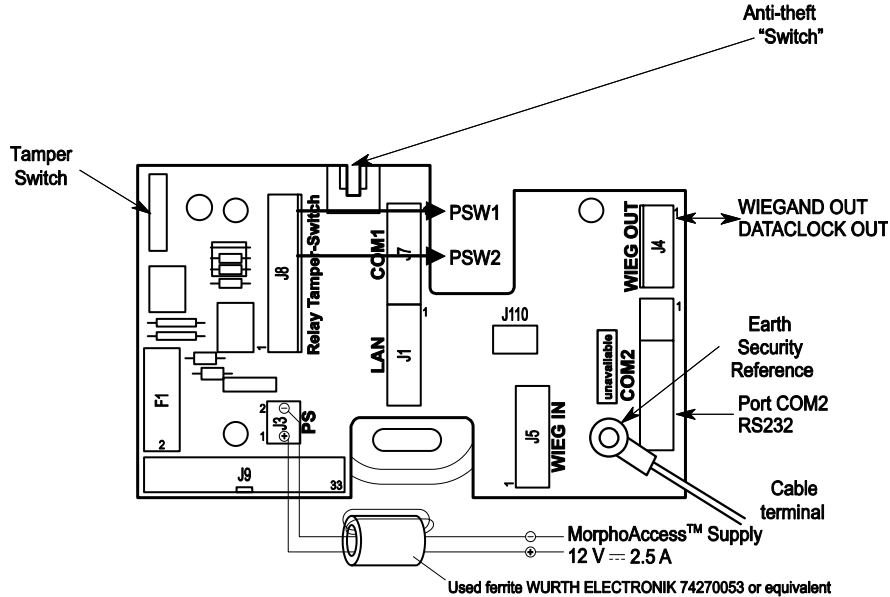
This upgrade is available for products with serial number starting with 01511XXXX.

This remark does not concern 13 pin card.

After card flash installation, for the first terminal power on, a memory initialization is performed during approximated 1 minute, then will increase the terminal starting time.

## ELECTRICAL INTERFACE

### Terminal block board

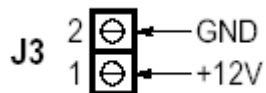


For EMC compatibility in order to be EC and FCC compliant (EN55022, EN55024 FCC part 15), it must be set an axial ferrite bead (2 turns) with the 12 V supply cable, and for any interface cable used, except Ethernet LAN.

J1	5 pin block	Ethernet Interface (LAN 10 Mbps)
J3	2 pin block	12 V supply $\pm$ 5% regulated
J4	4 pin block	Wiegand output to host or Data Clock output
J5	5 pin block	Wiegand peripheral input or Data Clock output
J7	5 pin block	COM1 RS422 serial interface
J8	7 pin block	Output relay and Tamper-Switch
J9	34 way ribbon cable	Cable connection to main assembly
J11	5 pin block	COM2 reduced RS232C serial
F1	Fuse	2.5 A quick blow fuse

## Power supply cable

The terminal blocks are shown viewed from the front with the chassis assembly in its normal position on the wall.



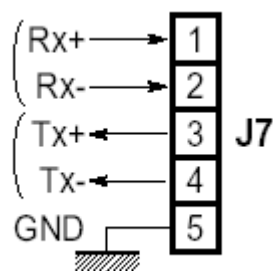
### Terminal block J3

Pin 1 +12 V Power

Pin 2 Ground Power

Power supply 12 V  $\pm$  5% (regulated) 2.5 A

## COM1 RS422 serial port wiring



### Terminal block J7

Pin 1 Rx+ Input

Pin 2 Rx- Input

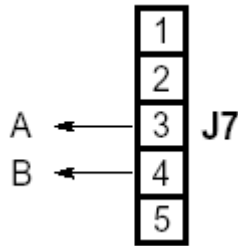
Pin 3 Tx+ Output

Pin 4 Tx- Output

Pin 5 Ground Ground

For a half-duplex RS422 connection, only Tx+, Tx- and ground are connected. Otherwise, as the unit is a peripheral, the connections must be crossed over: Rx on the MorphoAccess™ is connected to Tx on the host and Tx on the MorphoAccess™ is connected to Rx on the host.

## COM1 Deister wiring (optional)



### Terminal block J7

Pin 3 A Input/Output

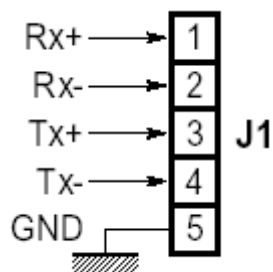
Pin 4 B Input/Output

To use the features of the optional Deister contactless card reader, connect the AB wires to the Tx port.

AB wires are connected to the Deister contactless card reader as defined in its install manual.

For more information about this option, please contact your SAGEM sales representative.

## Ethernet wiring



### Terminal block J1

Pin 1 Rx+ Input

Pin 2 Rx- Input

Pin 3 Tx+ Output

Pin 4 Tx- Output

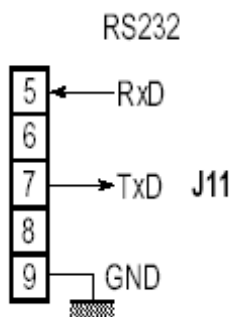
Pin 5 Ground Ground

See Ethernet color standard Appendix.

See Ethernet connection recommendations in Recommendations section.

## COM2 RS232 wiring

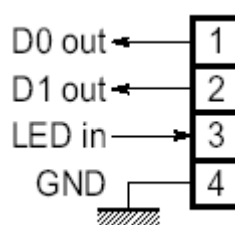
For a reduced RS232C (no handshake), only TxD, RxD and ground are connected on J11.



### Terminal block J11: Reduced RS232

Pin 5	RxD	Input
Pin 6	Not connected	
Pin 7	TxD	Output
Pin 8	Not connected	
Pin 9	Ground	Ground

## Wiegand output wiring

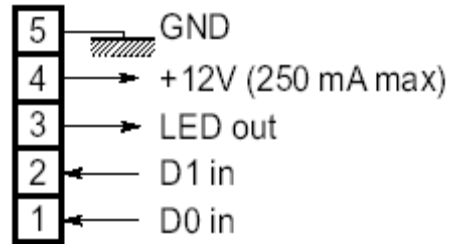


### Terminal block J4

Pin 1	Data 0	Output
Pin 2	Data 1	Output
Pin 3	LEDin	Input
Pin 4	Ground	Ground

Electrical interface conforms to the Security Industry Association's Wiegand standard March 1995.

## Wiegand input wiring



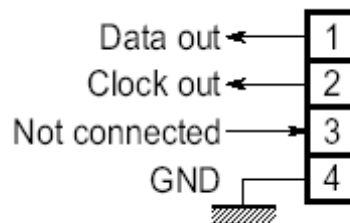
### Terminal block J5

Pin 1	Data 0	Input
Pin 2	Data 1	Input
Pin 3	LEDin	Output
Pin 4	+12V	Power
Pin 5	Ground	

Electrical interface conforms to the Security Industry Association's Wiegand standard March 1995.

The supply available to the peripheral is +12 V at 250 mA max.

## Data Clock output wiring



### Terminal block J4

Pin 1	Data	Output
Pin 2	Clock	Output
Pin 3	Not connected	
Pin 4	Ground	Ground

The electrical interface is 5 V TTL.

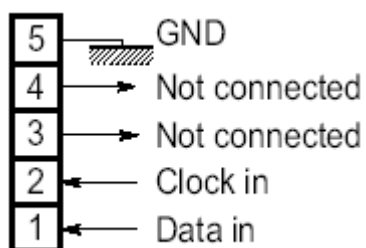


### Terminal block J5

Pin 3	Card present	Output
-------	--------------	--------

### Data Clock input wiring

#### Terminal block J5

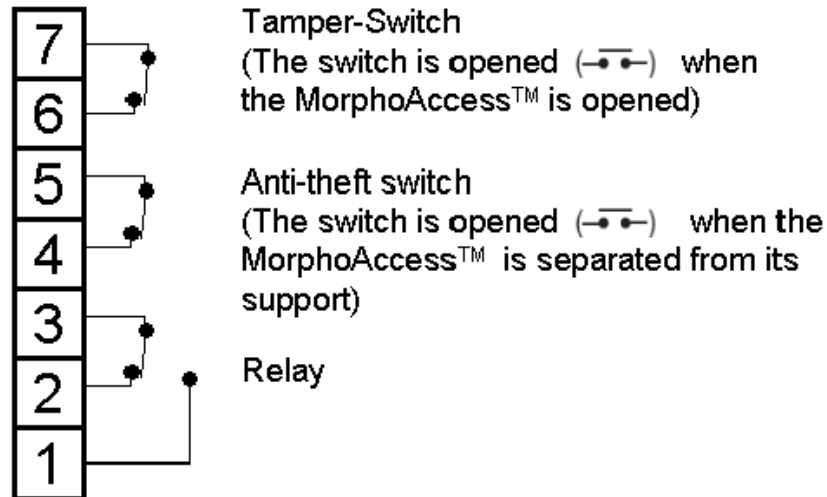


Pin 1	Data	Input
Pin 2	Clock	Input
Pin 3	Not connected	
Pin 4	Not connected	
Pin 5	Ground	Ground

The electrical interface is 5 V TTL compatible.

## Output relays and Tamper switches

A three-pin relay output is available. It has a common, a normally open contact and a normally closed contact.



### Terminal block J8

Pin 1	Normally open
Pin 2	Normally closed
Pin 3	Common
Pin 4	Anti-theft switch
Pin 5	Anti-theft switch
Pin 6	Tamper switch
Pin 7	Tamper switch

### Relay ratings

1 A at 30 VDC according to the safety extra low voltage requirements (42.4 VAC max, 60 VDC max) independently of the power supply.

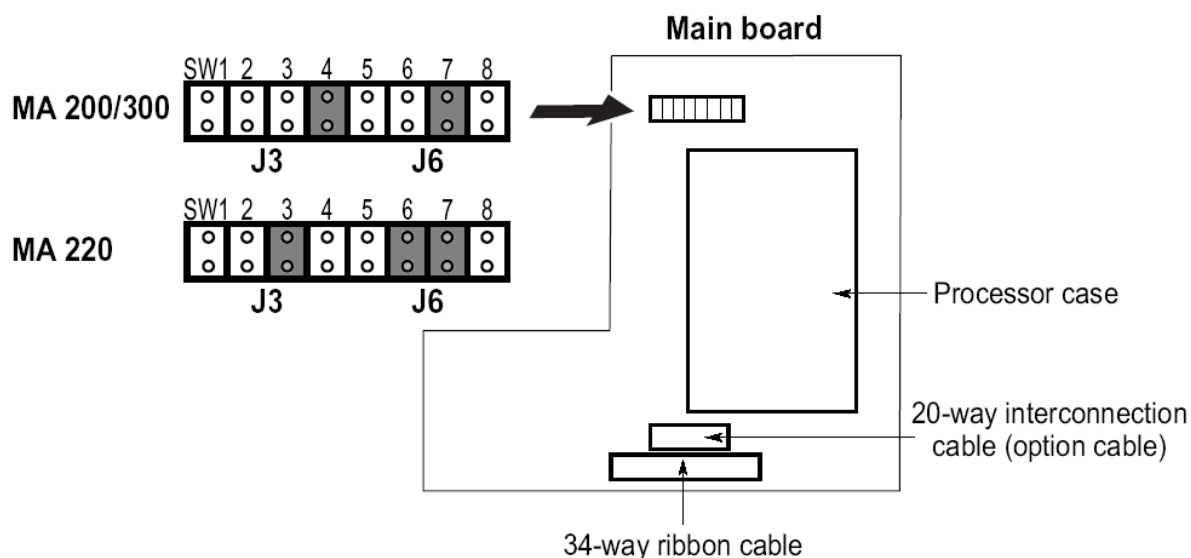
### Tamper-switch ratings

100 mA at 12 VDC max according to the safety extra low voltage.

### Anti-theft switch ratings

1 A at 30 VDC according to the safety extra low voltage requirements (42.4 VAC max, 60 VDC max) independently of the power supply.

## WIEGAND / DATALOCK: MOTHERBOARD CONFIGURATION



### SW1: Wiegand / Dataclock input

Open = Wiegand mode

**Closed** = Dataclock mode

### SW2: Wiegand / Dataclock output

Open = Wiegand mode

**Closed** = Dataclock mode

### SW3-6: Reserved (MA 200/300)

SW3 must be open

SW4 must be **closed**

SW5 must be open

SW6 must be open

### SW3-6: Reserved (MA 220)

SW3 must be **closed**

SW4 must be open

SW5 must be open

SW6 must be **closed**

### SW7-8: Wiegand / Dataclock input (Interruptions)

Open Open = Not allowed

Closed Open = Wiegand mode

Open **Closed** = Dataclock mode

**Closed Closed** = Not allowed

## USER INTERFACE

MorphoAccess™ terminal works upon three principles : Access control with identification, access control with authentication, and proxy mode.

These three principles consist in five functional modes :

- mode 0 : local identification (fingerprint capture) with a local base,
- mode 1 : authentication (ID receipt) and fingerprint capture with a local base,
- mode 2 : proxy mode; Command sending to the MorphoAccess™,
- mode 3 : authentication (contactless card reading minutiae) and fingerprint capture,
- mode 4 : authentication (contactless card reading ID) and fingerprint capture with a local base,
- mode 5 : modes 0 and 3, merged.
- Mode 6: authentication (keyboard ID) and fingerprint capture with a local base

The MorphoAccess™ 200 and 220 manages one base of 800<sup>(2)</sup> persons, locally or remotely. MorphoAccess™ 300 manages 16 bases of 3000 persons, remotely <sup>(3)</sup>.

---

2 In stand alone mode, the local base is sized for 800 persons, 2 fingers.

In MEMS mode, it is possible to manage up to 3000 persons in a base, 2 fingers.

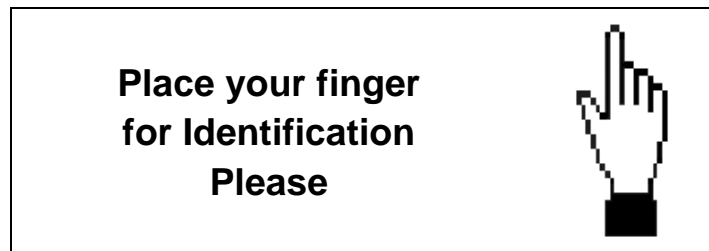
3 For more information, see *MorphoAccess Host System Interface Specification*.

## ACCESS CONTROL BY IDENTIFICATION (MORPHOACCESS™ 200)

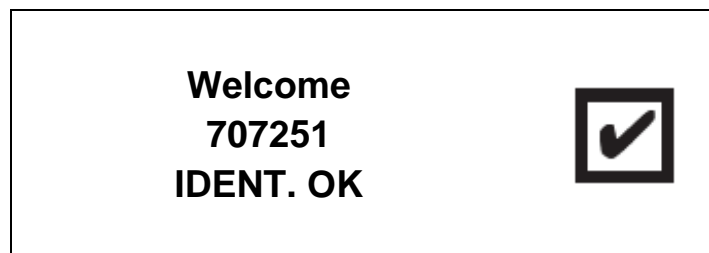
Identification mode	
<code>/cfg/Maccess/Admin/mode</code>	0

To configure MorphoAccess™ terminal in this mode, use the system menu and *edit /cfg/Maccess/Admin/mode*, then enter 0.

