MorphoAccess® J Series

USER GUIDE

DOCUMENT SSE-0000077399-01 - Version 1.0 - May 2010

Sagem Sécurité
SAFRAN Group

Warning

Printed in France.

Revision History

This Document table contains the history of changes made to this document.

Version	Date	Document Revision History
1.0	May 2010	Creation of MorphoAccess® J Series User Guide

Table of contents

Section 1 Introduction

Section 2 Terminal presentation

Section 3 Terminal configuration

Section 4 Stand alone modes (networked or not)

Section 5 Access control by identification

Section 6 Access control by authentification

Section 7 Proxy Mode

Section 8 Terminal Customization

Section 9 Man Machine Interface

Section 10 Appendix

Section 11 Support

List of figures

LIST OF FIGURES

Section 1

Introduction

Congratulations for choosing a MorphoAccess® J Series Automatic Fingerprint Recognition Terminal.

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

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

The MorphoAccess® J Series integrates Sagem Sécurité image processing and feature matching algorithms. This technology is based on lessons learned during 25 years of experience in the field of biometric identification and the creation of literally millions of individual fingerprint identification records.

Designed for physical access control applications, MorphoAccess® J Series terminals feature a compact, attractive design, coupled with high reliability and security. These latest-generation terminals are both robust and easy to use for a variety of applications, including office, headquarters and administrative building security, as well as protection of external access points.

To ensure the most effective use of your MorphoAccess® J Series terminal, we recommend that you read this User Guide completely.

1. Scope of the document

This guide deals with the use of the MorphoAccess® J Series, which is made up of following list of products.

			Contactless Smartcard Reader	
		Biometrics	MIFARE®	DESFire®
MorphoAccess® J Series	MorphoAccess® J-Bio	x		
	MorphoAccess® J-Dual	x	x	x

2. Safety instructions

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

It is strongly recommended to use a class II power supply at 12V ±5% and 0.5A. min (1A with Wi-Fi^{TM} option) according with Safety Electrical Low Voltage (SELV). The 12V power supply cable length should not exceed 5 meters.

This product is intended to be installed with a power supply complying with EN60950, in accordance with the NEC Class 2 requirements; or supplied by a listed EN60950 external Power Unit marked Class 2, Limited Power source, or LPS and rated 12VDC, 0.5A minimum (1A with Wi-Fi^{TM} option).

In case of building-to-building connection it is recommended to connect 0V to ground. Ground cable must be connected with the terminal block 0V GND.

Europe information

Sagem Sécurité hereby declares that the MorphoAccess® J Series terminal has been tested and found compliant with following listed standards: EN302 291-2 V.1.1.1 (2005-07) + recommendation 1999/519/CE with standard EN 50364; EN 301 489-3 V.1.4.1 (02), and low voltage Directive 2006/95/CE: CEI60950-1:2005 2nd edition.

USA information

Responsible Party: Sagem Sécurité, Le Ponant de Paris, 27, rue Leblanc - 75512 PARIS CEDEX 15 - FRANCE.

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

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

NOTE

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

Shielded cables must be used with this unit to ensure compliance with the Class B FCC limits.

SECTION 2

TERMINAL PRESENTATION

Sagem Sécurité
SAFRAN Group

1. Interfaces presentation

User interface

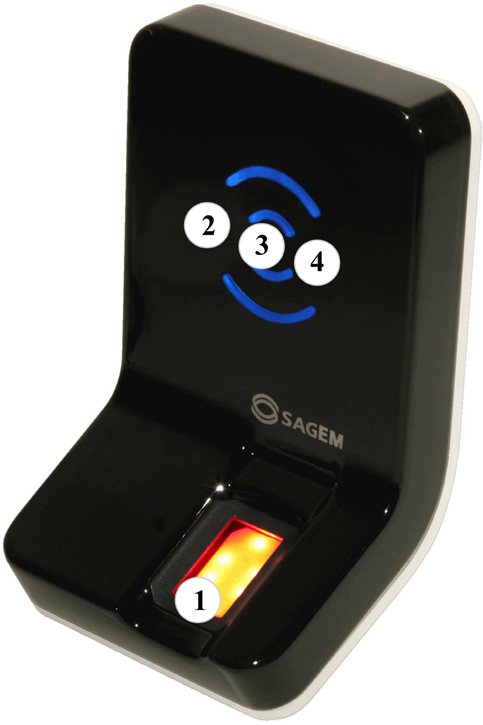


Figure 2 • 1: MorphoAccess® J Series front view

The MorphoAccess® J Series terminals offer a simple and ergonomic man-machine interface dedicated to access control based on fingerprint recognition:

- a high quality optical scanner to capture fingerprints (1),
- a multi-colour led (8 colors) (2),
- a multi-toned buzzer (3) ,
- on MorphoAccess® J-Dual, a contactless smartcard reader (MIFARE® and DESFire® (4)

Power supply interface (see figures 2 • 2 and 2 • 3)

The terminal can be powered by two different ways:

- Either by the two wires +12V DC/GND (11)
- Or by the Power Over Ethernet function

Ethernet interface can be used to power the MorphoAccess® J Series terminal through POE (Power Over Ethernet) mode. According to the POE standard two modes are available: power on data pins and power on dedicated pins.

On MorphoAccess® J Series terminal, POE can be used with RJ45 connector (9) or with block connector (12). Modes are implemented as follows:

- POE through RJ45 connector (9): on data pins or on dedicated pins.
- POE through block connector (12): on data pins.

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

A hardware reset button executes, when pressed, a power down/power up sequence (14). This reset button is located under the removable smoked front cover.

Administration interface (see figures 2 • 2 and 2 • 3)

The terminal can be configured through:

- A RJ45 Ethernet connector (LAN 10/100 Mbps), using TCP or SSL protocol (9)
- A 5 wires Ethernet connection (LAN 10/100 Mbps), using TCP or SSL protocol (12)
- A Wi-Fi^{TM} adaptor plugged in the rear USB host port (10)
- a USB mass storage key for punctual and limited modifications, plugged, when required, in the front USB port (13). This USB port is located under the removable smoked front cover.

Access control devices and systems interface (see figure 2 • 2)

The terminal offers several interfaces dedicated to access control systems and devices:

- the same Ethernet or Wi-Fi^{TM} link, as the one used for configuration, using UDP, TCP, or SSL protocol (9), or (12)
- one serial output port which supports these protocols : Wiegand /

DataClock / RS485 (5)

- two LED IN inputs (one for access granted, one for access denied), in an Access Control System (6)
- a relay switch to directly command a physical device such as a door lock (7),
- a tamper switch (8),

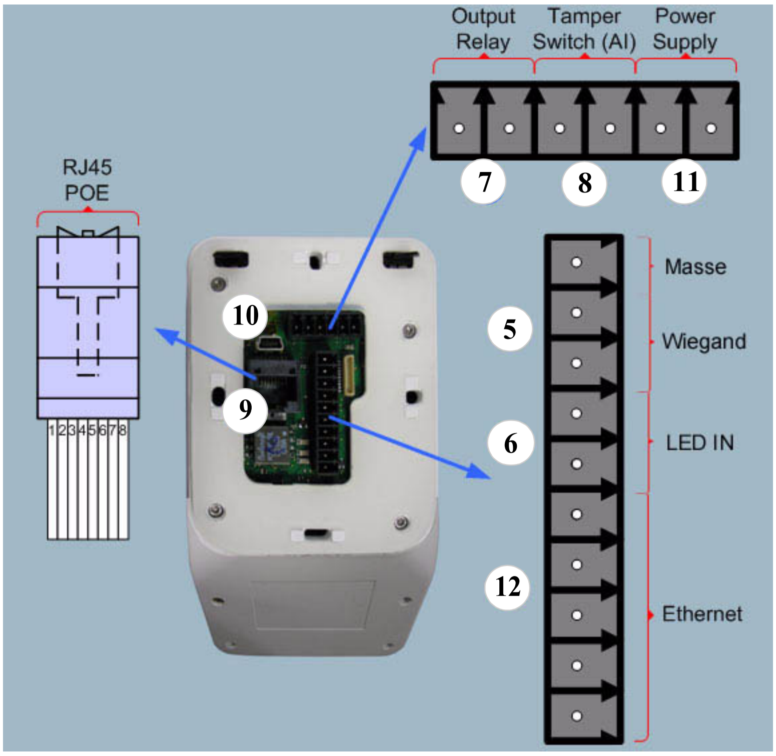


Figure 2 • 2: MorphoAccess® J Series rear view (connectors)

