Sagem Sécurité
SAFRAN Group

MorphoAccess®

Remote Messages Specification

Produced by Sagem Sécurité

www.sagem-securite.com

Table of Contents

REVISIONS HISTORY

Date	Description
May 2010	Add MorphoAccess® J Series

SCOPE OF THE DOCUMENT

This guide relates to the use of MorphoAccess® access control terminals:

- MorphoAccess® 100 Series
- MorphoAccess® J Series
- MorphoAccess® 500 Series

MorphoAccess® 100 Series are made up of following list of products:

		Biometrics	Contactless Smartcard Reader		
			iClass™	MIFARE™	DESFire™
MA 100 Series	MA 100	√			
	MA 110	√	√		
	MA 120	√		√	
	MA 120 D	√		√	√

MorphoAccess® J Series are made up of following list of products:

		Biometrics	Contactless Smartcard Reader	
			MIFARE™	DESFire™
	MorphoAccess®	√		

MorphoAccess® 500 Series is a generic appellation which gathers MorphoAccess® terminals belonging to MA 500+ Series, OMA 500 Series and MA 500 Series. Corresponding list of products is depicted in the table below.

		Biometrics	Contactless Smartcard Reader		Fake Finger Detection	Outdoor
			MIFARE™	DESFire™		
MA 500+ Series	MA 500+	√				
	MA 520+ D	√	√	√		
	MA 521+ D	√	√	√	√	
OMA 500 Series	OMA 520 D	√	√	√		√
	OMA 521 D	√	√	√	√	√
	OMA 520	√	√			√
	OMA 521	√	√		√	√
MA 500 Series	MA 500	√				
	MA 520	√	√			
	MA 521	√	√		√	

REFERENCES

Reading the following manuals may be useful to understand the functionalities presented in this document:

- Sagem Sécurité MorphoAccess® Installation Guides,
- Sagem Sécurité MorphoAccess® User Guides,
- Sagem Sécurité MorphoAccess® Host System Interface Specification,
- Sagem Sécurité SSL Solution for MorphoAccess®.

SUPPORTED PROTOCOLS

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

- Wiegand,
- Dataclock,
- RS485/422 (RS422 is only available on MorphoAccess® 500 Series),
- IP.

The format of the messages frames differs according to the protocol chosen. Note that Wiegand/Dataclock messages can be also enriched with extended error ID. This feature is described in section Wiegand or Dataclock: failure messages.

	Verification OK	Verification KO
Wiegand *The terminal acts as a magnetic badge reader.*	The ID of the identified user is sent. The frame format can be configured.	Nothing is sent. Or numerical ID describing the cause of the failure.
Dataclock *The terminal acts as a magnetic badge reader.*	The ID (ISO2) of the identified user is sent.	Nothing is sent. Or numerical ID describing the cause of the failure.
RS485/422 (*RS422 is only available on MorphoAccess®*	Identification result is sent.	The biometric check result (failure) is sent.

REMOTE MESSAGES ACTIVATION

Configuration of the protocols

The MorphoAccess® terminal can send remote messages at the same time through several channels (for example: Wiegand and IP). This chapter explains how to activate the sending of the remote messages for each channel available: Wiegand/Dataclock, Serial, and IP.

The configuration of each protocol requires modifying some parameters. If you do not know how to perform such operation, please refer to the *User Guide* of the MorphoAccess® terminal.

Parameters can be changed using remote management commands.

Wiegand – Dataclock

These outputs are multiplexed. It means that only one of them can be enabled: (TR- / D1) and (TR+ / D0).

Priority is given to *Wiegand* then *Dataclock*.

NOTE: It means activating Dataclock with Wiegand enabled will have **no effect** on the Dataclock layer.

On MorphoAccess® 100 Series and J Series, Wiegand, Dataclock and RS485 are multiplexed on the same serial port. Priority is given to *Wiegand* then *Dataclock* then *RS485.*

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 the 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.

app/send ID wiegand/frame length	
1-128	Defines the number of bits of the frame.
app/send ID wiegand/start format (before v2.00*: app/send ID wiegand/start*)	
	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.
app/send ID wiegand/stop format (before v2.00*: app/send ID wiegand/stop*)	
	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.
app/send ID wiegand/site format (before v2.00: *app/send ID wiegand/site*)	
n.m	Insert m bits of site value at offset n.
app/send ID wiegand/ID format (before v2.00*: app/send ID wiegand/ ID*)	
n.m	Insert m bits of ID value at offset n.

app/send ID wiegand/custom format (before v2.00*: app/send ID wiegand/custom*)	
0.0	Reserved for Sagem Sécurité custom protocols.