After starting the MorphoAccess™ terminal waits for fingerprint detection in identification mode.



If the identification is successful, the terminal triggers the access or returns the corresponding ID to central security controller<sup>4</sup>.



Once the person's identification is done, the terminal automatically loops back and waits for a new finger. This display remains for about 4 seconds.

---

<sup>4</sup> Port used to exchange ID is Wiegand/Dataclock or COM1/COM2 or Ethernet.

## ACCESS CONTROL BY IDENTIFICATION (MORPHOACCESS™ 300)

### Identification mode

`/cfg/Maccess/Admin/mode`

0

To configure MorphoAccess™ terminal in this mode, use the system menu and edit `/cfg/Maccess/Admin/mode`, then enter 0.

To select a user database, just press a key number to toggle the base number.

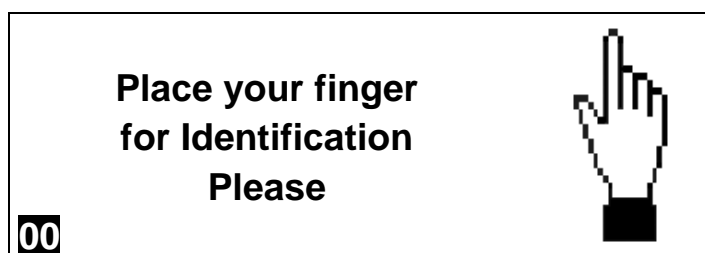
Only bases 0 to 15 can be selected and used.



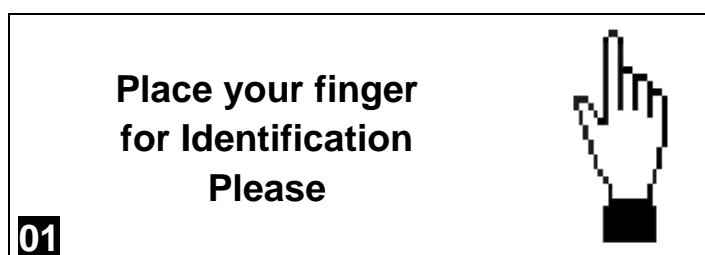
**5.4 version evolution. Old base selection style is no more available.**

To select base 0 to 9 simply press the corresponding key ('7' for base 7).

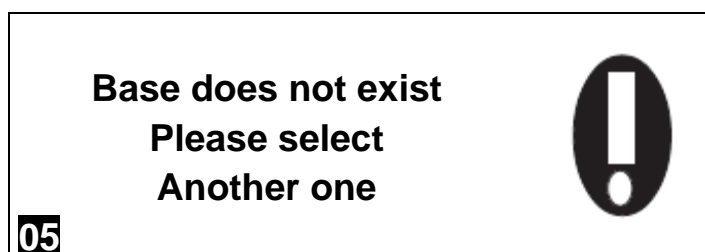
To select base 10 to 15, press '#' then the second digit. For example pressing '#' then '3' will select the 13<sup>th</sup> base.



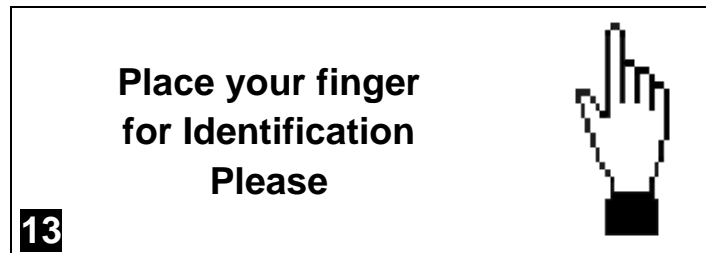
Key 1 pressed : now using base 1.



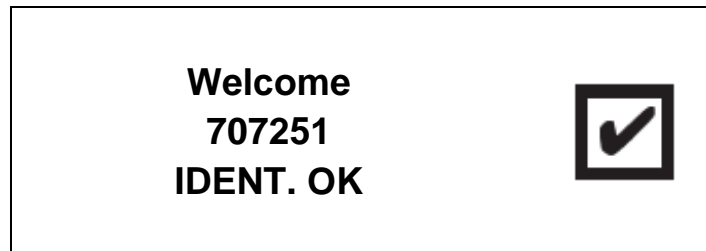
Key 5 pressed : now using base 5.



Key '#' then '3' pressed : now using base 13.



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



Once the person's identification is done, the terminal automatically loops back, selects base 0 and waits for a new finger. This display remains for about 4 seconds.

## ACCESS CONTROL BY AUTHENTICATION – ID SENT ON WIEGAND OR DATALOCK

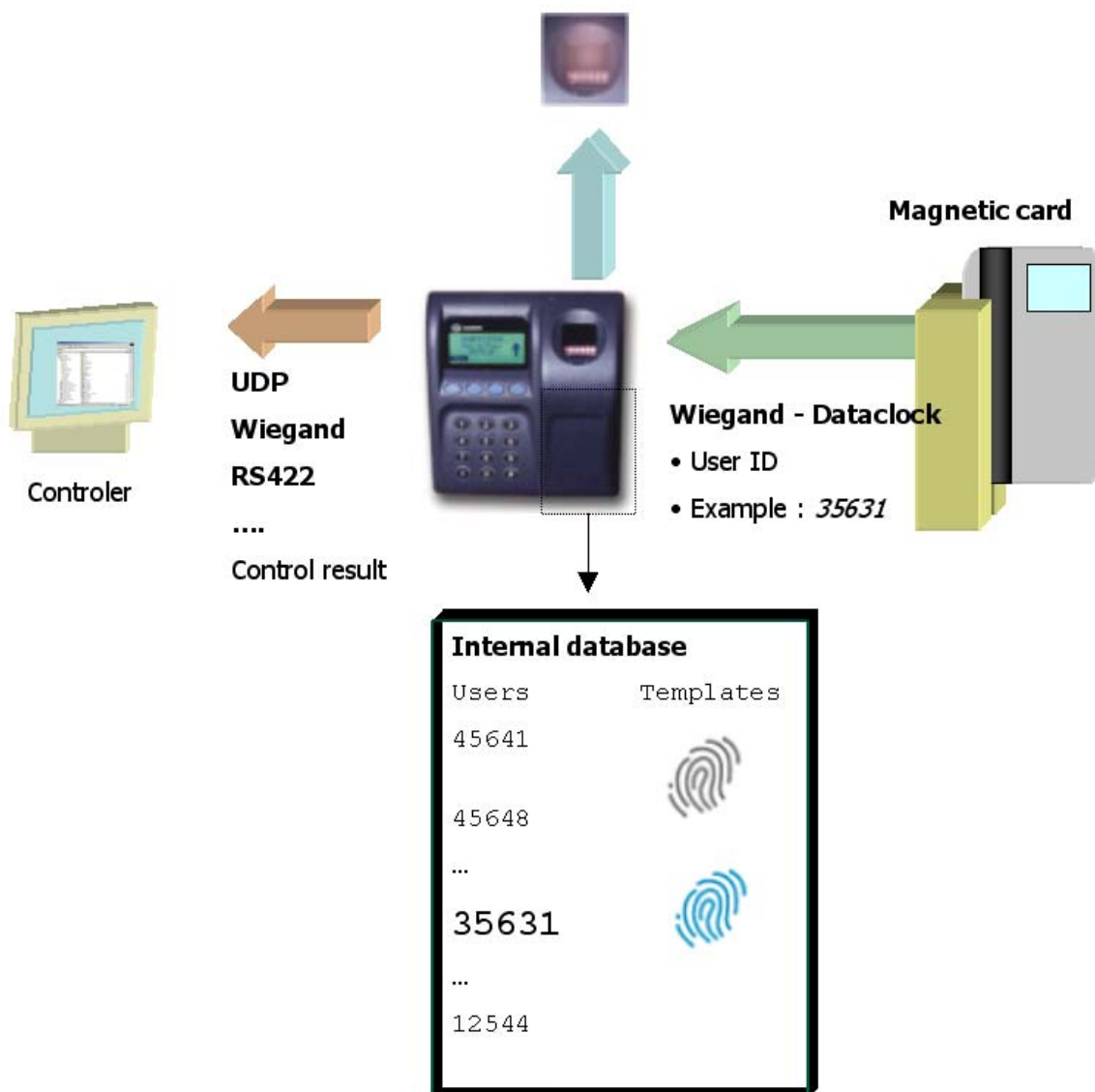
(MorphoAccess™ 200 and 300)

Authentication mode with local database

`/cfg/Maccess/Admin/mode`

1

This mode requires a peripheral equipment which will send the ID of the person to authenticate to the MorphoAccess™ Wiegand or Dataclock input.



**Pass your badge  
For Authentication  
Please**



To trigger authentication, pass the user badge so the external reader sends the user ID on MorphoAccess™ Wiegand or Dataclock input.



On MorphoAccess™ 300, the identifier is searched on every valid database (5.3 version).

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

**Authentication of  
92745  
Place your finger**



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

**Welcome  
92745  
AUTHENT. OK**



If the authentication fails a second attempt is possible without representing the card.

Once the person's authentication is done, the terminal automatically loops back, selects base 0 and waits for a new input ID. This display remains for about 4 seconds.

When using this feature with Wiegand input, ID should be a value between 0 and 65535.

## CONTACTLESS AUTHENTICATION WITHOUT DATABASE

Data (ID, name, templates, PIN, BIOPIN, card mode) on a MIFARE contactless card (MorphoAccess™ 220).

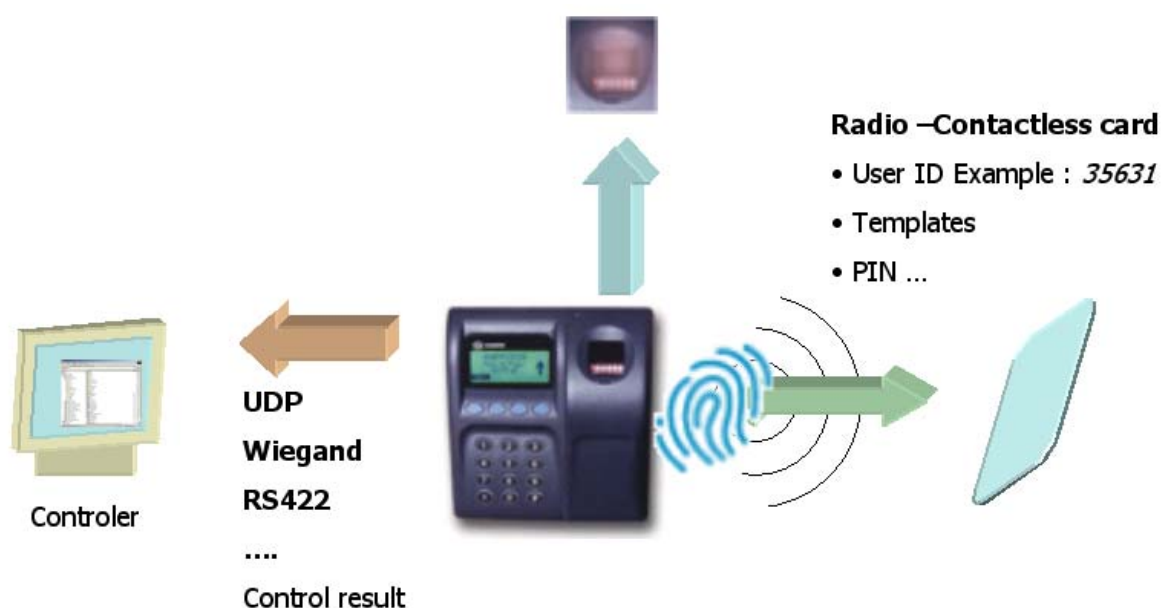
Data localization on the card may be specified. See section *Setting up contactless reader parameters* for more information.

Data are stored on the card according to the format detailed in the *Contactless card data structure (MorphoAccess 220 only)* section.

contactless authentication without database mode

`/cfg/Maccess/Admin/mode`

3



To configure the MorphoAccess in this mode, use Asystem and edit `/cfg/Maccess/Admin/mode`, then enter 3.

This mode divides into several sub modes.

If the authentication (or the PIN control) fails a second attempt is possible without representing the card.

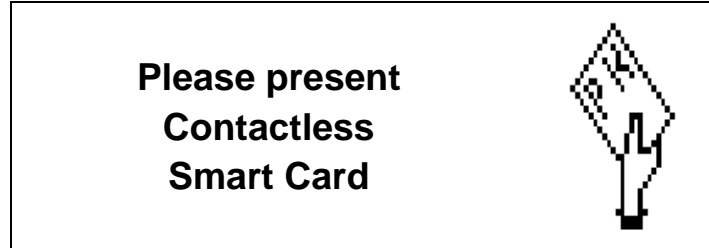
## ID only mode

Contactless authentication - ID only mode

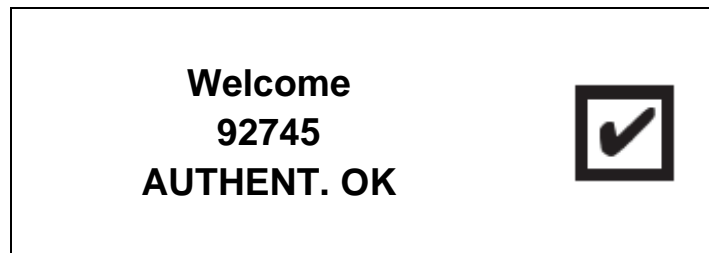
*/cfg/Maccess/Contactless/without DB mode*

1

In this mode the MIFARE card should contain the user ID.



So that MorphoAccess triggers the access or returns the user ID to the central security controller, user should just present his MIFARE card to the terminal.



## Templates or BIOPIN code mode

Contactless authentication - PK / BIOPIN mode

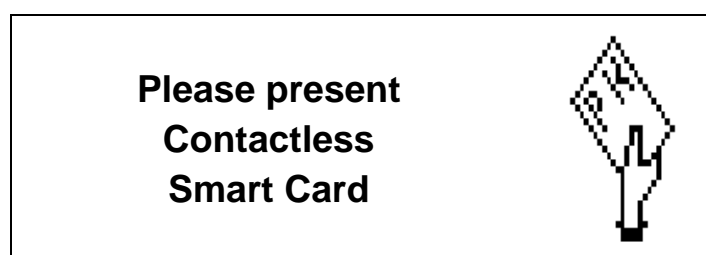
*/cfg/Maccess/Contactless/without DB mode*

2

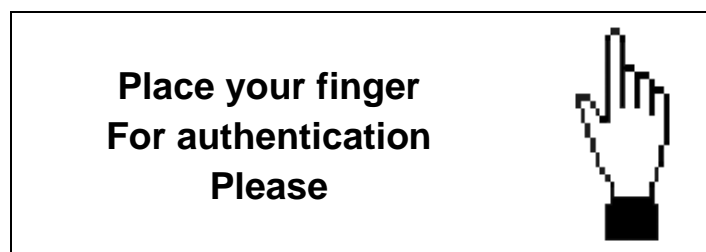
In this mode the MIFARE card should contain:

- User ID, name, and templates or,
- User ID, name and BIOPIN.