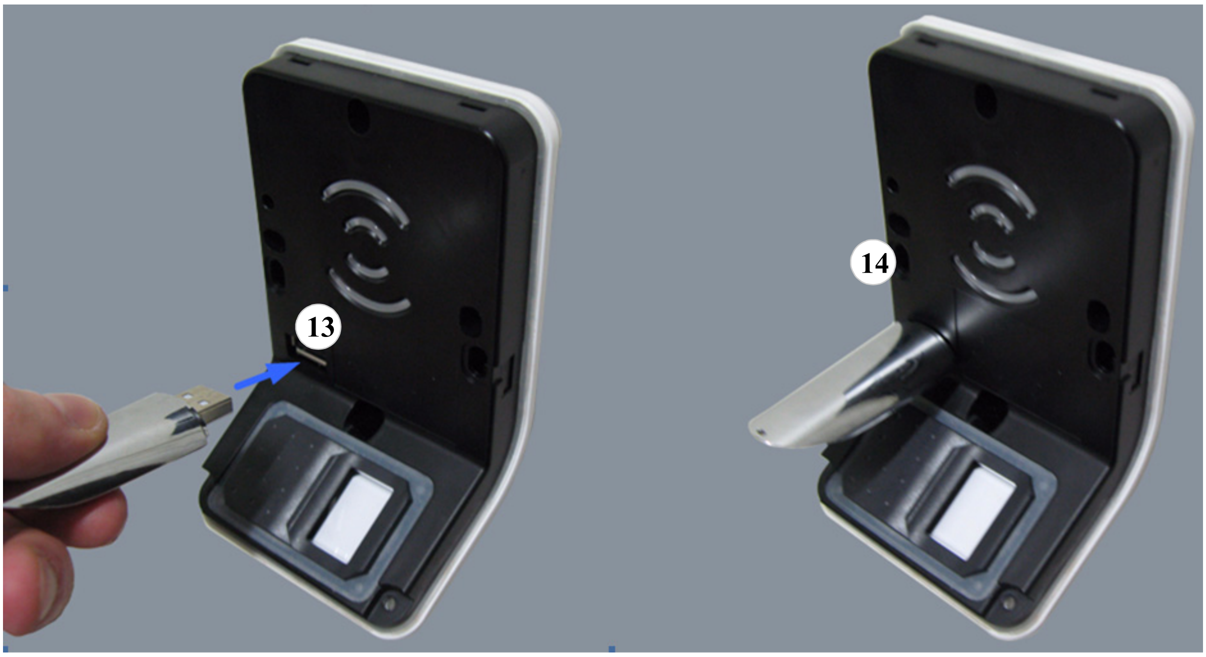


Figure 2 • 3: MorphoAccess® J Series with a USB mass storage key

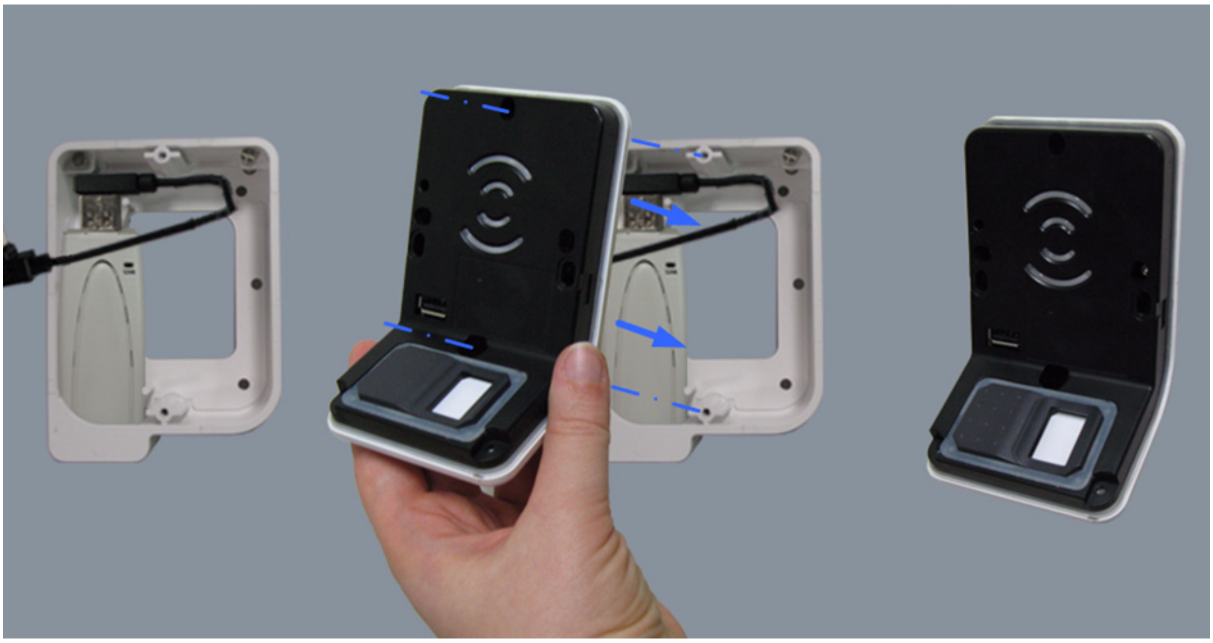


Figure 2 • 4: MorphoAccess® J Series with a Wi-Fi™ adapter

The *MorphoAccess® J Series Installation Guide* describes precisely each interface and connection procedure.

SECTION 3

TERMINAL CONFIGURATION

Sagem Sécurité
SAFRAN Group

This chapter details how to configure the MorphoAccess® J Series terminal. A parameter can be changed directly (using a USB mass storage key) on the terminal or remotely through a network.

1. Setting up the terminal IP address

The MorphoAccess® J Series terminal can run in stand alone mode but a TCP/IP connection is required to download records in the terminal and to configure its recognition mode.

It is possible to specify standard TCP parameters such as terminal network address, network gateway or mask.

These parameters can be set using a USB *mass storage* key.

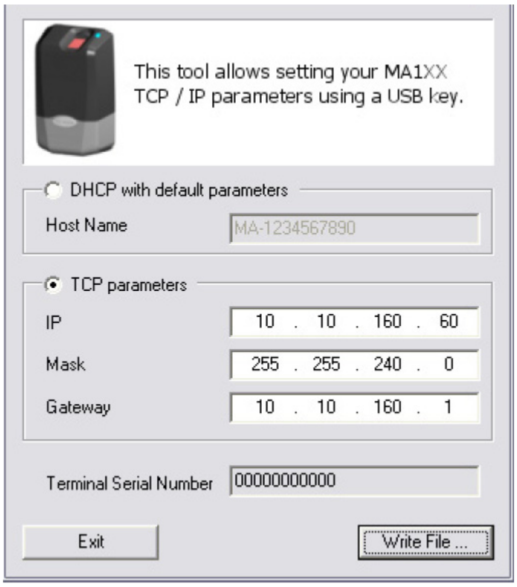
The complete procedure is decribed in section 2, *Configuring a standalone MorphoAccess®*. Once connected to the network, the MorphoAccess® J Series terminal can be configured using Configuration Tool application (for example).

2. Configuring a standalone MorphoAccess®

"USB" key administration

MorphoAccess® J Series terminals have no keyboard, no screen. However it is possible to change TCP/IP parameters without connecting the terminal on a network. This operation only requires a standard USB Mass Storage key (FAT16 formatted, 1 Gb maximum).

A decicated PC application, *USB Network Configuration Tool*, allows writing these new parameters on the key.



This tool allows setting your MA1XX TCP / IP parameters using a USB key.

○ DHCP with default parameters

Host Name: MA-1234567890

● TCP parameters

IP: 10 . 10 . 160 . 60

Mask: 255 . 255 . 240 . 0

Gateway: 10 . 10 . 160 . 1

Terminal Serial Number: 00000000000

Please refer to *USB Network Tool User Guide*.

Note about DHCP mode

The DNS server must be updated with MorphoAccess® terminal names, so that users can communicate with the MorphoAccess® terminal using the terminal's hostname. Please contact your network administrator.

Principle

This feature is available to change network parameters (IP, address, mask and gateway).

Store a file on a USB mass storage key

The administrator creates a configuration file on a PC using the ***USB Network Configuration Tool.*** This *configuration file* contains new network parameters. This file must be stored on a USB mass storage key.

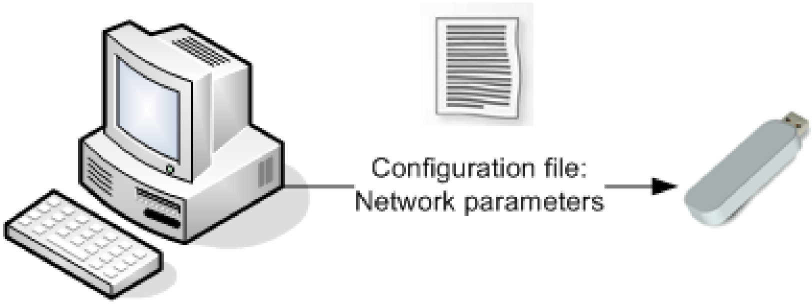


Figure 3 • 1: Build a setting file on a USB mass storage key

Apply changes on a standalone terminal

The front window of the MorphoAccess® must be removed to give access to the USB Host Interface of the terminal. The terminal must be powered on.

When the USB mass storage key is inserted in the MorphoAccess® USB interface, the *configuration file* is read: network parameters are applied.

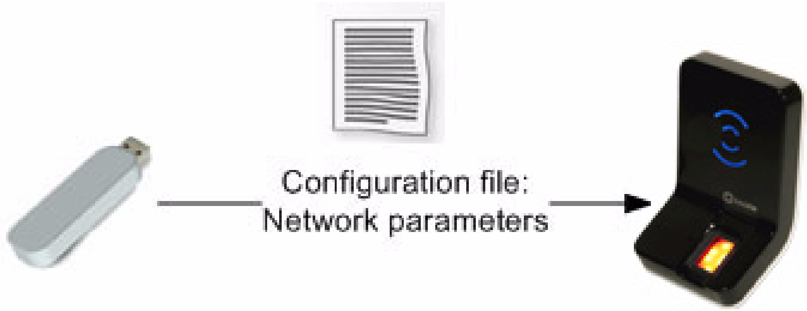


Figure 3 • 2: Apply setting file to the MorphoAccess®

At the end of the process, two medium-pitched «beeps» indicates that the USB mass storage key can be removed.

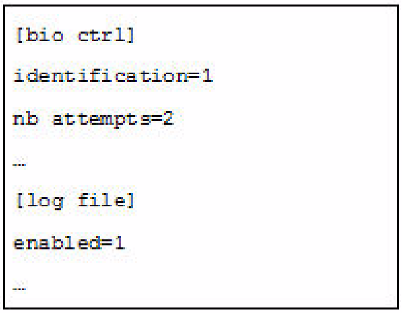
Please refer to *USB Network Configuration Tool User guide* for more information about this procedure.

3. Understanding MorphoAccess® configuration parameters management

Presentation

MorphoAccess® parameters (also named "configuration keys") are stored into files organized in sections and values.

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



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

Configuration organization

The application creates several files:

- app.cfg,
- adm.cfg,
- bio.cfg,
- net.cfg,
- gui.cfg
- wifi.cfg

The *app.cfg* file contains the application settings, *adm.cfg* contains administration parameters, *bio.cfg* the biometric sensor settings, *net.cfg* the Ethernet interface parameters, *wifi.cfg* some Wi-Fi™ parameters.

One file are reserved by the system to store factory settings:

fac.cfg.

Modifying a parameter

There is one way to modify a parameter:

- remotely through Ethernet or Wi-Fi™ link, with a client application running on the Host System.

Notation

In this manual a parameter is presented using this formality:

Short parameter description	
file/section/parameter	Value

For example to activate recognition mode based on identification, this key must be set to 1 (enabled, true, or yes when using the configuration application):

Identification mode activation	
app/bio ctrl/identification	1

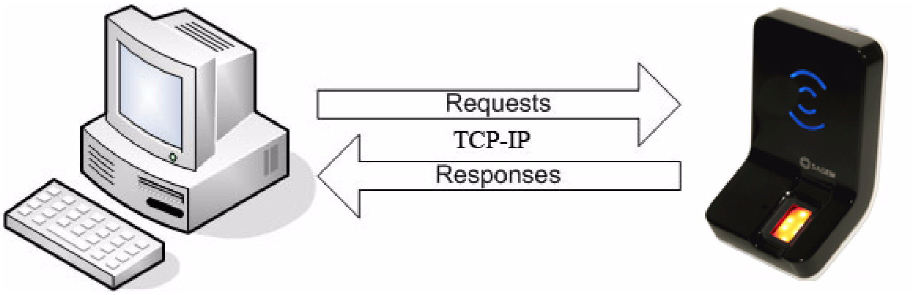
4. Configuring a networked MorphoAccess®

Introduction

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

- Biometric record addition,
- Configuration key reading,
- Access Control settings modification,
- Local database deletion,
- Biometric record deletion,
- Access control diary (log file) downloading,
- Firmware upgrade.

The PC acts as a TCP/IP client for the MorphoAccess®.



Remote management

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

Figure 3 • 3: Communication between a Host System and a MorphoAccess® J Series.

The MorphoAccess® works as a TCP/IP server waiting for request from a client.

Then the client (the PC) can send biometric templates to the terminal and manage the local database.

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

Network factory settings

By default the terminal IP address is 134.1.32.214. This address can be changed through IP (*Configuration Tool*) or with a USB flash drive (*USB Network Tool*).

The default server port is 11010.

Date/Time settings

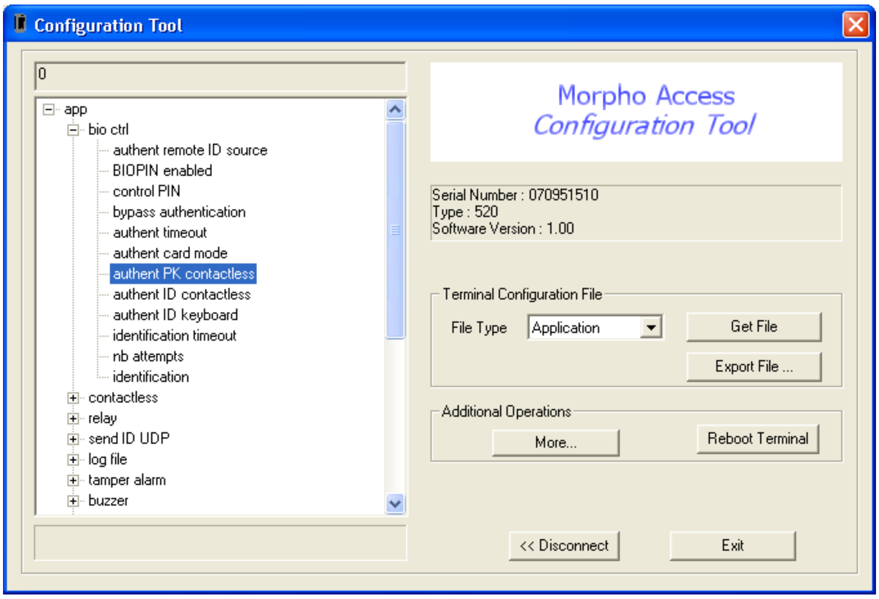
The date/time of the terminal can be initialized by a distant host system using an application such as the "Configuration Tool" ("More" button) described below.

SSL securing

This remote management TCP link can be secured using SSL. Please refer to *SSL Solution for MorphoAccess®* document for further details.

Modifying a configuration key using "configuration tool"

Configuration Tool can modify MorphoAccess® parameters. This program is an illustration of use of the TCP API. Please refer to *Configuration Tool User Guide* for further information about this program.



Serial Number : 070951510
Type : 520
Software Version : 1.00

File Type: Application

Figure 3 • 4: MorphoAccess® configuration tool

Network Wi-Fi™ configuration

Wi-Fi™ connection is available under the following conditions:

- a Sagem Sécurité Wi-Fi™ USB adapter must be plugged in the rear USB port of the terminal. Installation procedure is described in the *MorphoAccess® J Series Installation Guide*,
- a MorphoAccess® Wi-Fi™ Licence is loaded in the terminal (cf. paragraph "Downloading a licence"),
- the terminal must not be connected to a network with an Ethernet cable: Wi-Fi™ connection and Ethernet cable connection are mutually exclusive.

NOTE Both Wi-Fi™ USB adapter and licence can be ordered under the reference "MORPHOACCESS WI-FI PACK.

NOTE **When DHCP mode is activated**

A DHCP server and a DNS server are mandatory to use this feature.

The DHCP server automatically attributes an IP address to the MorphoAccess®.

The DNS server links the MorphoAccess® hostname to its real IP address.

It is also important that the DNS server is updated each time the DHCP server attributes another IP address to a MorphoAccess®.

NOTE

A MorphoAccess® Wi-Fi™ Licence is mandatory.

If the terminal is configured to use the Wi-Fi™ connection with the Wi-Fi™ USB adapter plugged in and if there is no licence present, the MorphoAccess® will display a error signal.

To solve this issue, unplug the Wi-Fi™ USB adapter and restart the terminal. To restart the terminal use the reset button located in front face of the terminal (see section 2, chapter 1. *Interfaces presentation*, sub-paragraph "Power supply interface" for more information on reset button).

See Wi-Fi™ parameters description in paragraph Wi-Fi™ configuration.

5. Upgrading the firmware

It is possible to upgrade current MorphoAccess® firmware through IP (Ethernet or Wi-Fi™).

The firmware can be obtained on a CD/ROM package from factory, or downloaded from Sagem Sécurité Website (login and password required) http://www.biometric-terminals.com/ .

Use the *MorphoAccess® Quickloader* to upgrade terminal system.

Please refer to *the MorphoAccess® Upgrade Guide* for more information about firmware upgrade procedures.

6. Downloading (adding) a licence

A licence unlocks additional features of the terminal. By default the MorphoAccess® J Series can match a fingerprint against a database of 500 users.

The MA 3K USERS licence extends MorphoAccess® J Series recognition capabilities to a database of 3,000 users (2 fingers per user).

Wi-Fi™ network (WLAN) use is enabled with another licence.

Licence number depends on the Device Licence ID. This unique identifier is checked by the Licence Manager tool.

The *Licence Manager* tool allows downloading a licence in the MorphoAccess® as explained in *Terminal Licence Management documentation.*

The *Licence Manager* tool is also able to display the name of the licences stored in the MorphoAccess® J Series terminal.

Section 4

Stand alone modes (networked or not)

Sagem Sécurité
SAFRAN Group

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

1. Recognition mode synthesis

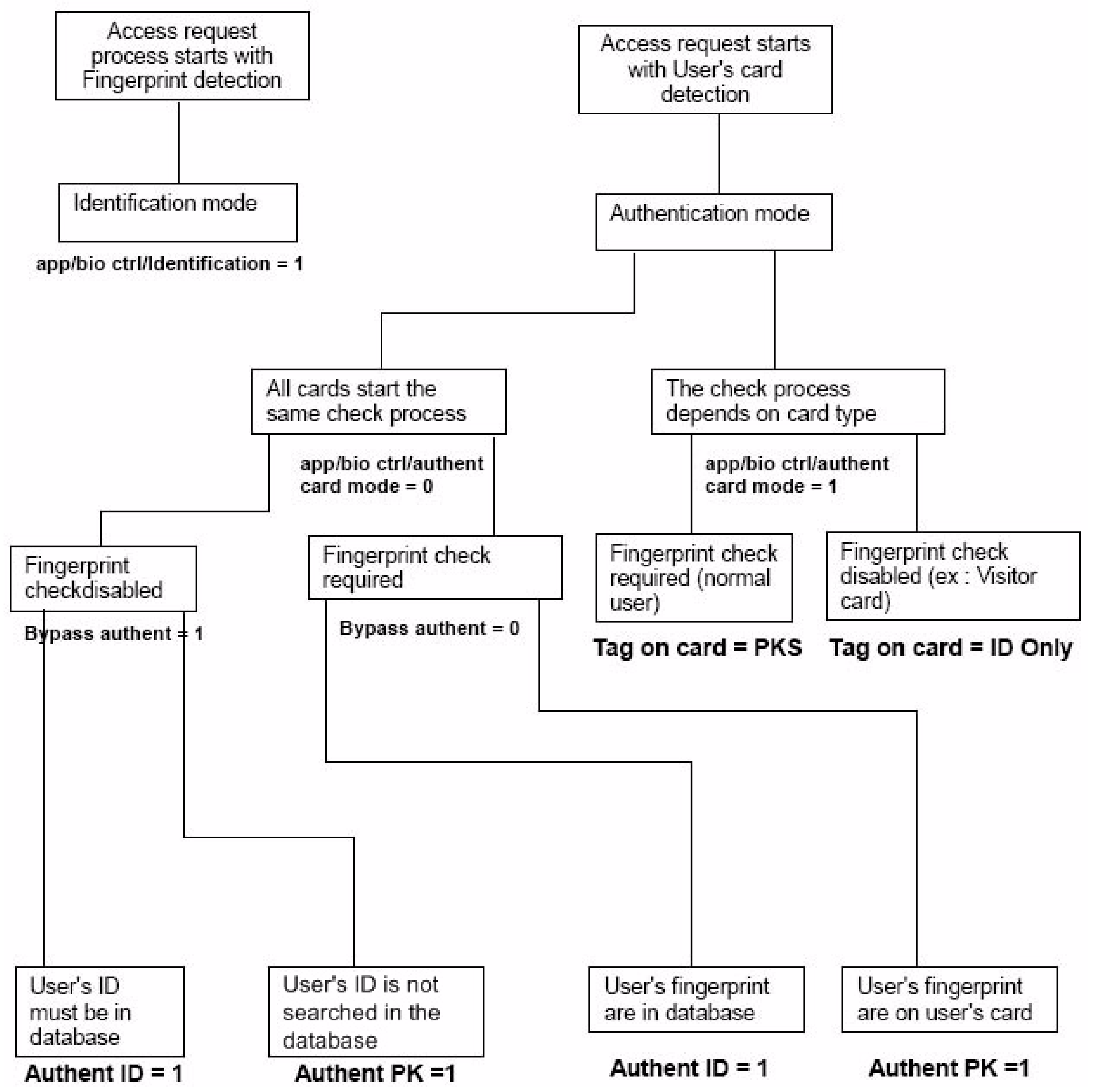

Access request process starts with Fingerprint detection
Identification mode
app/bio ctrl/Identification = 1
Access request starts with User's card detection
Authentication mode
All cards start the same check process
app/bio ctrl/authent card mode = 0
The check process depends on card type
app/bio ctrl/authent card mode = 1
Fingerprint checkdisabled
Bypass authent = 1
Fingerprint check required
Bypass authent = 0
Fingerprint check required (normal user)
Tag on card = PKS
Fingerprint check disabled (ex : Visitor card)
Tag on card = ID Only
User's ID must be in database
Authent ID = 1
User's ID is not searched in the database
Authent PK =1
User's fingerprint are in database
Authent ID = 1
User's fingerprint are on user's card
Authent PK =1

Figure 4 • 1: Recognition mode synthesis

2. Adding a user's record in the database

The management of the MorphoAccess® internal biometric database can be done remotely by a Host System.