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



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



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



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



## PIN code mode

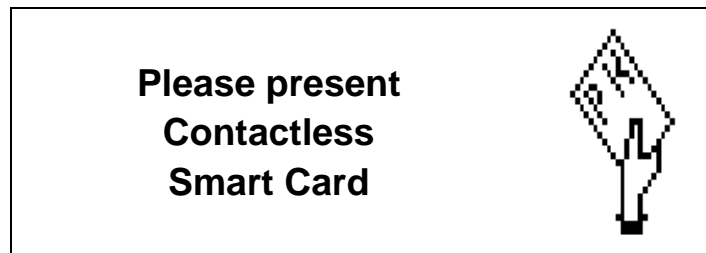
### Contactless authentication – PIN mode

*/cfg/Maccess/Contactless/without DB mode*

16

In this mode the MIFARE card should contain user ID, name, and PIN.

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



Then, user is invited to enter his PIN code.



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



## PIN code then templates or BIOPIN code mode

Contactless authentication – PIN – PK / BIOPIN mode

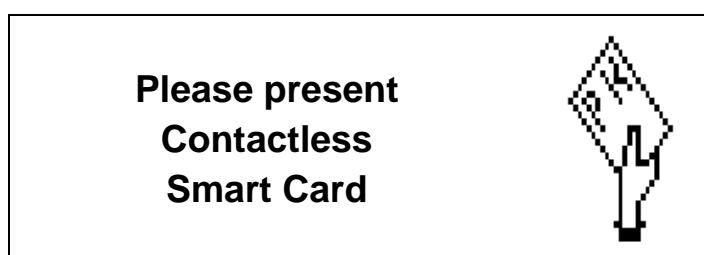
*/cfg/Maccess/Contactless/without DB mode*

18

In this mode the MIFARE card should contain :

- user ID, name, PIN, and templates or,
- user ID, name, PIN, and BIOPIN.

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

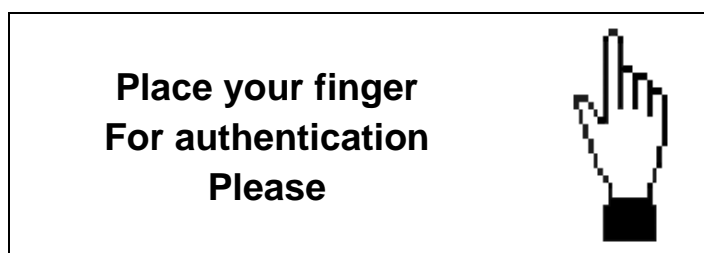


Then, user is invited to enter his PIN code.



If authentication is successful :

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



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



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



## Card defined mode

### Contactless authentication – card defined mode

*/cfg/Maccess/Contactless/without DB mode*

0

In this mode authentication method is not defined in advance but is set according to card mode data contained in the MIFARE card.

Possible modes are the same that the one described before (refer to previous paragraphs) and apart from card mode data, data requested are the same too.

Card mode value	Authentication method	Data requested (in addition to card mode data)
<b>1</b>	ID only	ID
<b>2</b>	Minutiae or BIOPIN	ID, name, templates or BIOPIN
<b>16</b>	PIN code	ID, name, PIN
<b>18</b>	PIN code then templates or BIOPIN code	ID, name, PIN, templates or BIOPIN

## CONTACTLESS AUTHENTICATION WITH : STANDARD CARD

ID on a MIFARE card, local templates (MorphoAccess™ 220).

Contactless authentication with database

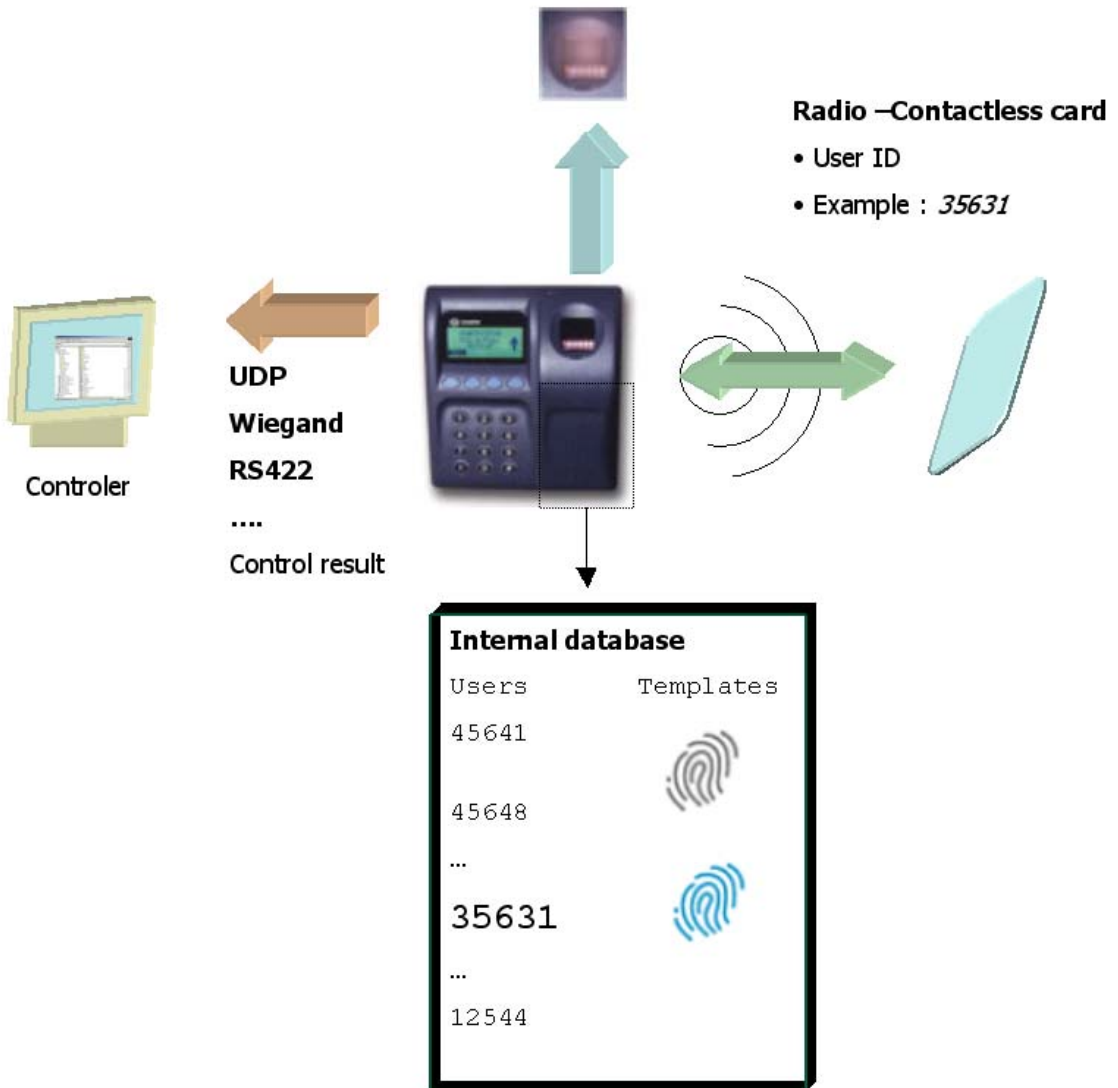
*/cfg/Maccess/Admin/mode*

4

Contactless authentication with database : id format

*/cfg/Maccess/Contactless/ID Format*

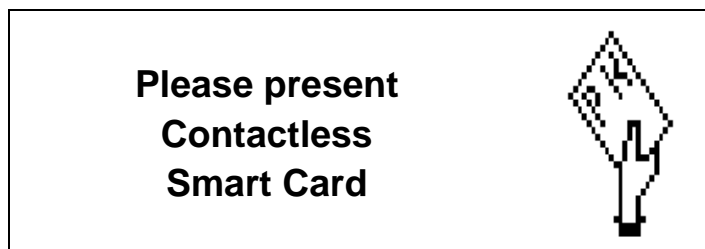
0



Data localization on the card may be specified. See section *Setting up contactless reader parameters* for more information.

Data are stored on the card according to the format detailed in the *Contactless card data structure (MorphoAccess 220 only)* section.

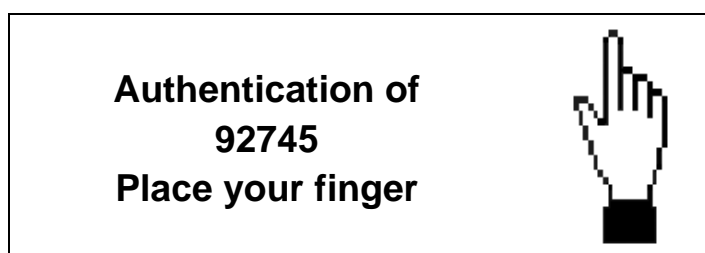
To trigger authentication, users should present their MIFARE card to the terminal. MorphoAccess™ will read the ID stored on the card.



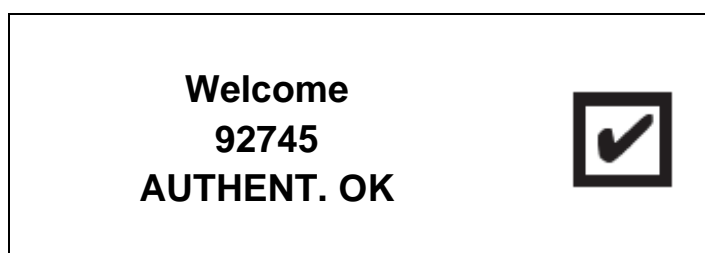
If the ID exists in the selected database, the MorphoAccess™ performs an authentication using the biometric templates associated to this ID.



On MorphoAccess™ 300, the identifier is searched on every valid database (5.3 version).



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



## CONTACTLESS AUTHENTICATION WITH DATABASE: BINARY ID

In this card the identifier is read at a given offset on the card and is supposed to be binary. This mode is useful for using the card serial number as an identifier.

### Contactless authentication with database

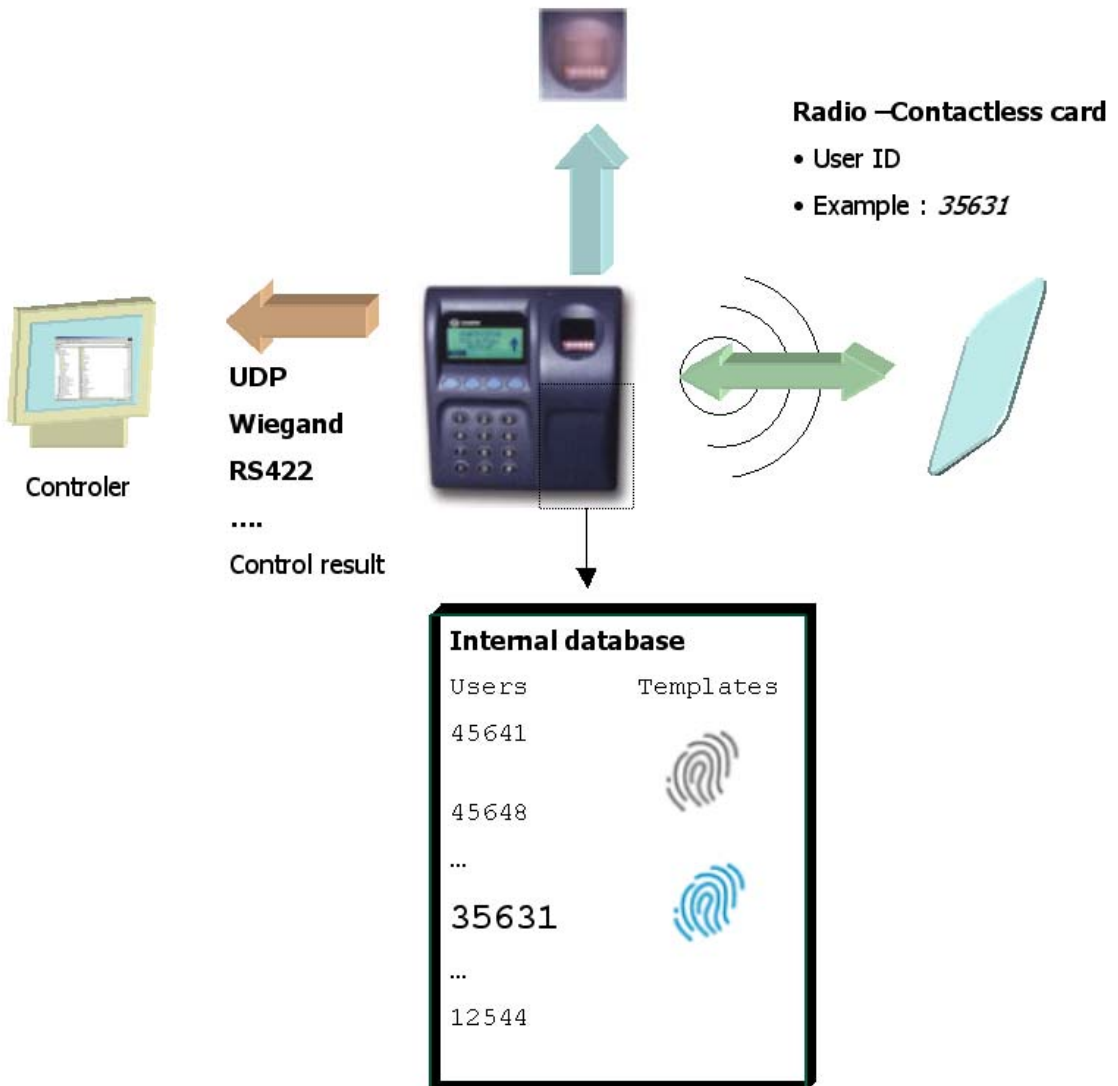
*/cfg/Maccess/Admin/mode*

4

### Contactless authentication with database: id format is binary

*/cfg/Maccess/Contactless/ID Format*

1



Contrary to the standard mode data are not stored in a structure.

Data localization on the card may be defined. See section *Setting up contactless reader parameters* for more information. The “block” notion is detailed in this section.

If the authentication fails a second attempt is possible without representing the card.

ID offset from first read bloc	
--------------------------------	--

<i>/cfg/Maccess/Contactless/ID offset</i>	[0-15]: ID offset in the first read block (B parameter).
---	--

ID size in bytes	
------------------	--

<i>/cfg/Maccess/Contactless/ ID size</i>	[1-8]: ID size in bytes
--	-------------------------

ID length in database is limited to 24 characters. It means that the binary ID length is limited to 8 bytes.

**Example:**

The ID on the card is the following:

A5 F4 98 C1 08 B1 or 182469953390769 in decimal format.

ID is stored under "182469953390769" in the database. ID format in the database is ASCII. The record ID must be:

"182469953390769"

=

0x31 0x38 0x32 0x34 0x36 0x39 0x39 0x35 0x33 0x33 0x39 0x30 0x37  
0x36 0x39.

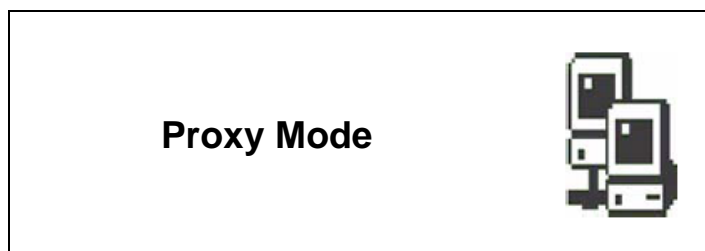
## PROXY MODE

### Proxy mode

`/cfg/Maccess/Admin/mode`

2

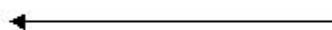
This mode allows controlling the MorphoAccess™ remotely using a set of biometric and databasing management function interface access commands.