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

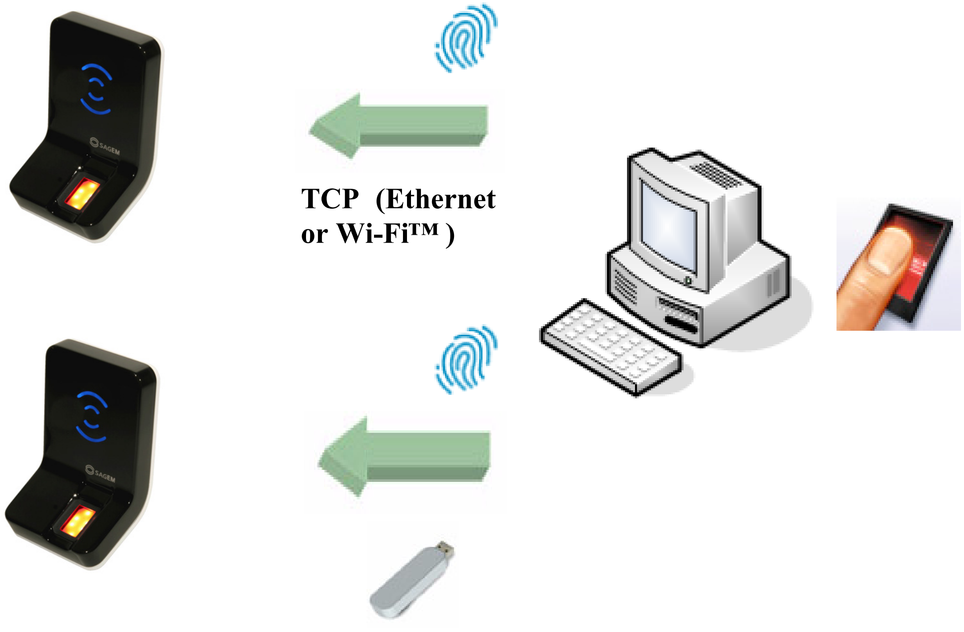


Figure 4 • 2:Adding a fingerprint in MorphoAccess® J Series terminals

This architecture allows managing several MorphoAccess® databases from only one PC enrolment station.

3. Access control presentation

Typical access control system

Typical architecture includes, at least one MorphoAccess®, a Host System (for enrolment) and a Central Security Controller (for area access final check, and physical access command).

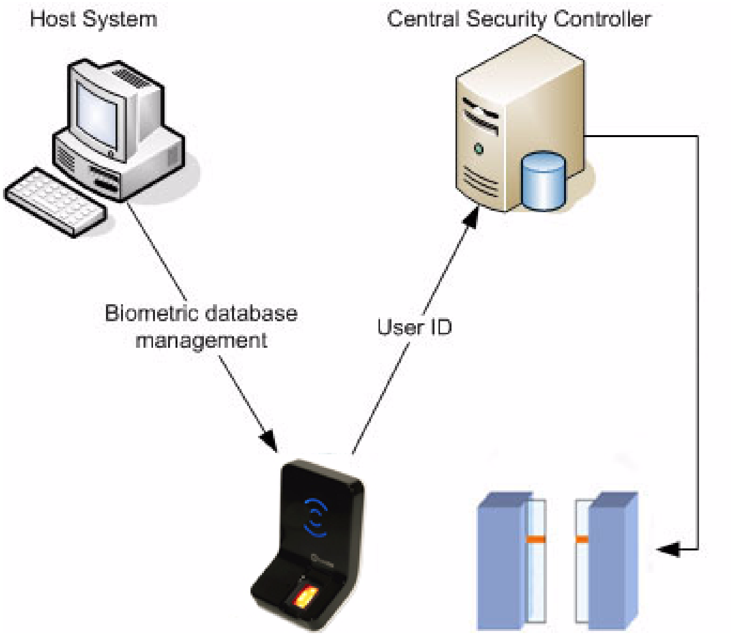


Figure 4 • 3:Typical access control system architecture

MorphoAccess® J Series biometric database management

The management of the MorphoAccess® internal biometric database can be done remotely by a Host System (typically a PC with MEMS™ application).

MorphoAccess® operating mode

The MorphoAccess® works according two exclusive operating modes.

- In Stand Alone Mode, the biometric database can be managed by a Host System and downloaded to the MorphoAccess®.
- In Proxy Mode, the terminal is remotely operated by a host system application that sends individual commands to the MorphoAccess®.

MorphoAccess® access control result sending

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

Identification - authentification

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

Identification (matching 1 versus N)

In this mode, the user which requires the access, is unknown, and the terminal searches for its identity. The captured fingerprint is compared will all the fingerprints stored in the database.

Fingerprint Minutiae are stored in terminal local database. The terminal can store 500 users (2 fingers per user) in the local database, or 3000 users with specific licence (MA 3K USERS licence).

In this mode the sensor is always switched on, waiting for a finger.

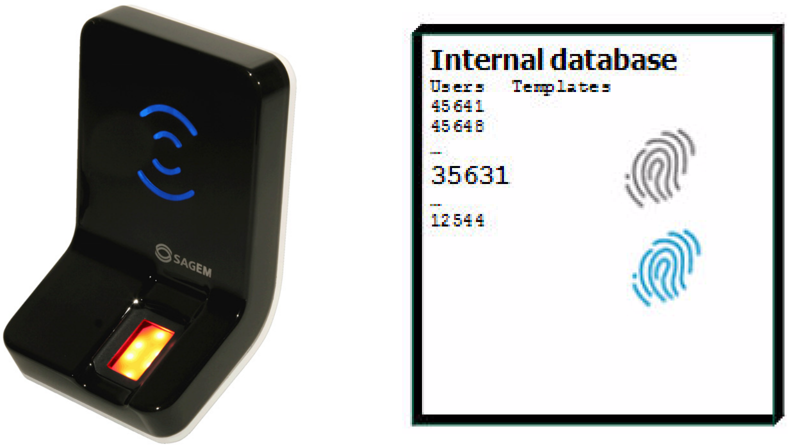


Figure 4 • 4:Identification mode

If the user is found, access is granted.

If the user is not recognized, access is denied .

See section *Access control by identification.*

Authentification (1 versus 1)

In that mode, the user provides his identity (his user identifier), and the terminal checks it.The captured fingerprint is compared with one or two reference templates associated to the user identifier provided before the fingerprint capture.

In authentication, user’s minutiae can be stored on a contactless card. It is also possible to store his minutiae in terminal local database.

Contactless card containing:

- User Identifier (ID)
- User's reference fingerprints

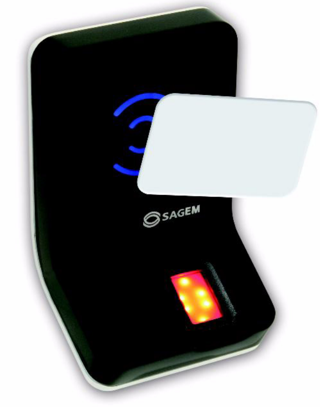


Figure 4 • 5:Authentification with contactless card

If the user is authenticated, access is granted.

If the user is not recognized, access is denied.

See section *Access control by authentification*.

Access control result communication

Scope

The result of the access request is signified to the user by a specific light signal, and an audible signal.

In addition to user information, the terminal is able:

- to activate an internal relay (to open a door),
- to register the access request result in an internal log file,
- and to send an access control result message to a distant system (usually a Central Security Controller) through several kind of communication links.

If access is granted (the user has been recognized), the led lights green and the buzzer emits a high-pitched "beep".

If access is denied (the user has not been recognized), the led lights red and the buzzer emits a low-pitched "beep".

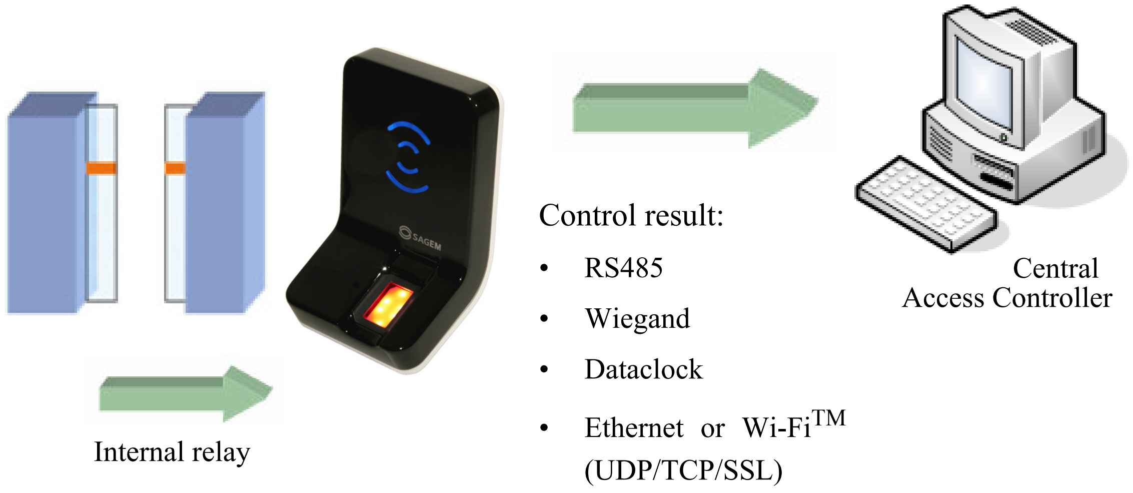


Figure 4 • 6:Access control result

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

Relay

After a successfull biometric control the MorphoAccess® relay may be activated during a specified period (for example, to unlock a door).

Wiegand User Id Emission

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

The message format includes only the user identifier (which must be a numeric value). By default, the message is sent only when the access control result is positive, but as an option this message can be sent when the result is negative, with an error code instead of the user identifier.

Dataclock User Id Emission

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

UDP/TCP User Id Emission

The ID of the recognized user can be sent through the IP link (Ethernet or Wi-Fi^{TM}) using UDP or TCP protocol (unsecured TCP or SSL).
The administrator may select the port adress.

See *SSL Solution for MorphoAccess*® documentation for details about SSL.

RS485 User ID emission

The ID of the recognized user can be sent through RS485.

Please refer to *MorphoAccess*® *Remote Messages Specification* for more information about the format of the User ID message sent through an IP link and through a RS485 port.

Wi-Fi™

Instead of Ethernet connection, the terminal can be connected using a wireless b/g connection. Please refer to paragraphs "Network Wi-Fi™ configuration" and "Wi-Fi™ configuration".

The message format and the protocols supported are the same: UDP, TCP or SSL.

It is not possible for a terminal to be connected through Ethernet and through Wi-Fi™ at the same time.

Access request result : Local Diary (log)

When enabled, the terminal creates a record for each access request in a local file. Each record includes: the date/hour of the access request, the user identifier (if available) and the result of the access rights local check.

The content of this file can be downloaded by the Host System.

The capacity of the file is 8 000 records: when the file is full, the recording of access request result automatically stops.

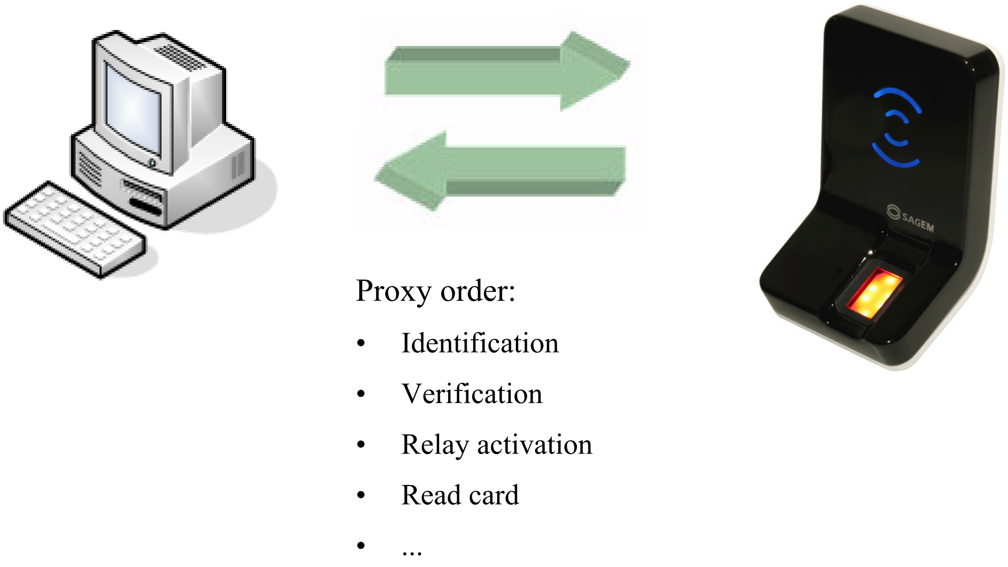
The record file can be erased using relevant command, by the Host System.

"Proxy" mode

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

- user identification,
- user verification,
- relay activation,
- read data on a contactless smart card,
- ...

This mode is used when the whole access right check process is fully monitored by an external device (such as a PC). It means that the local access control application of the terminal is not used, but only the biometric features (identification, authentification) and the user input/output features (the contactless card reader). In that case, the access control application is in the external device.



Proxy order:

- Identification
- Verification
- Relay activation
- Read card
- ...

Figure 4 • 7:Proxy mode

Section *Terminal configuration* gives more information about remote management.

Please refer to *MorphoAccess® Host System Interface Specification* for a complete description of TCP orders possibilities.

ACCESS CONTROL BY IDENTIFICATION

Sagem Sécurité
SAFRAN Group

This section only relates to terminals equipped with a contactless smartcard reader (see section *Scope of the document*).

1. Access control by identification

Identification mode activation	
app/bio ctrl/identification	1

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

After start-up, the MorphoAccess® waits for fingerprint detection. The sensor is lighted on.

The user places a finger on the sensor to start identification process.

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

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

Result is returned to the user by a light and audible signal.

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

At least one user (biometric template) must be stored in the local database. The reminal can store 500 users with 2 fingerprints each and 3,000 users with a MA 3K USERS licence.

If the terminal is running in identification mode with an empty database, the sensor is off and the led flashes «yellow» (please refer to *Convention* Section).

Section 6

Access control by authentification

Sagem Sécurité
SAFRAN Group

1. Introduction to authentication with contacless card

Selecting the type of contactless card to be supported

On MorphoAccess® J Series terminal equipped with a MIFARE®/DESFire® contactless smartcard reader (see section *Scope of the document*), the type of contactless smartcard enabled are defined by the following specific configuration key:

Enabled profiles	
app/contactless/enabled profiles	0-3

- 0 means " default mode (MIFARE® card only)"
- 1 means " Support of DESFire® card only"
- 2 means " Support of MIFARE® card only"
- 3 means "Support of both DESFire® and MIFARE® cards"

It is then necessary to configure the parameters listed in the next sections so as to set the wished recognition mode using contactless smart card. Note that when *app/contactless/enabled profiles* key is set to 0 and the parameters listed in the following sections are configured so as to set a recognition mode using contactless smartcard, MIFARE® card reading is automatically enabled.

For terminal configured for MIFARE® smart card only (see section *Scope of the document*), it is only necessary to configure the parameters listed in the next sections so as to set the wished recognition mode and enable MIFARE® card reading at the same time (i.e. set that key to 0).

Recognition modes

Various recognition modes using contactless card can be applied depending on the fingerprint templates location (user's contactless card or terminal database) and the required security level.

Recognition with DESFire® cards supposes that the user swipes a DESFire® (depending on configuration) card containing some structured data (identifier, biometric templates...).

Recognition with MIFARE® cards supposes that the user swipes a MIFARE® card containing some structured data (identifier, biometric templates...). Data are localized on the card by a block ("B" parameter) and are protected by a key (defined by "C" parameter). The "C" parameter defines which key is used during the authentication with the card.

2. Access control by authentication

This section only applies to MorphoAccess® J Series equipped with a MIFARE®/DESFire® contactless smartcard reader (see section *Scope of the document*).

Whatever is the contacless smart card type, the contained data has the same structure.

Various recognition modes can be applied depending on the user's fingerprint templates localization, and the required security level.

Authentication modes can be combined with a local identification (multi-factor mode).

Following modes are available:

Authentication with templates on contactless card:

Captured fingerprints are matched against templates *read on the card (PK).* Identifier and fingerprints must be stored on the card. It is also possible to skip the biometric control: in this case the terminal acts as a badge reader.

Authentication with template on local database and user ID on card:

Captured fingerprints are matched against templates *stored in the user's record stored in the local database*. Only the identifier is required on the card. It is also possible to skip the biometric control: in this case the terminal acts a badge reader.

Authentication based on contactless card mode:

In that mode, the access rights check to perform is specified on the contactless card. This indicator specifies either "fingerprint check enabled" or "fingerprint check disabled.

Depending on the card mode either templates are read on the card or the control can be bypassed (visitor mode). This mode is only compatible with contactless card with the "card mode" tag, and the corresponding data (user's fingerprints) must be stored on the card.

Please refer to *MorphoAccess® Contacless Card Specification* for a complete description of card structure and access mode.

Authentication with templates on a contactless card

Authentication with templates (PK) on contactless card	
app/bio ctrl/authent PK contactless	1

In this mode, each user's card contains his identifier and his fingerprints. The authentication process starts when the user presents his card in front of the terminal. Then, the sensor is lit up, and the user is required to place his finger on it. The terminal compares the captured fingerprint with the reference fingerprints read on the user's card. The authentication process is successful if the captured fingerprint matches with one of the reference fingerprints.

In this mode, the internal database is not used.

To enable this mode set app/bio ctrl/authent PK contactless to 1.

To disable this mode set app/bio ctrl/authent PK contactless to 0.

To start the authentification process, the user presents his card to the terminal.

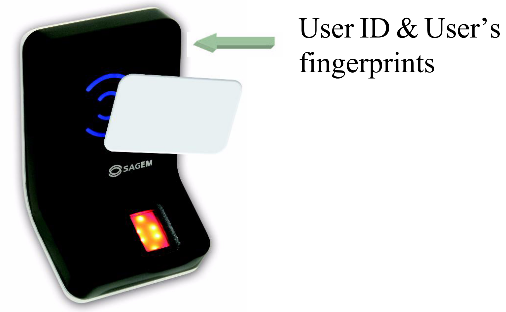


Figure 6 • 1: Authentication with user's fingerprints on contactless card

If the user's card is valid (same authentication keys as the terminal, User's Identifier and user's fingerprints found on the user's card), the user is invited to place his finger for biometric authentication.

If the authentication is successful, the terminal signals the result to the user, and (if applicable) to a distant system such as a Central Security Controller.

Once the user authentication is done, the terminal automatically loops back and waits for another user's card presentation.

Required tags on card

	ID	Card Mode	PK1	PK2	PIN	BIOPIN
Authen PK contactless	Yes	No	Yes	Yes	No	No

Card structure is described in *MorphoAccess® Contacless Card Specification*.

Authentication with template in local database and user ID on contactless card

Authentication with templates (PK) on contactless local database	
app/bio ctrl/authent ID contactless	1

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

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

ASCII User ID included in a TLV structured data

The user’s identifier must be stored into a TLV structure.

ASCII identifier in tagged structure	
app/contactless/data format	0
app/contactless/data length	0
app/contactless/data offset	0

A user's record with the same User ID and user's fingerprint templates must exist in the local database of the MorphoAccess® terminal.

To start the authentication process, the user presents his card to the terminal.

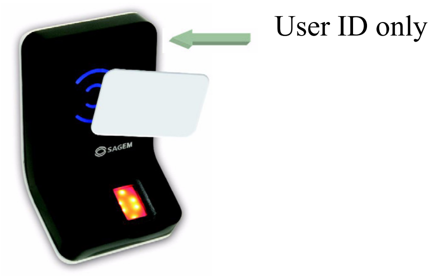


Figure 6 • 2: Authentication with User ID only on the user's card

If the user ID found on the user's card exists in the terminal database, then the optical sensor switches on, and the user is expected to place his finger on it.

If the authentication is successful, the terminal signals the result to the user, and (if applicable) to a distant system such as a Central Security Controller.

Once the user authentication is done, the terminal automatically loops back and waits for an other user's card presentation

Required tags on card

	ID	Card Mode	PK1	PK2	PIN	BIOPIN
AuthenID contactless	Yes	No	No	No	No	No

Card structure is described in *MorphoAccess® Contacless Card Specification*.

Note: a database must exist in the terminal.