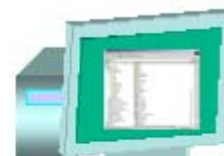
For more information, please contact SAGEM or refer to document *MorphoAccess Host System Interface Specification*.



MorphoAccess™



- ◆ RS232 RS422
- ◆ TCP IP



Host system

## MERGED MODE

### Merged mode

*/cfg/Maccess/Admin/mode*

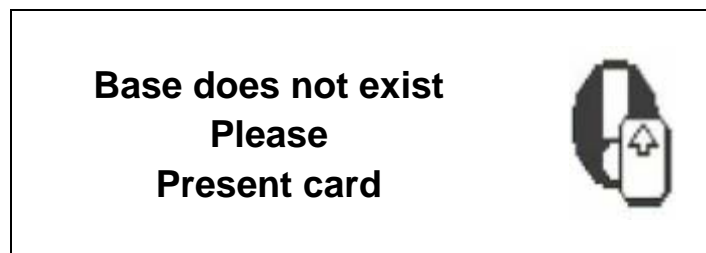
5

This mode is the fusion of identification mode (mode 0) and contactless authentication without database mode (mode 3).

So this mode allows to :

- run an identification if user places his finger (operation identical to identification mode),
- run a contactless authentication if user places his MIFARE card (operation identical to contactless authentication without database mode).

If there is no database, user is warned but MIFARE card presentation is still possible.



## AUTHENTICATION MODE WITH DATABASE: USING KEYBOARD ID

Mode «Authentication with ID entered on keyboard »

*/cfg/Maccess/Admin/mode*

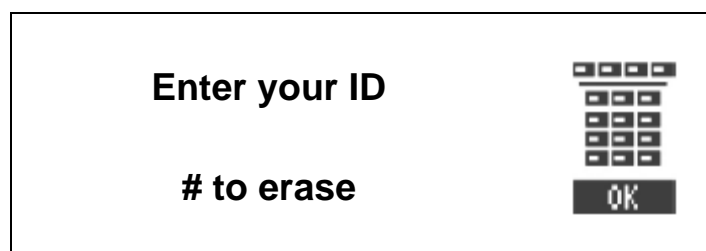
6

In this mode the ID of the person is entered on the MorphoAccess keyboard. If the ID exists in the local database, user is invited to place his finger for biometric authentication.

ID is entered using the keypad and the authentication starts

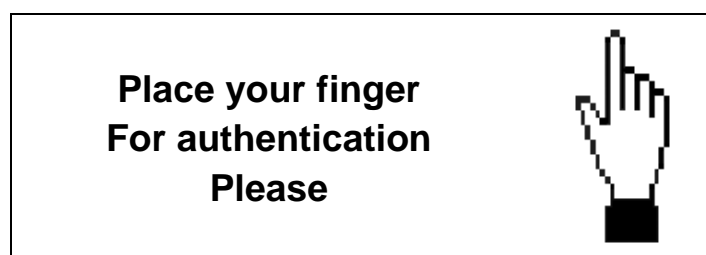


The default screen invites the user to enter his numerical identifier.



**Note:** ID length is limited to 24 numerical characters (the MorphoAccess key board is numerical).

Once the ID is entered, the user confirms with **F4** button.



If the user doesn't valid its ID after a 20 seconds timeout the ID is erased of the screen.

## SOFTWARE ADMINISTRATOR INTERFACE

Application of the SAGEM MorphoAccess™ terminal allows:

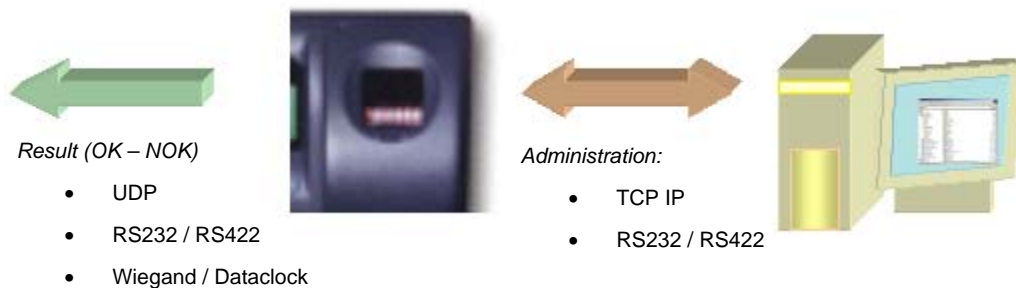
1. Biometric management operations:

- Transfer of biometric data between the MorphoAccess™ terminal and MorphoAccess™ Enrollment Management System (MEMS).
- In stand alone without the MorphoAccess™ management system (manages the biometric data in a local database on the MorphoAccess™) (MorphoAccess™ 200 only).
- The MorphoAccess™ shall be configured in one of either of these modes (see this chapter).

2. Access to the set up functions of the system (request Administrator mode).

*Note*

The MEMS handles the MorphoAccess™ through a set of command exchanges (two-way commands to and from the MEMS server and the MorphoAccess™ terminal). If you wish to know more about this protocol and the command set, please refer to *MorphoAccess Host System Interface Specification*.



## BIOMETRIC MANAGEMENT OPERATIONS

### Biometric Management between terminal and MorphoAccess™ Enrollment Management System (MEMS)

MorphoAccess™ terminal includes an interface layer to communicate with the access control system or the MEMS through Ethernet, RS422 and RS232.

The biometric management operations are:

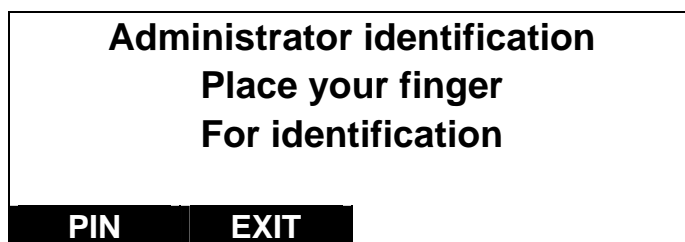
- Insert template/ID in database: The terminal inserts a new record in the database.
- Remove template/ID from database: The terminal removes the record identified by the ID in the database.
- Update template/ID in database: The terminal changes the template identified by the ID in the database.
- Download database: The terminal reads the new database and installs it in a local database according to the database identifier.

If the MorphoAccess™ application receives the commands from MEMS it will switch to base management mode. The operations sent by MEMS are automatically registered in the database of the MorphoAccess™ terminal.

Managing a base locally is not possible. All biometric data is stored on the MEMS and the terminal will act as a capture and send device only.

To access the Administrator menu with a MorphoAccess™ 300, first select the base in which the Administrator is enrolled then hit the following keys in sequence <#>, <\*> and <#>.

With a MorphoAccess™ 200 simply hit the following keys in sequence <#>, <\*> and <#>.



Biometric login is enabled if configuration key `/cfg/Maccess/admin/admin ident` is set to 1.

This operation creates a database with ID 0. This database can contain 800 records with two biometric data fields, an ID field and, if the Biometric login is enabled, an Administrator field.

In order to access the **Control menu**, the Administrator's fingerprint template or pin code must be entered. To enter the pin code, select the **PIN** menu.

Note : It is advised to change this pin code as early as you receive the terminal (see System and admin passwords)

You can use the correction key # to delete the last number hit. The PIN code can be changed in the configuration file `/cfg/Maccess/Admin` (see section MorphoAccess Administrator Pin page 57).

Note: It is advised to change this pin code as early as you receive the terminal

<b>Administrator identification</b>	
Enter PIN: **	
<b>OK</b>	<b>EXIT</b>

After a valid pin code or administrator identification, you will see the following screen:

<b>Administrator Mode</b>			
<b>Select a command please</b>			
<b>SYSTEM</b>	<b>EXIT</b>	<b>CL KEYS</b>	<b>MORE</b>

## Biometric management in stand-alone mode

*(MorphoAccess™ 200 only)*

In stand-alone mode, the MorphoAccess™ manages its own local database. This can be setup through the Administrator menus. On the keypad, hit the following keys in sequences `<#>`, `<*>` and `<#>`. The resulting screen is the **Administrator** menu.

<b>Administrator identification</b>	
<b>Place your finger</b>	
<b>For identification</b>	
<b>PIN</b>	<b>EXIT</b>

Biometric login is enabled if configuration key `/cfg/Maccess/admin/admin ident` is set to 1.

This operation creates a database with ID 0. This database can contain 800 records with two biometric data fields, an ID field and an Administrator field.

<b>Administrator identification</b>	
Enter PIN: **	
<b>OK</b>	<b>EXIT</b>

If the identification is successful, the application allows access to the biometric management functions. The biometric management operations are:

- Insert template/ID in database (enrolment): The terminal inserts a new record in the database.
- Remove template/ID from database (deletion): The terminal removes the record identified by the ID in the database.

<b>Administrator Mode</b>			
<b>Select a command please</b>			
<b>ENROLL</b>	<b>DEL</b>	<b>ERASE</b>	<b>EXIT</b>

## Insert template/ID in database

*(MorphoAccess™ 200 only)*

To insert template/ID in local database, select the **ENROLL** menu. You have to enter the ID of the person and validate it. The primary and secondary fingers are requested and their corresponding biometric templates are processed. If the process is successful, then the person is registered in the local database.

<b>Enrollment Mode</b>	
Enter Person ID :	
Press <#> for correction	
<b>OK</b>	<b>CANCEL</b>

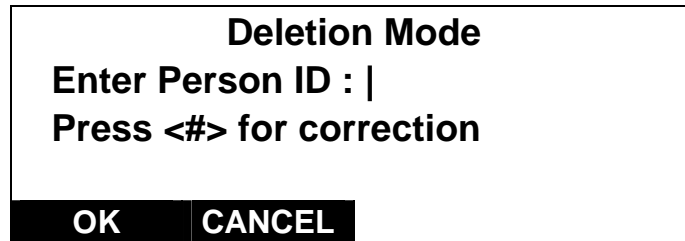
You can use the correction key # to delete the last digit entered. In the next screen you enroll your finger. The enrolled person may be either a “simple” user or an administrator.

## Remove template/ID from database

*(MorphoAccess™ 200 only)*

To remove a single template/ID record from the database, select the **DEL** menu. You will then have to enter the ID of the person and validate it. If

the ID number does not exist in the local database, an error message appears.

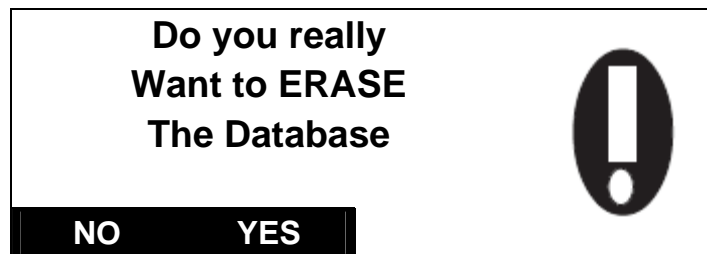


You can use the correction key # to delete the last digit entered.

## Remove all template/ID from database

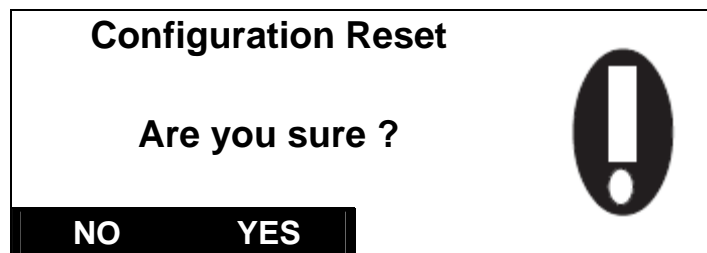
*(MorphoAccess™ 200 only)*

To remove all records from the local MorphoAccess™ database, select the **ERASE** menu option. A screen appears to confirm your command.



## Reset configuration to factory settings

To reset configuration to factory settings, select the **RST CFG** menu option. A screen appears to confirm your command



**Remark:** Network parameters will be kept.

**Remark:** System will reboot.

Warning about the “/cfg/Maccess/contactless/Reader Type” key MA220). This command reset the value of the “Reader type” key, it means that the MA220 restart as a MA200. Then the original value of the key (usually “2”), must be restore manually and the MA restarted to be again a MA220.

## Warm-up reset

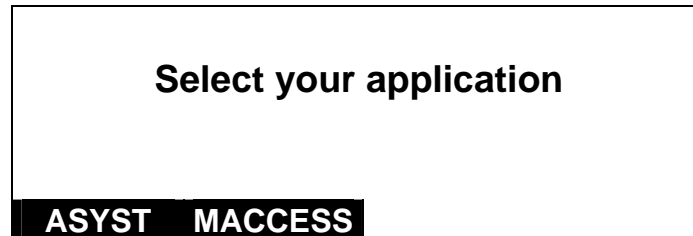
In order to update the modified parameters, it is necessary to reset the MorphoAccess™ terminal.

In the main menu of the administrator mode, with **MORE** key select the **REBOOT** key.

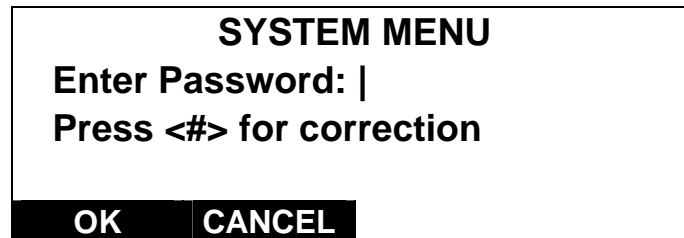
*/cfg/Maccess* parameters are updated immediately, and reboot action is unnecessary.

## ACCESS THE SET UP FUNCTIONS OF THE SYSTEM

To access the **System Menu**, you must leave the main application of the MorphoAccess™. You must access the Administrator Menu and select the **EXIT** key. It is possible to select the **ASYST** application or go back to the standard application (**MACCESS**).



Then, select the **ASYST** menu to enter in the system application



Enter the password to access to **SYSTEM MENU** (default value: "12345").

You can use the correction key # to delete the last digit entered. The password can be changed in the configuration file */cfg/system* (see section *MorphoAccess™ System Administrator Pin* page 59).

Note: It is advised to change this password as early as you receive the terminal

The **System Menu** will appear when the password is correct.

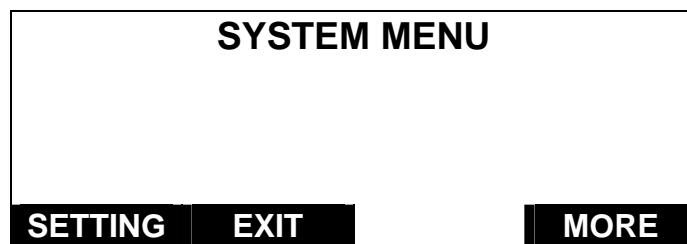


The **CONFIG** menu allows you to set up network and specify additional parameters.

The **VERSION** item allows you to browse for software modules present in your SAGEM MorphoAccess™ and see their revision number(s).

The **SER NB** item displays the terminal serial number, MicroBoot revision and Ethernet physical address of your machine.

The **MORE** key displays the rest of the system options.



The **SETTING** menu allows you to set the LCD contrast and the time and date.

## CONFIGURATION MENU

This menu allows modifying MorphoAccess™ parameters.

These parameters are stored as configuration key with the following structure: “*file/section/parameter/value*”.

They can be edited directly using the keyboard.