Binary user's identifier, non-structured data

This mode can not work when the *app/contactless/enabled* profiles configuration key value is different from 0.

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

It is possible to read non-byte aligned data. It is useful to read a user ID included in a Wiegand frame.

This mode is also useful to use the card serial number as user's identifier.

Binary identifier, non-structured data	
app/contactless/data format	1 (binary data)

Binary data are defined by their position from the first read block.

User ID length is limited to 8 bytes (app/contactless/data length 8.0).

User ID offset is limited to 15 bytes (app/contactless/data offset 15.0).

Data localization	
app/contactless/B	[1-215]: read block
app/contactless/data length	[number of bytes].[additional bits]
app/contactless/data offset	[number of bytes].[additional bits]

The interpretation (little or big endian) of the data can be defined.

Data interpretation	
app/contactless/data type	0.1 (binary data, MSB first) 0.0 (binary data, LSB first RFU)

A user's record with the same User ID value, and user's fingerprint templates must exist in the local database of the MorphoAccess®.

Authentication process is exactly the same as the one presented above.

Example - 4 bytes identifier.

The terminal is configured to read 4 bytes.

Read bytes are F4 E1 65 34.

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

Example - reading a MIFARE® card Serial Number (big endian format).

app/contactless/data format= 1

app/contactless/data type= 0.1

app/contactless/data length = 4.0

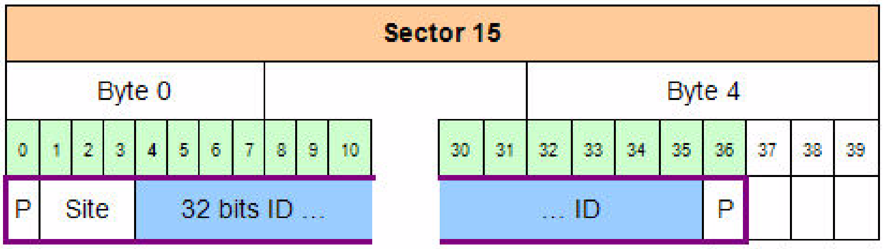
app/contactless/data offset= 0.0

app/contactless/B= 1

Example - reading 32-bits identifier in a complete Wiegand frame.

The card contains at sector 15 a complete 37 bits Wiegand frame (including parity bits, site code).

On this example a 32 bits identifier begins at bit four, parity bits are noted "P".



The corresponding configuration will read only the 32 bits ID on the card.

app/contactless/data format = 1	Binary identifier
app/contactless/data type = 0.1	Binary identifier read in MSB
app/contactless/data length = 4.0	4 bytes length
app/contactless/data offset = 0.4	ID begins bit 4 of sector 15
app/contactless/B = 46	Read at sector 15

It is possible to configure the MorphoAccess® Wiegand output to add parity bits.

Authentication based on contactless card mode

Authentication with contactless card mode	
app/bio ctrl/authent card mode	1 (Enabled)

In this mode the user's card decides of the type of control to perform.

The CARD MODE tag is required on the user's card. This tag can take several values.

- PKS [0x02]: fingerprint check required. The user identifier, template 1 and template 2 are required on the card. The authentication process is identical to "authentication with user's fingerprint templates on contactless card".
- ID_ONLY [0x01]: fingerprint check disabled. Only the user identifier is required on the user's card. There is no biometric control, the control is immediately positive. This feature is useful for visitor requiring an access without enrolment. Even if user's fingerprints are stored on the user's card, the terminal doesn't process it..

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

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

Required tags on card

if CARD MODE tag value is ID_ONLY (fingerprint check disabled).

	ID	Card Mode	PK1	PK2	PIN	BIOPIN
Authen card mode (ID_ONLY)	Yes	Yes	No	No	No	No

if CARD MODE tag value is PKS (fingerprint check required).

	ID	Card Mode	PK1	PK2	PIN	BIOPIN
Authen card mode (PKS)	Yes	Yes	Yes	Yes	No	No

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

Bypassing the biometric control in authentication

When this option is activated, only the user ID is required on the user's card. This option can be combined with any of the authentication modes. Activating this option means that the fingerprint check is disabled.

The terminal controls that the user ID exists in the database

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

Authentication with User ID only on contactless card

Disabling biometric control, but User ID must be present in the local database	
app/bio ctrl/bypass authentication	**1 (Enabled)**
app/bio ctrl/authent ID contactless	1 (Enabled)

Required tags on card

	ID	Card Mode	PK1	PK2	PIN	BIOPIN
bypass authentication	Yes	No	No	No	No	No

The terminal works only as a smart card reader

When combined «authent PK contacless» the MorphoAccess® always authorizes the access (if the user ID is present): the MorphoAccess® works as a simple smart card reader.

Disabling biometric control, access is always granted	
app/bio ctrl/bypass authentication	**1 (Enabled)**
app/bio ctrl/authent PK contactless	1 (Enabled)

Required tags on card

	ID	Card Mode	PK1	PK2	PIN	BIOPIN
bypass authentication	Yes	No	No	No	No	No

The terminal read binary ID on card and works as a smart card reader

In this configuration the MorphoAccess® reads binary data on card and send it without verification.

Disabling biometric control, access is always granted	
app/bio ctrl/bypass authentication	**1 (Enabled)**
app/bio ctrl/authent PK contactless	1 (Enabled)
app/bio ctrl/authent ID contactless	1 (Enabled)

Binary identifier, non-structured data	
app/contactless/dataformat	1 (Binary data)

Multi-factor mode

This mode is the combination of identification mode and contactless authentication modes.

This mode allows:

- running an identification if user places his finger on the sensor (operation identical to identification mode)
- running an authentication if the user presents his contactless card (operation identical to authentication with a contactless card with/without database mode).

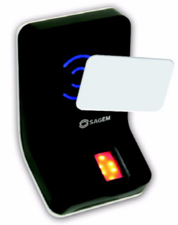


Figure 6 • 3: Multi-factor mode (identification and authentification)

If there is no database, the identification mode is out of service, but the authentication mode is still available.

This mode is activated by enabling one of the authentication with contactless card mode and identication mode.

Multi-factor mode	
app/bio ctrl/identification	1
And	
app/bio ctrl/authent PK contactless	0 or 1
app/bio ctrl/authent card mode	0 or 1

Required tag on card depends on the authentication mode.

Section 7

Proxy Mode

Sagem Sécurité
SAFRAN Group

1. Proxy mode (or slave) presentation

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

This operating mode allows to control the MorphoAccess® remotely (the link is IP) using a set of biometric and databases management commands.

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

- user identification,
- user verification,
- relay activation,
- read data on a contactless smart card,
- biometric database management (add/remove records),
- terminal configuration changes,
- read a contactless smart card.

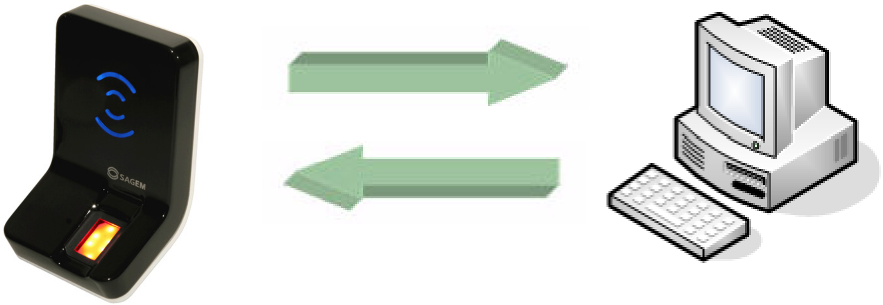


Figure 7 • 1: Proxy (slave) mode

Please refer to *MorphoAccess® Host System Interface Specification*: this document explains how to remotely manage a terminal.

For further details about SSL on the MorphoAccess®, please refer to the *SSL Solution for MorphoAccess®* documentation.

2. Proxy mode activation

To enable the proxy, all identification and authentication modes must be disabled. It means that all controls must be turned off: the terminal becomes a slave of the host system (the access control application is running on the host system).

Proxy mode	
app/bio ctrl/identification	0
app/bio ctrl/authent card mode	0
app/bio ctrl/authent PK contactless	0
app/bio ctrl/authent ID contactless	0
app/bio ctrl/bypass authentication	0

Section 8

Terminal Customization

Sagem Sécurité
SAFRAN Group

1. Setting up recognition mode

Two attempts mode

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

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

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

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

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

Parameters

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

By default, the two attempts mode is activated.

Setting up the number of attempts	
app/bio ctrl/nb attempts	1 (only one attempt) 2 (two attempts mode)

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

Setting up the identification timeout	
app/bio ctrl/identification timeout	5 (1-60)

In authentication mode a finger presentation period can be defined.

Setting up the authentication timeout	
app/bio ctrl/authent timeout	10 (1-60)

2. Setting up matching threshold

Setting up matching threshold	
bio/bio ctrl/matching th	3 (1-10)

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

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

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

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

3. Relay activation

If the control is successful, a relay may be activated to directly control a door.

Relay activation	
app/relay/enabled	1 (Enabled)

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

Relay aperture time in 10 ms	
app/relay/aperture time in 10 ms	300 (50 to 60,000)

The default state of the relay can also be defined. By default, the relay is opened when it is in idle state.

Relay default state	
app/relay/relay default state	0 (Opened) 1 (Closed)

❗ Access control installation using internal relay offers a lower security level, than an installation with a central access controller which is the only one allowed to open the door.

Relay external activation

MorphoAccess® relay is controlled by LED1 input	
app/relay/external control by LED1	1 (Enabled)

This function controls the relay with a push-button connected to LED1 input. It means either a successful recognition or a signal on LED1 will activate the relay.

- If LED1 is high impedance (push-button off) the relay is not activated.
- If LED1 is connected to GND (push-button on) the relay is activated.

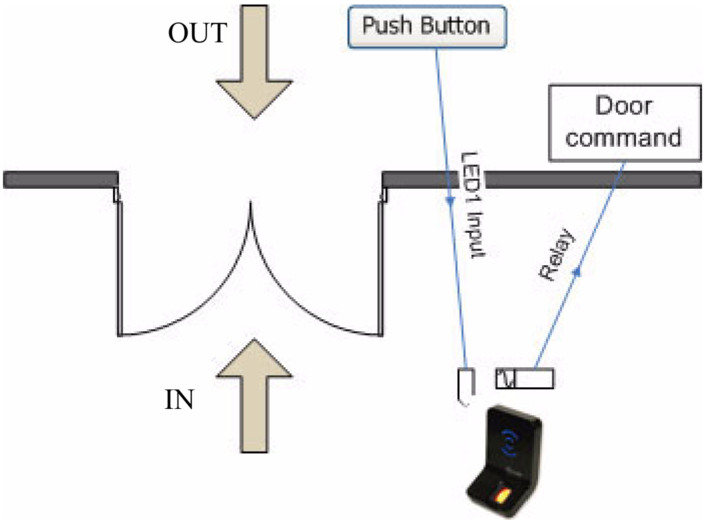


Figure 8 • 1: Internal relay activated by LED IN

Typically the MorphoAccess® relay controls the door.