<b>FILE: cfg/net</b> <b>SECTION: ip</b> <b>Address: 134.1.32.214</b>			
<b>PREV</b>	<b>NEXT</b>	<b>EXIT</b>	<b>EDIT</b>

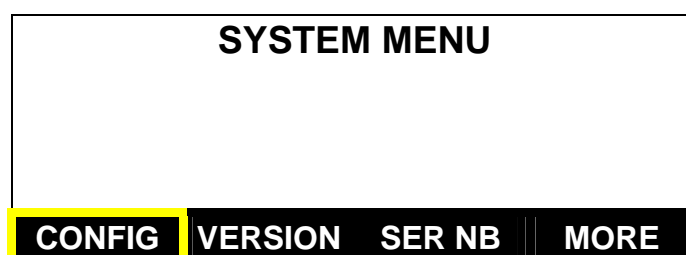
The *How to edit parameters? network parameters* section page 57 explains how to edit a value.

Some parameters are reserved and must not be changed.

## HOW TO EDIT PARAMETERS? NETWORK PARAMETERS EXAMPLE

Network Parameters
<i>/cfg/net/ip/address</i>
<i>/cfg/net/ip/default gateway</i>
<i>/cfg/net/ip/subnet</i>

In the **System** menu press the **CONFIG** key to access the configuration files.



*File selection:*

Press the **NEXT** key until the **File** menu displays */cfg/net*.

*Section selection :*

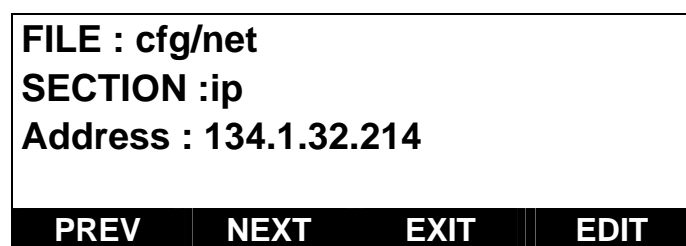
Press the **EDIT** key. The **Section** menu displays *ip*.

*Parameter selection :*

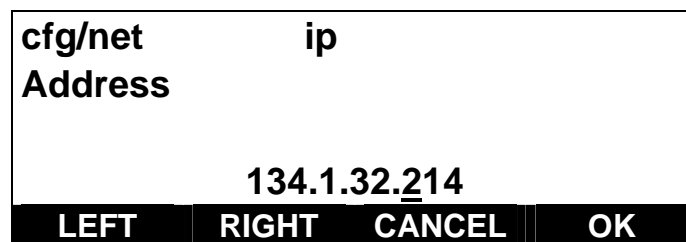
Press the **NEXT** key until *address* is displayed then press the **EDIT** key.

*Go to previous selection:*

Use the **EXIT** key.



You can now edit you MorphoAccess™ IP address.



The **LEFT** and **RIGHT** keys move the cursor.

The alphanumeric keys enter digits as necessary. The # key deletes the digit immediately to the left of the cursor. The **EXIT** key aborts editing and restores the previous address value.

The IP subnet mask and IP default gateway are set up in the same way. Contact your network Administrator for these values.

## SYSTEM AND ADMIN PASSWORDS

### MorphoAccess™ System Administrator Pin

System Administrator Pin	
<i>/cfg/system/System/Pwd</i>	« 12345 » default

This password restricts access to “system application”.

Default value is « 12345 ».

<b>FILE: cfg/system</b>			
<b>SECTION: System</b>			
<b>Pwd: 12345</b>			
<b>PREV</b>	<b>NEXT</b>	<b>EXIT</b>	<b>EDIT</b>

### MorphoAccess™ Administrator Pin

Administrator Pin	
<i>/cfg/Maccess/Admin/PwdAdmin</i>	« 12345 » default

This password restricts access to “Admin mode”.

Default value is « 12345 ».

<b>FILE: cfg/Maccess</b>			
<b>SECTION: Admin</b>			
<b>Pwd: 12345</b>			
<b>PREV</b>	<b>NEXT</b>	<b>EXIT</b>	<b>EDIT</b>

## SETTING UP HOST COMMUNICATION.

Communication mode		
<i>/cfg/Maccess/Admin/Host Com</i>	0	Stand alone
	1	Connected through COM1
	2	Connected through COM2
	3	Connected through ETHERNET

This parameter allows management of a local database within the MorphoAccess™ using a remote station or with local facilities.

```

FILE : cfg/Maccess
SECTION :Admin
Host Com : 3

PREV | NEXT | EXIT | EDIT
  
```

The default value of Host Com key is 3 (MEMS). In this case, the biometric management is between terminal and MorphoAccess™ Enrollment Management System (MEMS).

To configure the MorphoAccess™ terminal to manage the local database, this default value must be changed to 0.

COM1 or COM2 mean serial link administration.

You cannot use the stand-alone mode to manage your local database if the MorphoAccess™ biometric data is managed by the MEMS.

The MorphoAccess™ shall be used either in stand-alone mode or in connected mode (with MEMS) but never in both modes.

Configuring the key to 0 will disable MEMS connection.

For more information about commands accepted by the terminal please refer to *MorphoAccess™ Host System Interface*.

## SETTING UP MATCHING PARAMETERS

### Setting up juvenile recognition

Setting up juvenile recognition		
<i>/cfg/Maccess/bio/juvenile</i>	0	Disabled (default)
	1	Enabled

Since software release 2.0, the MorphoAccess™ is able to manage both juvenile and adult finger images.

```

FILE : cfg/Maccess
SECTION :bio
juvenile : 0

```

<b>PREV</b>	<b>NEXT</b>	<b>EXIT</b>	<b>EDIT</b>
-------------	-------------	-------------	-------------

This provides a solution with reliable performance to the automatic processing of finger images with small to normal ridges, extending the capability of the terminal by providing access control to a wider range of population.

Since the encoding time is a little bit longer when the juvenile option is turned on, we offer the possibility to the user set up the terminal either in "Juvenile" mode or in standard mode.

When the juvenile mode is turned on, key set to 1, young children can easily be enrolled in the MorphoAccess™.

### Setting up anti-latency

Setting up anti-latency		
<i>/cfg/Maccess/bio/anti latency</i>	0	Disabled (default)
	1	Enabled

The anti-latency processing consists to filter marks left on the sensor. In some extreme conditions it is possible that a mark left on the sensor triggers an identification or verification.

From the 4.4 release of MorphoAccess firmware it is now possible to filter marks left on the sensor.

```

FILE : cfg/Maccess
SECTION :bio
Anti Latency : 0

PREV | NEXT | EXIT | EDIT

```

When the MorphoAccess detects a mark the identification is stopped and the application loops back and look for a new fingerprint.

With regards to the previous releases of the MA application the main change is that a fingerprint placed two consecutive times on the sensor in the same position will be rejected from the second attempt.

When the anti-latency mode is turned on, key set to 1, latent fingerprint marks will not trigger identification or verification.

## Setting up recognition mode

A typical identification workflow may be composed of two steps:

- The MorphoAccess™ terminal proceeds to a first fast identification (using a "light" coding method).
- If the user is not identified, a second step follows immediately using a smarter coding method ("gabor" coding). 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.

In order to optimize biometric control it is possible to determine how these coding methods will be linked. These parameters may be adjusted in the *cfg/Maccess/Bio* section.

### Coding selection

The *cfg/Maccess/Bio/identification strategy* parameter allows determining the identification strategy.

```

FILE : cfg/Maccess
SECTION :bio
identification strategy: 2

PREV | NEXT | EXIT | EDIT

```

Three modes may be selected:

- 0:[*Light only*]

Gabor coding is disabled. The control is faster in any case (identification succeeded or not).

This setting is advised for users familiarized with biometric control and in standard conditions of use.

- 1 : [*Light then gabor*] (default mode for older versions (<5.2))

Identification will proceed in two steps like described in the previous paragraph. Light coding, and in case of failure gabor coding.

Some identifications are slower but chances of success are increased.

- 2: [*Advanced mode: light coding then gabor on the second try*] (default mode)

In this mode gabor coding is disabled. Like in the [*Light only*] mode the answer of the control is immediate.

Unlike the mode [*Light only*], in case of failure, the gabor coding will be reactivated for the immediate next control to increase chances of success for a second try.

After a given time of inactivity or after a second failure the terminal automatically switches in the [*light only*] mode. This period may be modified.

### Coding duration

```

FILE : cfg/Maccess
SECTION :bio
advanced timeout: 2
    
```

<b>PREV</b>	<b>NEXT</b>	<b>EXIT</b>	<b>EDIT</b>
-------------	-------------	-------------	-------------

The *cfg/Maccess/Bio/advanced timeout* parameter allows setting in seconds the period while the gabor coding will be activated when the terminal is set in [*Advanced mode*] mode.

- 0: If the light identification failed, the terminal will be temporarily switched in the [*light then gabor*] mode. After this second identification the terminal is in [*light only*] mode.
- 1-3600: This value determines (in seconds) how long the terminal will activate the [*light then gabor*] mode if no finger is presented on the sensor. After this period it switches automatically in [*light only*] mode.

Default value is 5 seconds.

When the terminal switches in "light only" mode the sensor will briefly flash.

Recognition mode (light, gabor ...)	
<i>/cfg/Maccess/bio./</i>	
<i>identification strategy</i>	0 Light only 1 Light then gabor (default)

	2 Advanced mode
<i>advanced timeout</i>	[1-3600] seconds 5 seconds is the default value

## Matching threshold

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

Identification and authentication thresholds may be defined independently.

*Identification mode:*

<b>FILE : cfg/bio</b>			
<b>SECTION : matching threshold</b>			
<b>identify: 3</b>			
<b>PREV</b>	<b>NEXT</b>	<b>EXIT</b>	<b>EDIT</b>

*Authentication mode:*

<b>FILE : cfg/bio</b>			
<b>SECTION : matching threshold</b>			
<b>Authenticate : 3</b>			
<b>PREV</b>	<b>NEXT</b>	<b>EXIT</b>	<b>EDIT</b>

This parameter can be set to values from 0 to 10. This parameter specifies how tight the matching threshold is. Threshold scoring values are identified hereafter

0	Low threshold for test purpose only	There are few rejections, but many recognitions
1	Very few persons rejected	FAR < 1%
2		FAR < 0.3%
<b>3</b>	<b>Recommended value</b> (default 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 few recognitions, and many rejections

## USER INTERFACE SETTINGS

### Multilingual application

#### Language

The MorphoAccess™ can operate using other language than English. It can also operate in eight other 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*.

The default language of the MorphoAccess™ is defined in the */cfg/Maccess/Language/default*.

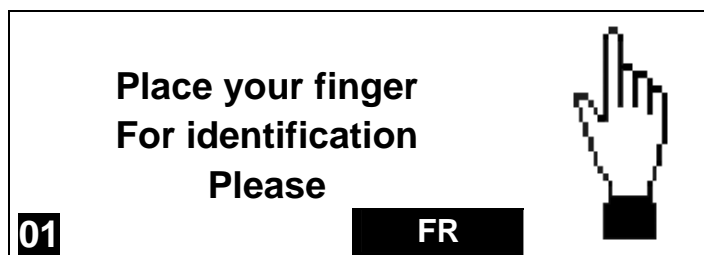
The allowed values are:

Default language	
<i>/cfg/Maccess/Language/default</i>	0 English (default)
	1 Spanish
	2 French
	3 German
	4 Italian
	5 Portuguese
	6 Language6
	7 Language7
	8 Language8
	9 <b>User defined language</b>

**Caution: In the MorphoAccess 5.41 the User defined language is the number 9, instead of 3 in anterior versions.**

#### Language selection

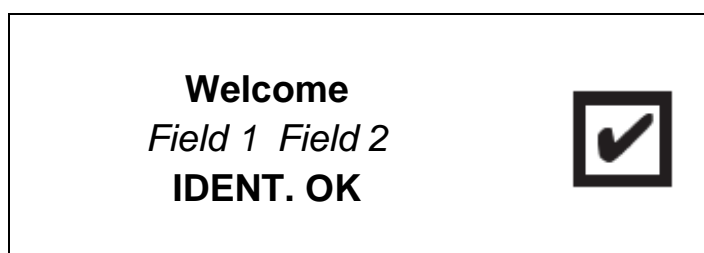
A user may choose his language by pressing a button. The language choice is circular.



Language selection	
<i>/cfg/Maccess/G.U.I./change</i>	<p>0 The change language button is disabled. Users cannot change their language.</p> <p>1 Users can choose their language using the change language button.</p>

## Identification information

On a positive identification, it is possible to display information about the identified user. This information should be present in the additional fields of its record.



The allowed values are:

Identification information (local database)	
<i>/cfg/Maccess/G.U.I./</i>	
<i>Welcome Field 1</i>	<p>0 Nothing is displayed.</p> <p>1 System displays ID of identified person.</p> <p>X System displays data present in additional field number X of identified person.</p>
<i>Welcome Field 2</i>	<p>0 Nothing is displayed.</p> <p>1 System displays ID of identified person.</p> <p>X System displays data present in additional field number X of identified person.</p>

Example:

First and second additional field have been selected. They contain first and family name of all records present in the database. On identification, system will display the following screen:



This feature needs a database containing the appropriate additional fields.

## Clock

When using time mask feature, users may find useful to synchronize with their MorphoAccess™. A clock can be displayed.



Time is displayed in the 24 hours format.

Display hour	
<i>/cfg/Maccess/G.U.I./display hour</i>	0 Clock is not displayed. 1 Clock is displayed and refreshes every minute.

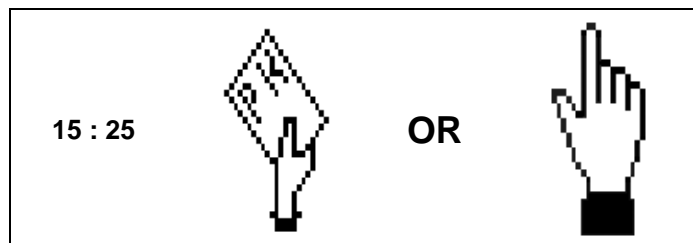
## Idle mode

In identification mode it is possible to switch the MorphoAccess™ in idle mode in order to shut down sensor red light and green screen back light. Pressing a key wakes the MorphoAccess™ up.

Idle mode settings	
<i>/cfg/Maccess/G.U.I./idle timer in min</i>	0 MorphoAccess™ never enters idle mode. n MorphoAccess™ enters idle mode after n minutes.

## DISPLAY PERSONALIZATION

The MorphoAccess™ offers a full graphic mode. Three different appearances may be selected.



Each appearance may be user-redefined. Please refer to *MorphoAccess Screen Customization* for more information.

With this feature it is possible to create non-Latin information messages.

Graphic mode activation	
<i>/cfg/Maccess/BMP mode /</i>	
<i>enabled</i>	0 Display uses graphic and text (default and historical mode). 1 Display uses bitmaps. Bitmaps are contained in files <i>picto0.bin</i> , <i>picto1.bin</i> or <i>picto2.bin</i> . They are customizable.

File selection	
<i>/cfg/Maccess/BMP mode /</i>	
<i>file</i>	0 <i>picto0.bin</i> (default) 1 <i>picto1.bin</i> 2 <i>picto2.bin</i> .

Note: see the document *MorphoAccess Screen Customization Guide V2.0.pdf* to know the modifications of the Bitmap tool

## SETTING UP CONTACTLESS READER PARAMETERS

(MorphoAccess™ 220 only)

A MIFARE card is defined by a unique serial number.

- The card is divided in 16 sectors.
- Each sector is divided in 4 blocks.
- Each block contains 16 bytes of data.
- Data are encoded with two sets of key.

To be able to read a card, the reader should use the same key set. Fourth blocks cannot be read, they are used to store key sets.

Data can be accessed by blocks as follows:

	Block 0	Block 1	Block 2	Block 3
<b>Secteur 0</b>	Block 1	Block 2	Block 3	
<b>Sector 1</b>	Block 4	Block 5	Block 6	
...				
<b>Sector 15</b>	Block 46	Block 47	Bloc 48	

Blocks are numbered in an absolute way, 1 for block 0 sector 0, then 3 blocks for each sector.

SAGEM biometric data (ID, name and templates) are located on the card thanks to a **BNC** address where:

- <B> is the first block number to read,
- <N> is the number of blocks to read,
- <C> selects a security key.

Data are described in *Contactless card data structure (MorphoAccess 220 only)* section and in document *MorphoAccess™ Host System Interface Specification*.

With a MorphoAccess™ 220, contactless parameters can be defined from the CONFIG menu in file /cfg/Maccess, in section Contactless.

Reader type (MA220)	
<i>/cfg/Maccess/contactless/</i>	
<i>Reader type</i>	0 No MIFARE reader is used. 1 External MIFARE 2 Deister reader is used. Internal MIFARE reader is used.

**Warning** : the value of this key is set to 0 (zero) by the ILV command « Default\_Init » and by the « RST CFG » action of the Administrator mode.

First block number to read	
<i>/cfg/Maccess/contactless/B</i>	4 (default) to 13

Number of blocks to read (form B)	
<i>/cfg/Maccess/contactless/N</i>	2 When an ID is stored. 28 When templates are stored.

Security key	
<i>/cfg/Maccess/contactless/C</i>	1 MIFARE security key A then B is selected (default) 2 MIFARE security key A is selected. 3 MIFARE security key B is selected.

## LOG FILE

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

Those configuration keys can be defined from the **CONFIG** menu in file */cfg/Maccess*, in section Admin.

The allowed values are:

Log activation	
<i>/cfg/Maccess/Admin/Log file</i>	0 MorphoAccess™ is not logging its activities.
	1 MorphoAccess™ is logging its activities.

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

## SETTING UP TIME MASK

When using MEMS commands, 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. For more information, see *MorphoAccess Host System Interface Specifications*.

Time mask activation	
<i>/cfg/Maccess/Admin/Time mask</i>	<p>0 Time mask feature is disable (default).</p> <p>1 Time mask feature is enabled. Users must be on time to have their access granted..</p>

## SETTING UP DOWNLOAD AGENT - (SDL)

In order to upgrade the MorphoAccess™ terminal to future versions, a download agent is running. This agent allows connecting to the terminal and proceeding maintenance operations. For more information about the protocol used to communicate with this agent, please contact your SAGEM sales representative.

SDL activation	
<i>/cfg/sdl/Download/Active</i>	0 Inactive 1 SDL commands are allowed (default)

Password to present in order to connect the agent (8 digits)	
<i>/cfg/sdl/Download/Password</i>	« 12345678 » (default)

**Remark:** the password must contain exactly 8 digits.

Number of failed attempts before deactivating the agent.	
<i>/cfg/sdl/Download/Ratif</i>	3 (default)

## WIEGAND / DATALOCK CONFIGURATION

### Note

The terminal may send or receive either Dataclock frames or Wiegand frames. The mode depends on hardware configuration described in the **Wiegand / Dataclock hardware** section.

You can use the output Wiegand or Dataclock to send the corresponding ID to the central security controller. Wiegand ports are configured in 26-bit format and Dataclock ports are compatible with ISO track 2 data formats.

I/O Dataclock are ISO2 compliant.

In Wiegand mode, ID is sent in binary format.

In Dataclock mode, ID is sent in BCD format.

### Wiegand / Dataclock : ID sending

The ID of the recognized user may be send on Wiegand or Dataclock output.

Please refer to *MorphoAccess Remote Messages Specifications* for more information about this functionality.

Sending ID Wiegand or Dataclock	
<i>/cfg/Maccess/Wiegand/dataclock/</i>	
<i>send</i>	0 ID is not sent (default) 1 ID is sent

## Wiegand / Dataclock : advanced informations

Specific ID may be defined for various error cases. They can be set between 0 and 65535.

Error ID definition	
<i>/cfg/Maccess/Wiegand/dataclock/</i>	
<i>Send failure ID</i>	0 Identification error action: Inactive (default) 1 Identification error action: Active
<i>Not in time ID</i>	[0 65535 (default)] Time mask Identification error
<i>Not in dB ID</i>	[0 65535 (default)] Identification error for unknown person in base (mode 4)
<i>Not ident ID</i>	[0 65535 (default)] Identification error for not identified person
<i>TimeOut ID</i>	[0 65535 (default)] Identification error for authentication time-out
<i>Error ID</i>	[0 65535 (default)] Identification error for other cases

## Wiegand : facility code

This code may be set between 0 and 4294967295, depending on Wiegand data format (see section *APPENDIX 2 - WIEGAND DATA FORMAT* page 107).

Installation Code (« facility code »)	
<i>/cfg/Maccess/Wiegand/dataclock/</i>	
<i>Facility code</i>	7 (default) [0 4294967295]

« **Wiegand IN** »

Facility code is checked on input frames.

« **Wiegand OUT** »

Facility code is copied on output frames.

## Wiegand : facility code verification

It is possible to accept frame with any facility code.

Site code verification	
<i>/cfg/Maccess/Wiegand/dataclock/</i>	
<i>pass through mode</i>	0 Facility code is checked (default) 1 Facility code is ignored

## Dataclock : Data and Strobe levels

To configure the Data and Strobe levels in Dataclock(14) mode, you must select the Dataclock level key in section *cfg/Maccess/Wiegand/Dataclock*.

Dataclock level	
<i>/cfg/Maccess/Wiegand/dataclock/</i>	
<i>Dataclock level</i>	0 Data and strobe are not inverted (default). 1 Strobe is inverted. 2 Data is inverted. 3 Data and strobe are inverted.

## Wiegand / Dataclock : LED OUT – CARD PRESENT signals

This parameter signification depends on hardware configuration.

Signal LED OUT – Card Present	
<i>/cfg/Maccess/Wiegand/dataclock/</i>	
<i>led out/card present</i>	
0	Autodetect The led out signal can behave as a card present signal depending on the hardware configuration of the system: <b>DataClock IN/ DataClock OUT: Card present</b>

	<p><b>Wiegand IN/ DataClock OUT:</b> card present (priority goes to dataclock out)</p> <p><b>Wiegand IN/ Wiegand OUT:</b> led out</p> <p><b>DataClock IN/ Wiegand OUT:</b> inactive.</p>
1	<p>Force Led out</p> <p>The led out signal only behaves as a led out signal.</p>

## Wiegand / Dataclock : LED IN signal

Use this signal to wait a controller “ACK” or to drive the terminal led.

LED IN signal	
<i>/cfg/Maccess/Wiegand/dataclock/</i>	
<i>Led IN</i>	
0	(default) Active The led in signal is ignored.
1	Inactive The MorphoAccess™ led is driven by the <i>led in</i> signal: <ul style="list-style-type: none"> <li>• <i>led in</i> = 0      led is green</li> <li>• <i>led in</i> = 1      led is off</li> </ul>
2	The Wiegand in port is used as a dual led in port. D1 is connected to Led in green and D0 to Led in red. This feature improves integration in an access control system (ACS). Result of biometric matching is validated by the ACS through Led in signals.

When the ACS validates the control a timeout must be specified.

ACK timeout	
<i>/cfg/Maccess/Wiegand/dataclock/</i>	
<i>Timeout</i>	Time in seconds during which the MorphoAccess™ will wait for an acknowledgement signal from the ACS through Led in signals. ("Led IN 2" mode).

## Setting up Wiegand Interface

When set up to communicate with Wiegand protocol, the MorphoAccess™ can handle multiple data format.

Default format (26-bit) is described in appendix 2.

The Wiegand frame format is defined using six configuration keys. Different protocol can be defined for input and output.

Wiegand frame timings are not customizable. Additional security (ciphering) is not handled. All Wiegand protocols are reverse.

### Frame definition

Here after are listed the customizable parameters of a Wiegand frame.

#### - Length

A Wiegand frame can contain up to 128 bits.

#### - Control bits

In a Wiegand frame, start and stop bits are used as control bits. They can be fixed to 0 or 1 or be used as parity (odd or even) bits calculated over bits of the frame.

#### - Data

In the Wiegand protocol, three data are handled: the Site code (also called Facility code or Comparison number), the ID (also called Badge number or Sequence number) and a custom data. Data can have a variable bit size and can be located anywhere in the frame. Data are inserted in the frame MSB first.

### Configuration keys.

The corresponding configuration keys are in file */cfg/Wiegand* in either section *IN* or *OUT*:

#### Wiegand frame Personalization

*/cfg/ Wiegand /IN or OUT*

<i>Length</i>	1-128	Defines the number of bits of the frame.
<i>Start</i>		Defines the start control bit.
	0.0	Reset to 0.
	1.0	Set to 1.
	2.n	Even parity calculated over the n first bits.
	3.n	Odd parity calculated over the n first bits.
	4.0	No start bit

<i>Stop</i>		Defines the stop control bit.
	0.0	Reset to 0.
	1.0	Set to 1.
	2.n	Even parity calculated over the n last bits.
	3.n	Odd parity calculated over the n last bits.
	4.0	No stop bit
<i>Site</i>	n.m	Insert m bits of site value at offset n.
<i>ID</i>	n.m	Insert m bits of ID value at offset n.
<i>Custom</i>	0.0	Reserved for SAGEM custom protocols.

Note: The number of bits of the Wiegand ID is limited to 64 bits

**Examples :**

See *APPENDIX 2 - WIEGAND DATA FORMAT* page 107.

## ID SENDING ON UDP

You can use the Ethernet port to send the corresponding ID to the central security controller. Connection should be made using port 11020.

Please refer to *MorphoAccess Remote Messages Specifications* for more information about this functionality.

ID sending on UDP	
<i>/cfg/Maccess/Ethernet/</i>	
<i>Send</i>	0 Not activated 1 L'ID is sent on UDP
<i>IP</i>	« aaa.bbb.ccc.ddd » IP of the central security controller.

## ID SENDING ON RS232 OR RS422


You can use the serial port to send the corresponding ID to the central security controller. You can use COM1 or COM2 or both.


Please refer to *MorphoAccess Remote Messages Specifications* for more information about this functionality.

### ID sending on « COM1 »

#### Activation

Sending ID on COM1	
<i>/cfg/Maccess/COM1/Send</i>	
	0 Nothing is sent (default) 1 L'ID is sent on COM1

 ID transmission on port COM1 is disabled when ILV is activated on the same channel (i.e. *cfg/Maccess/Admin/Host Com* set to 1).

 COM1 parameters are defined by *cfg/ser0*.


#### Identifier format (COM1)


ID format (COM1)	
<i>/cfg/Maccess/COM1/Format</i>	
	0 L'ID is sent in ASCII. 1 L'ID is sent in Hexa. 2 L'ID is sent in BCD

### ID sending on « COM2 »

#### Activation

Sending ID on COM2	
<i>/cfg/Maccess/COM2/Send</i>	
	2 Nothing is sent (default) 3 L'ID is sent on COM2

 ID transmission on port COM2 is disabled when ILV is activated on the same channel (i.e. *cfg/Maccess/Admin/Host Com* set to 2).

 COM2 parameters are defined by *cfg/ser1*.

### Identifiant format (COM2)

ID format (COM2)	
<i>/cfg/Maccess/COM2/Format</i>	
	0 L'ID is sent in ASCII. 1 L'ID is sent in Hexa. 2 L'ID is sent in BCD

## SERIAL PORT PARAMETERS

The following parameters will be applied for distant administration and ID sending.

### COM1 port (ser0)

Baudrate (bps)	
<i>/cfg/ser0/parameters/</i>	
<i>baudrate</i>	1200 bps 2400 bps 4800 bps 9600 bps (default) 19200 bps 28800 bps 38400 bps 57600 bps 115200 bps

Data bits		
<i>/cfg/ser0/parameters/</i>		
<i>databits</i>	5	5 databits
	6	6 databits
	7	7 databits (default)
	8	8 databits

Parity		
<i>/cfg/ser0/parameters/</i>		
<i>parity</i>	0	No
	1	Odd
	2	Even (default)

Note: Since the embedded version 5.40 the default value of  
*/cfg/ser0/parameters/ databits* is 8 (8 databits)  
*/cfg/ser0/parameters/ parity* is 0 (No parity)

Stop bits		
<i>/cfg/ser0/parameters/</i>		
<i>stop bits</i>	1	1 bit de stop
	2	2 bits de stop (default)

Flow control		
<i>/cfg/ser0/parameters/</i>		
<i>flow control</i>	0	(default value) No.
	1	Hardware (CTS/RTS)
	2	Software (XON/XOFF)

## Using a Deister contactless reader on COM1

To connect a Deister reader on COM1 the serial link parameters must have the following values :

DEISTER reader utilization	
<i>/cfg/ser0/parameters/</i>	
<i>Baudrate</i>	9600
<i>Databits</i>	8
<i>Stopbits</i>	1
<i>Parity</i>	0
<i>Flow ctrl</i>	0

## COM2 port (ser1)

COM2 (ser1)
<i>/cfg/ser1/parameters/</i>
<i>Please refer to COM1 port (ser0) section</i>

## RELAY ACTIVATION

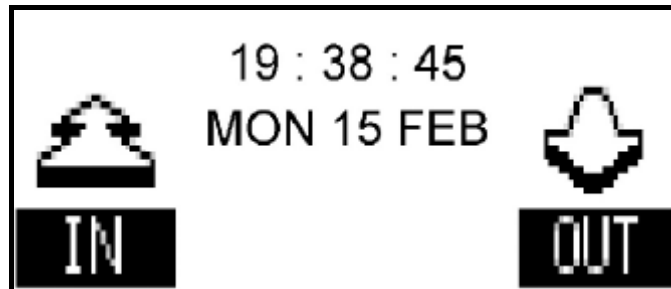
A relay may be activated .

Relay parameters	
<i>/cfg/Maccess/Relay</i>	
<i>Active</i>	0 (default value) Relay not active 1 <i>reserved</i> 2 Relay active
<i>Time in 100 ms</i>	[10 –200], 30 by default. Relay aperture time in 100 ms.

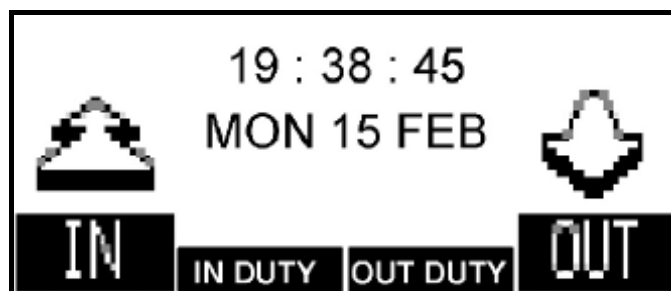
## TIME AND ATTENDANCE

Since software release 5.0, the 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 (in text mode):



*two functions mode*



*four functions mode*

When entering, the user has to press the key function 1 on the keyboard to log his entry time.

When exiting, the user has to press the key function 4 on the keyboard 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.