- To enter in the building the user must be successfully recognized by the MorphoAccess®.
- A simple push-button connected to LED1 on the MorphoAccess® will trigger the door to leave the building.

4. LED IN feature

When this feature is activated, the terminal waits for an acknowledge signal (LED IN) from a Central Access Controller system, before granting the access.

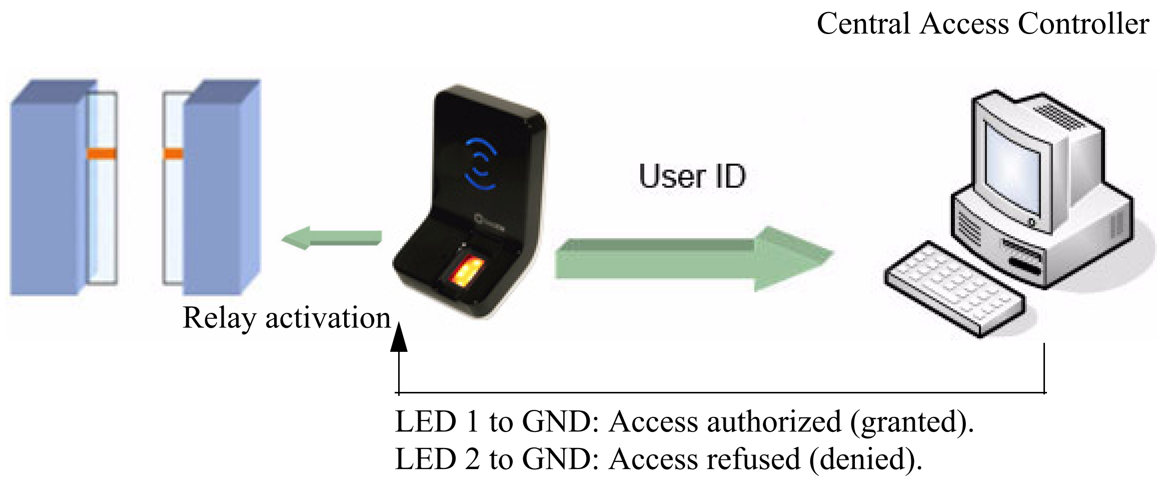

Central Access Controller
User ID
Relay activation
LED 1 to GND: Access authorized (granted).
LED 2 to GND: Access refused (denied).

Figure 8 • 2: LED IN feature

1.If the user is recognized the MorphoAccess® sends the user identifier to the controller.

2.The MorphoAccess® waits during an adjustable timeout, for the closure of a switch between LED1 and GND, or between LED2 and GND.

3.The controller checks the user's access rights.

4.The controller sets LED1 to GND to grant the access or sets LED2 to GND to deny the access In case of time-out, the access is also denied..

5.The "wait for access request" mode restarts only when LED1 and LED2 are reset to default state again.

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

LED IN mode activation	
app/led IN/enabled	1

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

LED IN acknowledgement timeout in 10 ms	
app/led IN/controller ack timeout	0 to 268435455

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

A controller with distinct outputs (one for "access forbidden", one for "access authorized") has to be connected to LED1 and LED2 I/O board

5. Access request log file

MorphoAccess® is logging its activities	
app/log file/enabled	1 (Enabled)

The terminal can log all access requests in a internal log file. It creates a record per access request.

The created record includes:

- the date and the time of record creation,
- the result of the access control (granted or denied, and if denied for which reason),
- the identifier of the user (if available).

It is possible to download the log file into the host system. For more information about this feature, refer to the *MorphoAccess® Host System Interface Specification*.

6. Remote messages: sending the User ID to the central security controller

After access control rights check, the MorphoAccess® can export the result of the control to a Central Security Controller, and can also log the result in a local diary, or activate a physical device, such as a door electric lock.

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

Presentation

The MorphoAccess® can send access control result message, after each access rights local check to a Central Security Controller by different means and through different protocols. This information can be used for instance to display on an external screen the result of a biometric operation, the name or the ID of the person identified, log the access request, perform additionnal access rights check depending on the role of the controller in the system.

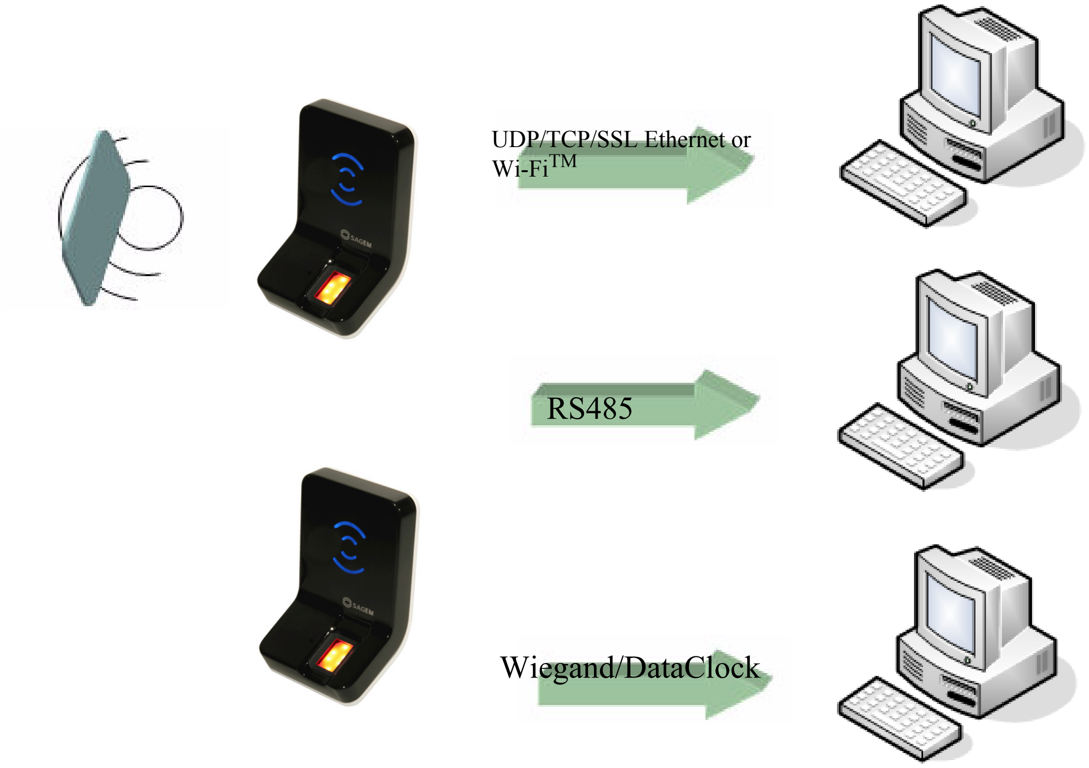


Figure 8 • 3: Sending access control result to a distant system

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

Supported protocols

The MorphoAccess® terminal can send access control result messages to a controller through the following protocols:

- Wiegand,
- Dataclock,
- RS485,
- IP (TCP or UDP or SSL) through Ethernet or Wi-Fi ™

For further information about the SSL on MorphoAccess® , please refer to *SSL Solution for the MorphoAccess®* documentation.

Note about terminal clock deviation

The message send through IP and RS485 includes the date/time of operation. The terminal clock has a +/- 4 sec per day typical time deviation at +25°C. At 50°C, the time deviation may be up to -8 sec per day.

For application requiring time precision (such as SSL, DESFire®), MorphoAccess® clock must be synchronized regularly with an external clock (using the appropriated ILV command).

7. Anti-tamper and anti-pulling switches

Description

The MorphoAccess® J Series, like the MorphoAccess® 500 Series, is able to detect two kinds of unsual events:

- the front glass is removed, by monitoring anti-tamper switches
- the terminal is removed from the wall, by monitoring the anti-pulling switches

When one of those event is detected, the MorphoAccess® J Series terminal acts as required by the related configuration key (see section below):

- Ignore the event (default) : usefull during normal maintenance operations
- Send an alarm message to the Central Access Controller, through the usual channel of the access control result messages (Wiegand, DataClock, RS485, Ethernet or Wi-Fi™.
- Generate an audible alarm signal with the buzzer and a visual alarm signal with the status LED.

Please refer to the *MorphoAccess® J Series Installation Guide* for more information about the anti-tamper and the anti-pulling switches.

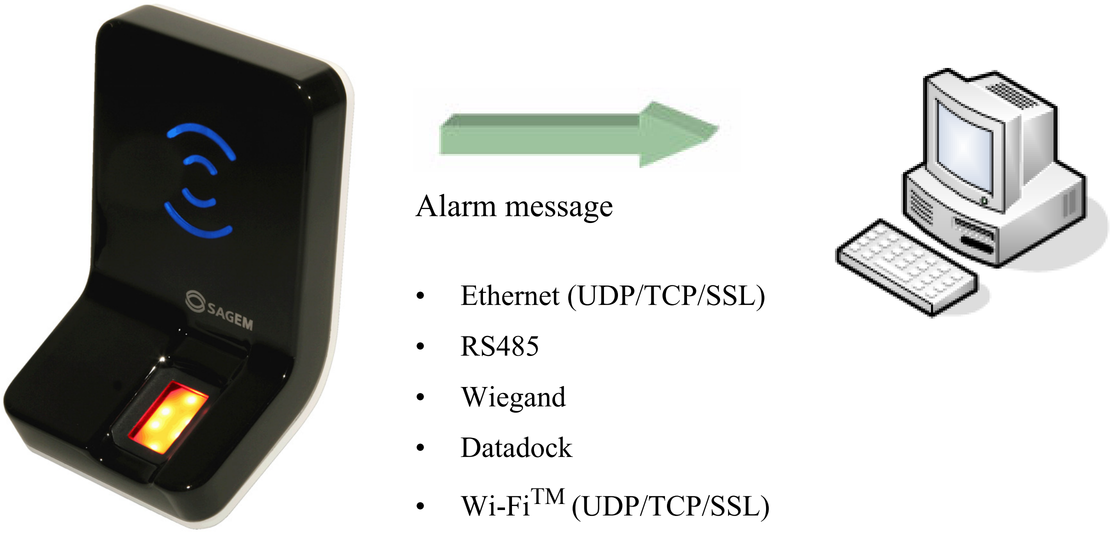


Figure 8 • 4: Tamper switch and anti-pulling switches

Configuration keys

To send an alarm on an output (Ethernet, RS485, Wiegand, Dataclock, Wi-Fi™), the corresponding interface must be activated otherwise no alarm will be sent.

Because RS485, Wiegand, and Dataclock are multiplexed on the same lines, only one of these protocols shall be enabled at one time, else priority is given to Wiegand, then Dataclock, then RS485.

Those configuration keys are:

- app/send ID wiegand/enabled,
- app/send ID dataclock/enabled,
- app/send ID serial/enabled,
- app/send ID serial/mode (to select RS485 link),
- app/send ID UDP/enabled,
- app/send ID ethernet/mode (to choose between UDP or TCP),
- app/send ID ethernet/SSL enabled (Please refer to SSL Solution for MorphoAccess® documentation).

Setting the configuration key a*pp/tamper alarm/level* to an appropriate value configure security switch management feature.

Tamper Alarm Level	
app/tamper alarm/level	0 (0 - 2)
0 Anti-pulling and anti-tamper switches ignored. **1** An alarm message is sent to the controller by the same channel as the access control result message (if enabled). **2** In addition to previous level, the terminal buzzer outputs an audible alarm signal, and the terminal status LED displays a red blinking light.	

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

Tamper Alarm ID	
app/failure ID/alarm ID	65535 (0 - 65535)
app/failure ID/enabled 1 (Enabled)	1

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

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

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

The configuration key *app/failure ID/alarm ID* must be set to 62221 to link the intrusion event to this identifier and the configuration key *app/failure ID/enabled* must be set to 1.

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

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

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

8. Setting up time mask

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

Time mask activation	
app/modes/time mask	1 (Enabled)

To use this feature the local database must have been created with a **specific additional field**. If this field does not exist activating this feature will forbid the access to every user.

Please refer to *MorphoAccess*® *Host Interface Specification* to understand how to create a database with time mask feature.

SECTION 9

MAN MACHINE INTERFACE

Sagem Sécurité
SAFRAN Group

1. Convention

Intermittent "Pulse": led is 1 second OFF, 0.05 second ON.

For example:.

Intermittent blue "Pulse"

Fast "Pulse": led flashes quickly. The rhythm is the same than when a hard drive works.

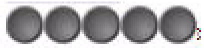
Intermittent orange "Pulse"

Slow intermittent Fast orange "Pulse" "Pulse": led is 1 second OFF, 1 second ON.

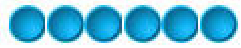
For example:

Slow intermittent red "Pulse"

2. Identification - Waiting for a finger on the sensor

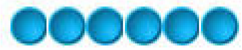
Sensor	ON	
Led	OFF	

3. Authentification - waiting for user's contactless card

Sensor	ON	
Led	ON "blue"	

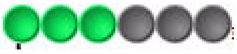
MAN MACHINE INTERFACE

4. Multi-factor mode - waiting for user’s finger or contactless card

Sensor	ON	
Led	ON "blue"	

5. Access granted

The user is recognized and the access is allowed.

Sensor	ON	
Led	Green 1 second	
Buzzer	ON 0.1 second - High - pitched	♪

6. Access denied

The user is not recognized, or the access is not allowed to this user (by Time Mask feature or by Central Access Controller).

Sensor	ON	
Led	Red 1 second	
Buzzer	ON 0.7 second - Low - pitched	♪

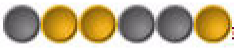
7. Timeout while waiting for finger on the sensor

Time-out occurs during the wait for a valid fingerprint on the sensor (authentication only).

Sensor	ON	
Led	Red 1 second	
Buzzer	ON 0.7 second - Low - pitched	♪

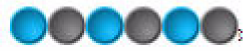
8. No database or empty database

The selected access control mode requires at least one record in the local database.

Sensor	OFF	
Led	Slow intermittent yellow «Pulse»	

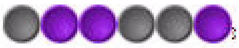
9. USB mass storage key can be removed

When a USB Mass Storage key is used to configure the terminal, and when the configuration process is completed, the USB Mass Storage key can be removed from the USB port.

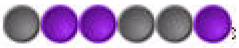
Sensor	-	-
Led	Fast intermittent cyan «Pulse»	
Buzzer	ON 2 medium-pitched beeps	♪

10. Terminal maintenance

A configuration operation is in progress (biometric database update, configuration key value change, access request log file acquisition, etc…). Normal process will be available again as soon as the configuration operation is completed. This signal is displayed during remote management through TCP, and during USB mass storage key processing.

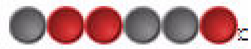
Sensor	OFF	
Led	Slow intermittent purple «Pulse»	

Sensor firmware update is in progress (only after start up of the terminal after a terminal firmware update)..

Sensor	Alternaly on, off	
Led	Slow intermittent purple «Pulse»	

11. Sensor start up error

The terminal fails to start the biometric sensor. If the trouble persists after several terminal start-ups, please contact customer service.

Sensor	OFF	
Led	Slow intermittent red «Pulse»	

SECTION 10

APPENDIX

1. MorphoAccess® 100 and 500 Series compatibility

The MorphoAccess® J Series is fully compatible with the MorphoAccess® 100 and 500 Series devices.

2. MorphoAccess® 200 and 300 Series compatibility

This tables present parameters equivalence between MorphoAccess® J Series and MorphoAccess® 220 and 320 Series.

Multi-factor mode (/cfg/Maccess/Admin/mode 5 on MorphoAccess® 200 and 300 Series) is activated when *app/bio ctrl/identification* is set to 1.

MA220/320	MorphoAccess® J Series equipped with a MIFARE® /DESFire® contactless smartcard reader
Contactless authentication with ID on card, template in local database	
/cfg/Maccess/Admin/ mode 4	app/bio ctrl/authent ID contactless 1
Contacless authentication: card mode	
/cfg/Maccess/Contactless/ without DB mode 0 **/cfg/Maccess/Admin/ mode 3 or**	app/bio ctrl/authent card mode 1
/cfg/Maccess/Admin/mode 5 **(multi-factor mode)**	app/bio ctrl/identification 1
Contactless authentication: Biometric verification	
/cfg/Maccess/Contactless/ without DB mode 2 **/cfg/Maccess/Admin/ mode 3 or**	app/bio ctrl/authent PK contactless 1
/cfg/Maccess/Admin/mode 5 (multi-factor mode)	app/bio ctrl/identification 1
Contactless authentication: ID «only», no biometric verification	
/cfg/Maccess/Contactless/ without DB mode 1 **/cfg/Maccess/Admin/ mode 3 or**	app/bio ctrl/authent PK contactless 1 app/bio ctrl/bypass authentication 1

/cfg/Maccess/Admin/mode 5 (multi-factor mode)	app/bio ctrl/identification 1

3. Contactless Card modes table

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

Operations	Authent card mode	Authent PK contactless	Authent ID contactless	Bypass authenti-fication
Authentication with templates on card - biometric control disabled Read ID on contactless card. Send ID.	0	1	0	1
Card mode authentication - biometric control disabled Read card mode, ID, templates (if required by card mode) on contactless card. Whatever card mode, send ID.	1	0	0	1

4. Required tags on User's contactless card

Operations	ID	Card Mode	PK1	PK2	PIN	BIOPIN
Authentication with templates in database	Yes	No	No	No	No	No
Authentication with templates on card	Yes	No	Yes	Yes	No	No
Card mode authentication (ID_ONLY)	Yes	Yes	No	No	No	No
Card mode authentication (PKS)	Yes	Yes	Yes	Yes	No	No
Authentication with templates in database - biometric control disabled	Yes	No	No	No	No	No
Authentication with templates on card - biometric control disabled	Yes	No	No	No	No	No
Card mode authentication (ID_ONLY) - biometric control disabled	Yes	Yes	No	No	No	No
Card mode authentication (PKS) - biometric control disabled	Yes	Yes	Yes	Yes	No	No

with :

- ID : User identifier
- Card Mode : enable/disable fingerprint check
- PK1 : User's fingerprint #1
- PK2 : User's fingerprint #2
- PIN : Personal Identification Number (not supported)
- BIOPIN : biometric PIN (not supported)

5. Troubleshooting

Terminal IP address is unknown or terminal is not reachable

Use *USB Network* Tool to set a valid network address in your terminal. Refer to *USB Network Tool User Guide*.

Sensor is off

Verify that the base contents at least one record.

Check that identification mode is enabled.

Terminal returns erratic answers to ping requests

Check the subnet mask. Ask your network administrator for the right value.

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

6. Bibliography

The documents below are available on a CD/ROM package from factory or downloadable on our web site at www.biometric-terminals.com (login and password required).

Administrator Information

MorphoAccess® J Series User Guide
This document describes operating mode and terminal settings

MorphoAccess® Parameters Guide
The complete description of terminal configuration files

SSL Solution for MorphoAccess®
The complete description of the SSL Solution deployment for MorphoAccess®

Installation Information

MorphoAccess® J Series Installation Guide
This document describes terminal physical mounting procedure, electrical interfaces and connection procedures

Developer Information

MorphoAccess® Host Interface Specification
A complete description of remote management commands

MorphoAccess® Remote Messages Specification
Details how the MorphoAccess® sends the access control result to a Central Security Controller

MorphoAccess® Contactless Card Specification
This document describes the MorphoAccess® contactless card feature

Support Tools

Configuration Tool User Guide
Configuration Tool user guide, via IP

USB Tool User Guide
Configuration Tool user guide, via USB mass storage key

Upgrade Tools User Guide
Upgrade Tool user guide about firmware upgrading procedures

SECTION 11

SUPPORT

Sagem Sécurité
SAFRAN Group

Customer service

Sagem Sécurité

SAV Terminaux Biométriques

Boulevard Lénine - BP428

76805 Saint Etienne du Rouvray

FRANCE

Phone: +33 2 35 64 55 05

Hotline

Sagem Sécurité

Support Terminaux Biométriques

18, Chaussée Jules César

95520 Osny

FRANCE

hotline.biometrics@t.my-technicalsupport.com

Phone: + 33 1 58 11 39 19 (9H00am to 6H00pm French Time, Monday to Friday)

http://www.biometric-terminals.com/

http://www.sagem-securite.com/