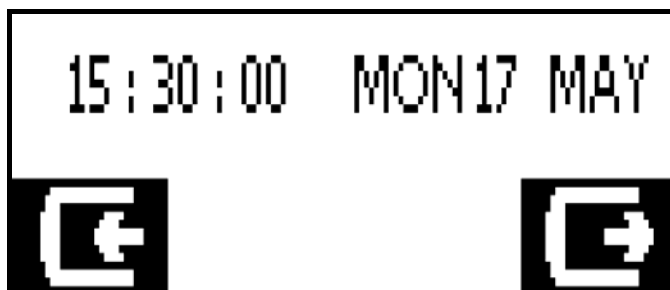
After selection, the MorphoAccess™ switches in biometric mode (identification or authentication).

If the user has selected the wrong operation (IN/OUT...), the function key 4 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).

Note : In case of badge wait (mode 1,3,4,5) or Id presentation, the timeout message is nor displayed nor logged and/or sent to the controller.

Time attendance can also be displayed in graphic mode:



*two functions mode*



*four functions mode*

Time Attendance can be configured from the CONFIG menu thanks to the keys present in the section */cfg/Maccess/time attendance*.

The allowed values are:

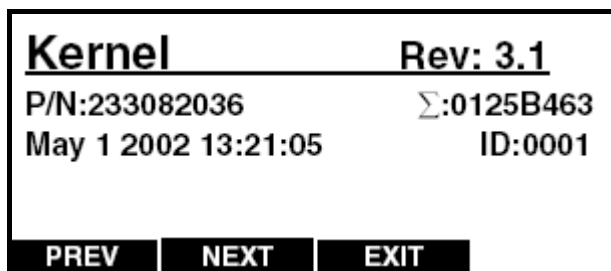
Configuration time attendance		
<i>/cfg/Maccess/time attendance/</i>		
<i>mode</i>	0	Time attendance is disabled.
	1	Time attendance is enabled with two functions: IN and OUT.
	2	Time attendance is enabled with four functions IN, IN (from) DUTY, OUT (on) DUTY and OUT.
<i>display</i>	0	Keys label are in English.
	1	Keys label are in Spanish.
	2	Keys label are in French.
	3	Switches to graphic mode (default value).

For more information about log configuration and retrieving, refer to the *MorphoAccess Host System Interface Specifications*.

## THE VERSION MENU

From the System Menu, press the **VERSION** key to access the information file.

This display contains information that may be necessary if the SAGEM MorphoAccess™ requires technical support. It should not normally be necessary to access this display unless requested by SAGEM technical support personnel.



**Kernel** is the name of the module being displayed.

**Rev** is the revision of the module.

**P/N** is the part number for the module.

**X** is the checksum for the module.

The next line shows the date of the module's creation.

**ID** is the ID for the module in the system.

The **PREV** and **NEXT** buttons allow you to browse for all modules present in your SAGEM MorphoAccess™.

**EXIT** returns to main menu.

## THE SERIAL NUMBER MENU

From the System Menu, press the SER NB key to display the serial number.

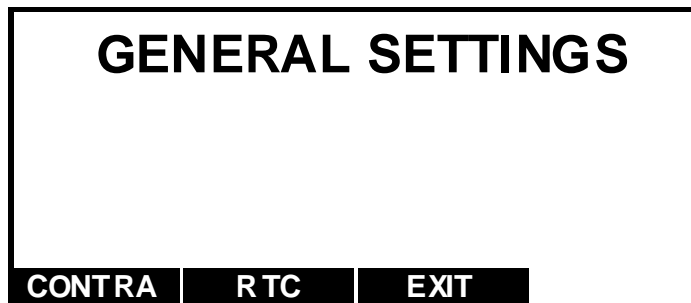
**Serial #** is your SAGEM MorphoAccess™'s serial number.

**MicroBoot revision** is the revision number of your SAGEM MorphoAccess™'s MicroBoot. This revision number may be needed when requesting technical support.

**ETH** is the physical Ethernet address, also known as the MAC address. This address may be required by your network Administrator.

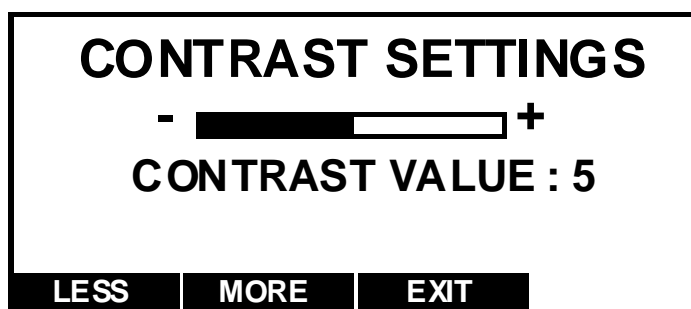
## THE SETTING MENU

From the System Menu, press the **SETTING** key to access the parameter settings.

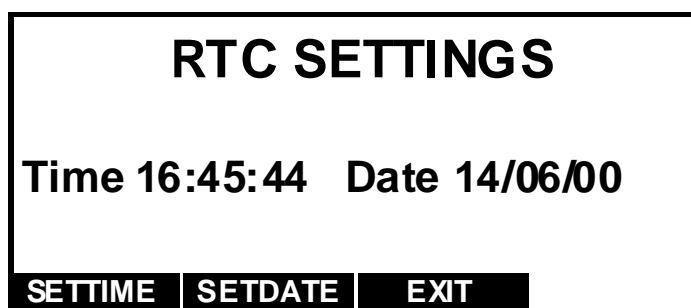


The **CONTRA** selection allows you to adjust the contrast of the LCD display.

The **MORE** key increases the contrast, the **LESS** key decreases the contrast.



The **RTC** menu allows you to set the current date and time.



The **SETTIME** key allows you to set the time. Enter the time in the following format: HHMMSS. The **VALID** key records your setting. The **CANCEL** key aborts editing and returns to the previous menu.

## TIME SETTINGS

TIME (HHMMSS) : 120000

VALID | CANCEL

The **SETDATE** key allows you to set the current date. Enter the date in the following format: DDMMYY. The **VALID** key records your setting.

The **CANCEL** key aborts editing and returns to the previous menu.

## DATE SETTINGS

DATE (DDMMYY) : 100600

VALID | CANCEL

**NB** : You can use the correction key # to delete the last characters entered.

Note : see section *Recommendations* page 104 about date synchronisation.

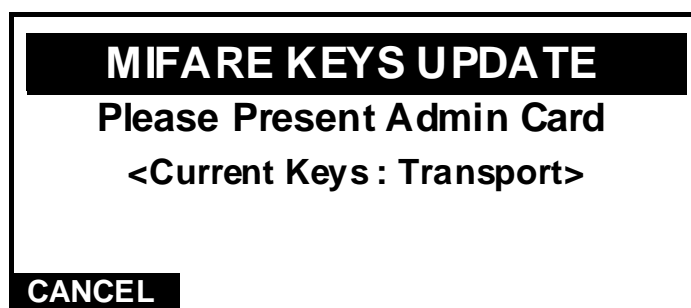
## ACCESS THE MIFARE KEYS UPDATE MENU (MORPHOACCESS 220)

Each data sector on a MIFARE card is protected in reading and writing by 2 keys of 6 bytes each. These keys are noted A and B. Since the card is composed of 16 sectors, there are actually 32 keys.

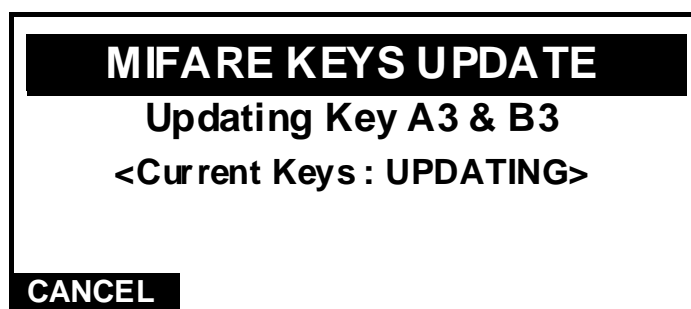
When you present a MIFARE card to the MorphoAccess for an authentication, data can be read only if the keys which protect it are the same as the keys initialized into the reader. By default both keys A and B are set to 0xFFFFFFFF for the 16 sectors in the MIFARE module of the MorphoAccess™. These default values are called Transport keys.

You can change the value of the keys thanks to the hotkey **CL KEYS** in the Administrator menu(17). You will need for that an administrator card containing the new keys to initialize. Please check the Enrollment Station documentation to know how to create an administrator card.

While you are in the administrator menu, press the key **CL KEYS**. The **MIFARE KEYS UPDATE** screen appears.



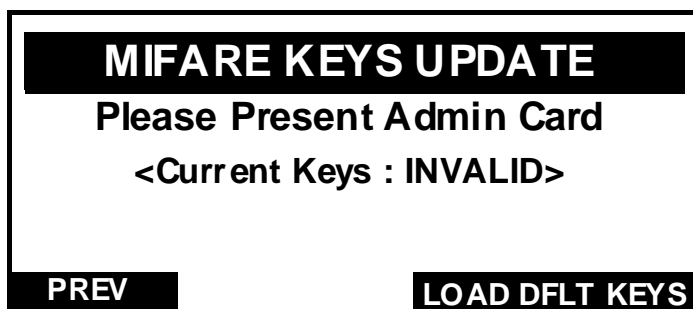
Present the administrator card to start the update.



When the MorphoAccess™ finishes to update the keys for the 16sectors, a successful message appears. The keys status indicates now "user" keys, meaning keys different from 0xFFFFFFFF have been loaded into the reader. Then the MorphoAccess™ comes back to the administrator menu after 2 seconds.

If for some reasons the update is not successful (power shutdown before the end of the operation for instance), a new hotkey will be available the

next time you will enter in the **CL KEYS** menu. The keys status will indicate "INVALID" keys.



Pressing the **LOAD DFLT KEYS** hotkey will allow you to re-update the 32 keys with the default value 0FFFFFFF.

## CONTACTLESS CARD DATA STRUCTURE (MORPHOACCESS 220 ONLY)

### Data structure

With MorphoAccess™ 220, a MIFARE can be used to trigger an authentication. In that case, biometric data are stored in a TLV format (Tag – Length – Value).

Data on the card is a concatenation of TLV.



**T:** 1 byte data identifier.

**L:** 2 bytes size of the V field. Length is encoded in little endian.

**V:** value of the data field.

The section *Setting up contactless reader parameters* describes the data location (first block read).

### MorphoAccess™ Tags

#### ID Tag

Data type	Size	Tag (Hex)
ID	24	0x32

This tag contains a unique card identifier. This ID can be used as an index in the local database of the MorphoAccess™. It is sent to the access control system on a positive authentication. This tag holds a length fixed string. Data are then padded with null characters.

#### Name Tag

Data type	Size	Tag (Hex)
Name	20	0x20

This tag contains the name of the cardholder. This name will be displayed on a positive authentication. This tag holds a length fixed string. Data are then padded with null characters.

### Minutiae 1 Tag

Data type	Size	Tag (Hex)
Minutiae 1	170	0x30

This tag contains the minutiae of the first enrolled finger according to the PKCOMP170 format.

### Minutiae 2 Tag

Data type	Size	Tag (Hex)
Minutiae 2	170	0x31

This tag contains the minutiae of the second enrolled finger according to the PKCOMP170 format.

### PIN Tag

Data type	Size	Tag (Hexa)
PIN	15	0x33

This tag contains the user PIN code (ASCII and numerical).

### BIOPIN Tag

Data type	Size	Tag (Hexa)
BIOPIN	15	0x34

This tag contains the user BIOPIN code (used instead of the user minutiae).

### CARD MODE Tag

Data type	Size	Tag (Hexa)
Card mode	1	0x35

This tag contains the authentication method to use.

## ADMIN CARD FORMAT (MORPHOACCESS 220 ONLY)

Keys stored on the contactless reader are defaulted to 0xFFFFFFFF.

These keys may be changed using a remote command (ILV) or through a particular contactless card: an “admin card”. This card will store previous and new keys. This card is encoded with *old* keys and contains *new* keys.

### SAGEM keys

#### Mifare 1K card

Data	Size	Tag (Hexa)
SAGEM keys	192	0x03

The keys are 6 bytes long. There are 32 keys to initialize, representing 192 data bytes.

#### Mifare 4K card

Data	Size	Tag (Hexa)
SAGEM keys	480	0x03

The keys are 6 bytes long. There are 80 keys to initialize, representing 480 data bytes.

## Mapping

A succession of TLV will contain all the keys.

### Mifare 1K card

192 bytes of data + 3 bytes of tag. 13 blocs will be required (195/16). 13 bytes will be left empty in the last used block.

This map will represent the position of each key:

Sector	Block 1			Block 2				Block 3			Block 4
0	Reserved										
1	T	L	K1	K2	K3	K4	K5	K6	K7		Current key*
2	K8	K9	K10	K11	...						Current key*
3	...										Current key*
4	K24	..									Current key*
5	K32	...									Current key*

- Key 1 will correspond to key A and will be copied in sector 0.
- Key 2 will correspond to key B and will be copied in sector 0.
- Key 3 will correspond to key A and will be copied in sector 1.
- Key 4 will correspond to key B and will be copied in sector 1.
- ...

\* : If no key is stored in the reader, default keys will be required (0xFFFFFFFF).

### Carte Mifare 4K

Mapping is the same than with 1K cards. There are 80 keys instead of 32: 31 blocks will be required on the card (483/16). 13 bytes will be left empty in the last used block.

## Communication protocol

The communication protocol available allows the terminal to send commands to a host through the communication COM1/COM2 ports.

All the commands will be formatted with an "Identifier Length Value" structure as described below:

Identifier	Length	Value
------------	--------	-------

Identifier called **I** This is the identifier of the command.

Length called **L** This is the length of the Value field in bytes.

Value called **V** The parameters or data.

The commands will be encapsulated in a packet structure described on the next figure.

STX	ID	RC	ILV	<b>CRC</b>	DLE	ETX
-----	----	----	-----	------------	-----	-----

**CRC:** compliance CRC16 V41

Fields name	Definition	Value
<STX>	Start Text	0x02
<ID>	Packet Identifier	0xE1
<RC>	Request Counter	[0 255]
<ILV>	Identifier Length Data (DLE data bytes are stuffed)	
<CRC>	Transmission error control	Depends on the frame
<DLE>		0x1B
<ETX>	End Text	0x03

For more information, refer to document *MorphoAccess Host System Interface Specifications*.

## MORPHOACCESS TECHNICAL CHARACTERISTICS

### Display

Back-light LCD 136 x 34 dots.

### Keyboard

Back-light with 12 numerical keys

With 4 functions keys.

### Fuse

2.5 A quickblow.

### Memory

512Kbytes.

Optional 32-Mbyte Flash memory for data storage only on MA 300.

### Peripherals interfaces

COM1: RS422.

COM2: RS232C (MA xx0 only).

Ethernet 10 Base T.

Wiegand or Dataclock ISO2 output.

Wiegand or Dataclock ISO2 input.

Relay.

Tamper switch.

Antitheft switch.

### Power supply

12 V  $\pm$  5% power supply

Cable cross section depends on the length 0. mm<sup>2</sup> recommended.

SAGEM recommends to use MorphoAccess™ Supply ref 251411986.

## Size and weight

This product is designed for indoor use only.

- 70 x 160 x 145 mm0
- 750 g.

## Environmental conditions

Operating temperature	+ 0 °C to + 40 °C.
Humidity	10 % < RH < 80 %.
Light	The MorphoAccess™ should be installed in controlled lighting conditions (avoid direct exposure to sunlight).
UV Storage conditions	Avoid exposure to UV

## Storage conditions

- Temperature - 20°C to 70°C.
- Humidity < 95%.

## Cleaning precautions

A dry cloth should be used.

Acid liquids or alcohol , abrasive materials are forbidden.

## Recommendations

### Areas containing combustibles

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

### General precautions

- Do not attempt to repair your SAGEM MorphoAccess™ 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 use your SAGEM MorphoAccess™ in damp areas (swimming pool...). Protect it from water and other liquids.
- Do not expose your SAGEM MorphoAccess™ to extreme temperatures.
- Use your SAGEM MorphoAccess™ with original accessories. Attempts to integrate the MorphoAccess™ with unapproved accessories will void your warranty.
- Due to electrostatic discharge, and depending on the environment, synthetic carpet should be avoided in areas where the SAGEM MorphoAccess™ has been installed.

### Ethernet connection

It is recommended to use a category 5 shielding cable (120 OHM). It is also strongly recommended to insert a repeater unit every 90 m.

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 synchronisation

If you expect to use the MorphoAccess™ for Time and Attendance applications or any other application requiring high time precision we recommend to synchronize regularly your terminal time with an external clock.

The terminal clock has a  $40 \cdot 10^{-6}$  ppm time deviation.

## Warning

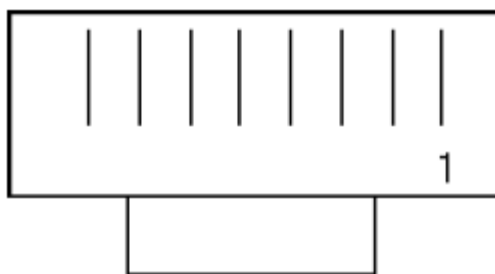
The manufacturer cannot be held responsible if the above recommendations are not followed or if the SAGEM MorphoAccess™ is incorrectly used.

## APPENDIX 1 - ETHERNET COLOR STANDARD

Pinout	Signals	EIA/TIA T568B color	EIA/TIA T568A color	Corel L120 color
1	TD(+) Transmit Data Plus (Output)	White Orange	White Green	Grey
2	TD(-) Transmit Data Minus (Output)	Orange	Green	White
3	RX(+) Receive Data Plus (Input)	White Green	White Orange	Pink
4	No connection	Blue	Blue	Orange
5	No connection	White blue	White blue	Yellow
6	RX(-) Receive Data Minus (Input)	Green	Orange	Blue
7	No connection	White Brown	White Brown	Purple
8	No connection	Brown	Brown	Brown

### RJ45 Pinout

Compliant with 10 base T IEEE Specification.



## APPENDIX 2 - WIEGAND DATA FORMAT

The 26 bits of transmission consists of two parity bits and 24 code bits.

The 8 first code bits are encoding the facility code. This code identifies each MorphoAccess™ in a network.

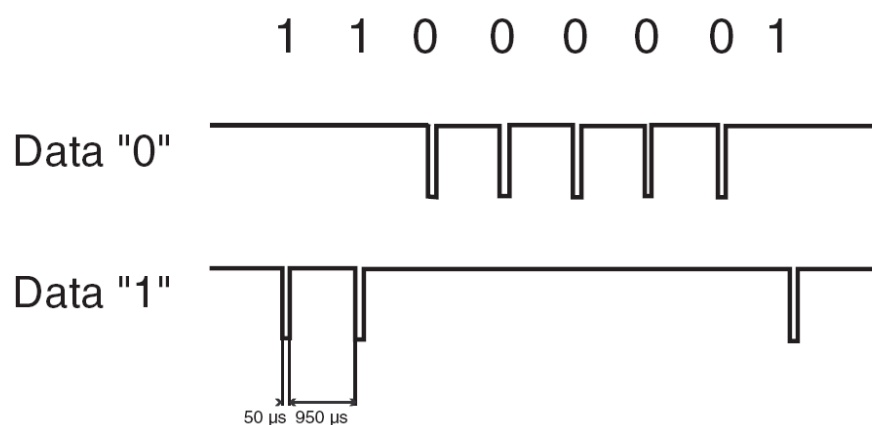
The 16 other bits are data bits.

The first bit transmitted is the first parity bit. It is even parity calculated over the first 12 bits.

The last bit transmitted is the second parity bit. It is odd parity bit calculated over the last 12 code bits.

Even parity (1 bit)	Facility code (8 bits)	Data (16 bits)	Odd parity (1 bit)
------------------------	---------------------------	-------------------	-----------------------

Compliant with access control 26-Bit - Wiegand reader interface standard 03/1995.



## Examples

The corresponding configuration keys are in file /cfg/Wiegand in either section IN or OUT:

### 26-bit: default format

```
/Length: 26
/Start: 2.12 //even parity calculated over the first 12 bits
/Site: 1.8 //1-byte facility code inserted in first
/ID: 9.16 //2-byte ID inserted in second
/Custom: 0.0
/Stop: 3.12 //odd parity calculated over the last 12 bits
```

### 34-bit

```
/Length: 34
/Start: 0.0 //reset to 0
/Site: 1.16 //2-byte comparison number inserted in first
/ID: 17.16 //2-byte sequence number inserted in second
/Custom: 0.0
/Stop: 1.0 //set to 1
```

### 37-bit: HID format

```
/Length: 37
/Start: 2.18 //even parity calculated over the first 18 bits
/Site: 0.0
/ID: 1.35 //35-bit ID (max value is 4294967295)
/Custom: 0.0
/Stop: 3.18 //odd parity calculated over the last 18 bits
```

## APPENDIX 3 - ISO 7811/2-1995 - TRACK 2 DATACLOCK FORMAT

Compliant with ISO07811/2-1995 - Track 2.

### Data encoding table

Value	Bit pattern	Meaning
0	0 0 0 0-1	"0"
1	1 0 0 0-0	"1"
2	0 1 0 0-0	"2"
3	1 1 0 0-1	"3"
4	0 0 1 0-0	"4"
5	1 0 1 0-1	"5"
6	0 1 1 0-1	"6"
7	1 1 1 0-0	llyll
8	0 0 0 1-0	"8"
9	1 0 0 1-1	"9"
10 (A <sup>hex</sup> )	0 1 0 1-1	unused character
11 (B <sup>hex</sup> )	1 1 0 1-0	start sentinel (start character)
12 (C <sup>hex</sup> )	0 0 1 1-1	unused character
13 (D <sup>hex</sup> )	1 0 1 1-0	field separator
14 (E <sup>hex</sup> )	0 1 1 1-0	unused character
15 (F <sup>hex</sup> )	1 1 1 1-1	end sentinel (stop character)

The least significant bit of every digit is sent first; the fifth bit is an odd parity bit for each group of 4 data bits.

The complete message always looks as follows:

left edge	start	data characters	end	LRC	right edge
-----------	-------	-----------------	-----	-----	------------

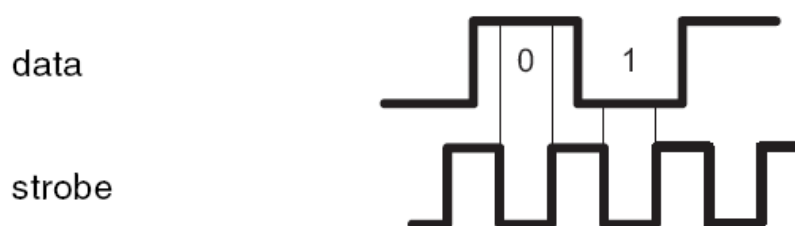
The LRC is calculated by the following procedure: each of the 4 bits in the LRC character is an even parity bit of the equivalent bits in the telegram including start and stop sentinel.

The fifth bit is the odd parity of the 4 LRC bits (it is not calculated over all the parity bits).

Input data should be preceded and followed by a clock synchronization pattern (NULL data).

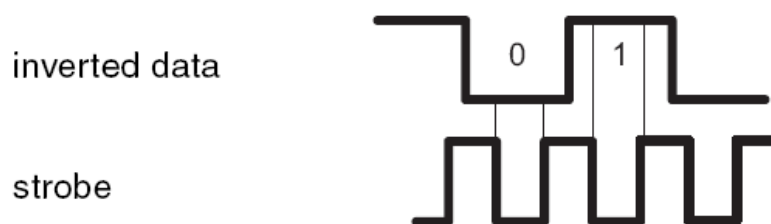
## Dataclock levels

In normal operation mode (default) input and output signals are defined



as:

Other modes are (only for output):



## APPENDIX 4 - RESERVED CONFIGURATION

Those keys are for internal use only.

For proper operation, this settings should not be changed.

/cfg/lcd0/display/type: 1

/cfg/lcd0/contrast/value: 0

/cfg/serx/mode/connection: EXT

/cfg/serx/mode/mode: 450

db/seq flash/start: 0

/cfg/bio/video/channel: 0

/cfg/bio/video/rotation: 0

/cfg/lic/licences/\*

/cfg/bio/base n/timestamp: 0

/cfg/Maccess/bio/segment gabor:1

/cfg/Maccess/contactless/keys status/\*

/admin/security/\*

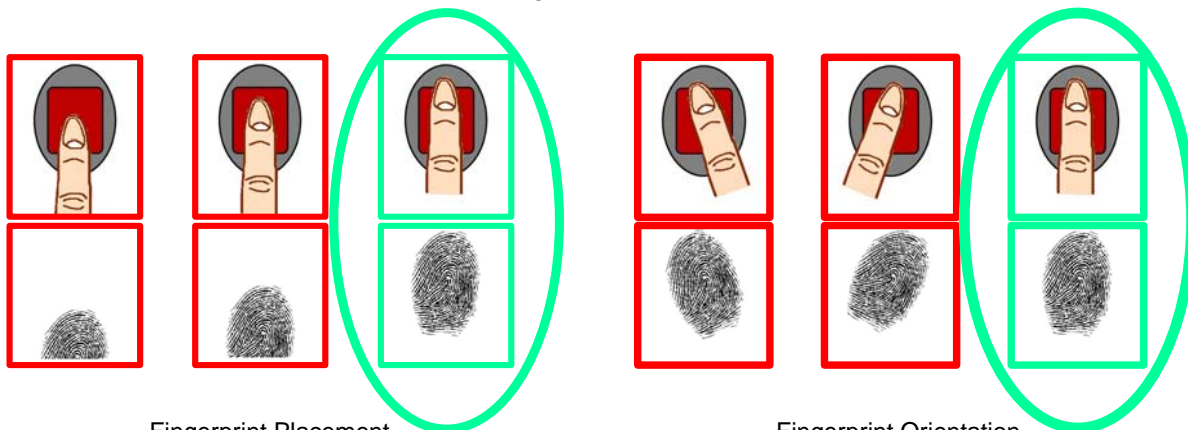
/cfg/Maccess/language/version : 1 if version 5.41

## APPENDIX 5 - FINGERPRINT PLACEMENT RULES

To ensure a good quality contact of your finger on the terminal **you must leave your finger on the sensor until sensor light is turned off.**

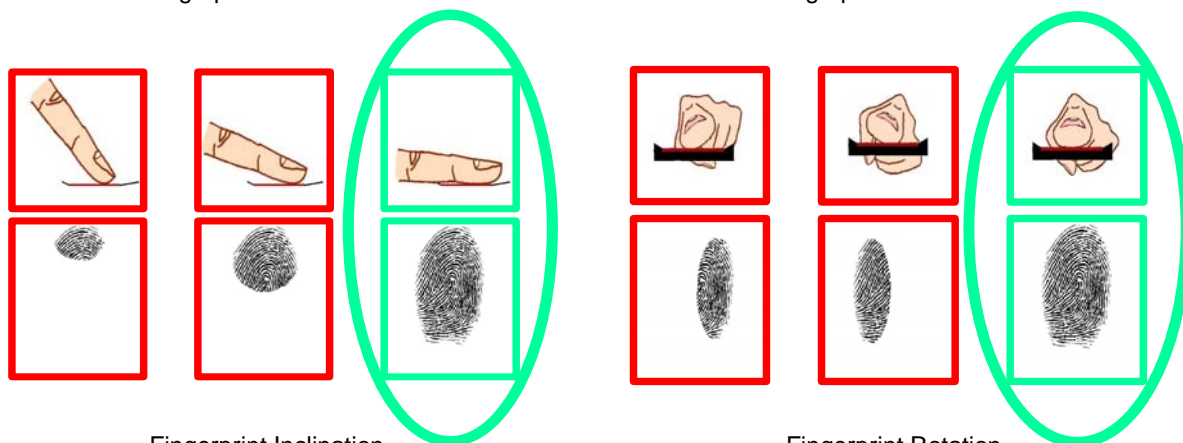


Area containing most of the information



Fingerprint Placement

Fingerprint Orientation



Fingerprint Inclination

Fingerprint Rotation

## APPENDIX 6 – RECOGNITION MODES

Recognition mode is defined by:

<code>/cfg/Maccess/Admin/mode</code>	0 to 6
--------------------------------------	--------

Mode	Description	Local database required?
0	Identification	Yes
1	Authentication with ID coming from Wiegand or Dataclock	Yes
2	Proxy	No
3 (*)	Contactless authentication with fingerprints on card	No
4	Contactless authentication with ID on card	Yes
5 (*)	Fusion: mode 0 and 3	Yes
6	Authentication with ID entered through the keyboard	Yes

(\*): Mode 3 and 5 allows defining the control steps with this key:

<code>/cfg/Maccess/Contactless/without DB mode</code>	0, 1, 2, 16, 18
---	-----------------

Mode	Description
0	Card mode
1	ID “only”, no biometric verification
2	Biometric verification or BIOPIN
16	PIN code
18	PIN code <i>then</i> biometric verification or BIOPIN

## BIBLIOGRAPHY

---

### **MorphoAccess Host System Interface Specifications**

Describes MorphoAccess™ communication protocol (Serial and Ethernet).

---

### **MorphoAccess Remote Messages Specifications**

Complete specifications describing remote messages send during control (Wiegand, Dataclock, Ethernet and Serial).

---

### **Finger Positioning**

Highlight finger-positioning principles.

---

### **MorphoAccess Screen Customization**

Explain how to create personalized screen.

---

### **Database Manager User Guide 1.0**

This tool allows saving / restore local databases. Use Ethernet link.

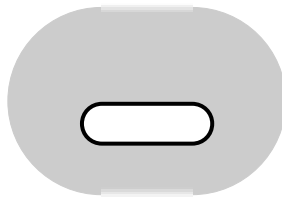
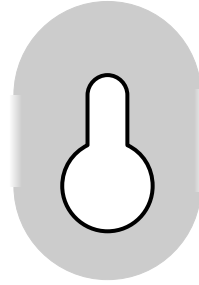
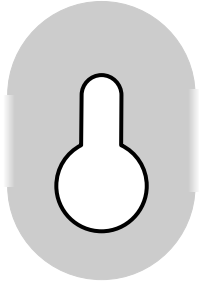
---

### **Easy Downloader User Guide 1.1**

This software is designated to update MorphoAccess™ firmware.

## DRILLING TEMPLATE

---





# SAGEM Défense Sécurité

Siège social : Le Ponant de Paris

27, rue Leblanc - 75512 PARIS CEDEX 15 - FRANCE

Société anonyme à directoire et conseil de surveillance

au capital de 36 405 229 € 562 082 909 RCS PARIS