Wiegand « any bit » examples

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
```

26-bits: 24 bits ID

```
/Length: 26

/Start: 2.12    //even parity calculated over the first 12
bits

/Site: 0.0      //no facility code

/ID: 1.24       //3-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
```

DATACLOCK REMOTE MESSAGES

Presentation

The payload data encapsulated in a Dataclock frame is either the ID of the person identified, in case of successful identification, or an ID describing the reason of the identification failure (if the Failure ID are activated, see chapter Wiegand or Dataclock: failure messages).

Dataclock frame content is described in section Appendix 3 - ISO 7811/2 - 1995 - Track 2 Dataclock Format.

Activation

A configuration entry allows enabling the Dataclock output.

app/send ID dataclock/enabled	
0	ID is not sent (default).
1	ID sent.

WIEGAND OR DATACLOCK: FAILURE MESSAGES

Presentation

Failure ID option allows sending extended error codes through the Wiegand or Dataclock layer. You can activate this option and associate any value between 0 and 65535 for each existing failure case.

NOTE: This feature has no impact on the IP and Serial (RS422/RS485) remote messages.

The administrator has to check that the identifier is not already stored in the database.

Software Configuration

app/failure ID/enabled	
0	Nothing is sent through Wiegand or Dataclock when biometric control fails.
1	A specific identifier is sent through Wiegand or Dataclock when biometric control fails.

Specific identifier can be associated with a given failure case.

app/failure ID/not recognized ID	
0 - 65535	This value is sent when a user is not identified (i.e. a biometric operation has failed).
app/failure ID/timeout ID	
0 - 65535	This value is sent when the identification/verification operation aborts due to a timeout error.

app/failure ID/alarm ID	
0 - 65535	This value is sent when the back cover is removed (tamper switch detection).
Since v2.00 : app/failure ID/not on time ID	
0 - 65535	This value is sent when the access is refused due to the time mask

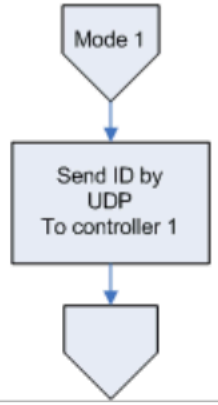
Activation of simple UDP

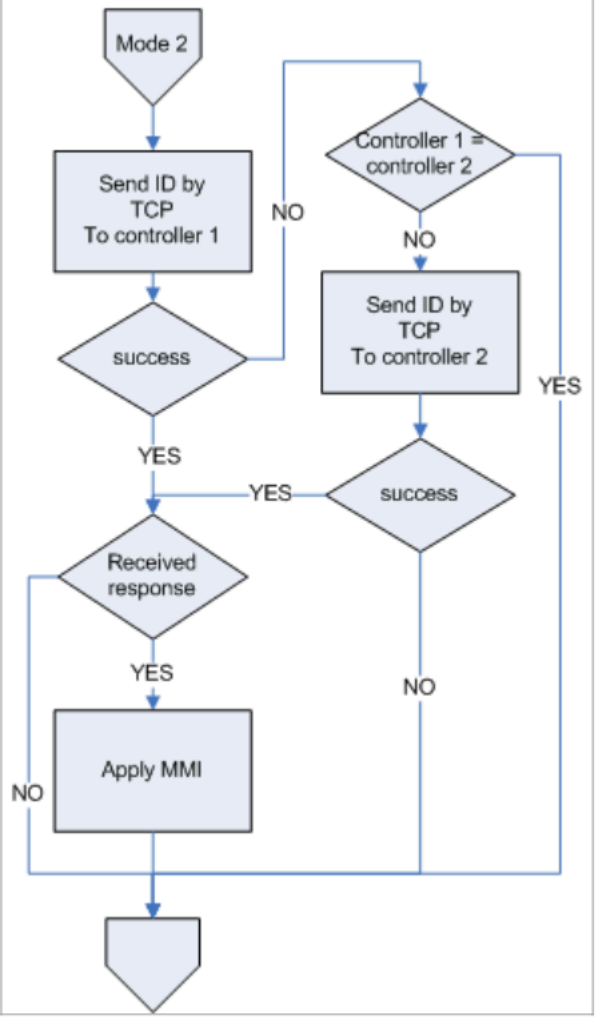
Configuration keys allow enabling the UDP remote messages.

app/send ID UDP/enabled	
0	Messages sending deactivated on the IP link.
1	Messages sending activated on the IP link.
app/send ID UDP/host name	
Hostname	It defines the destination computer on the networks.
app/send ID UDP/host port	
11020	IP messages are sent to the port 11020 through UDP protocol, but the port can be modified. **Note:** Check that your firewall is correctly configured.

Activation of enhanced TCP features

Configuration keys allow enabling the IP remote messages.

app/send ID ethernet/mode		
0	Messages sending deactivated on the IP link.	
1	Messages sending activated in UDP protocol. Not that this way should be used only in case of enhanced UDP/TCP mode and not for simple UDP logging. See value 3 of this mode for more details.	

app/send ID ethernet/mode		
2	Messages sending activated in TCP protocol. In this mode, a second controller could be used in case of failure (see schema for details). If controllers 1 and 2 have the same IP and port, controller 2 is disabled and the MorphoAccess® never tries to connect to it.	

- 1 (default value): if connection to controller failed, or an erroneous response is received from controller, then the MorphoAccess® terminal can act as controller. If the biometric control result was “Access Allowed”, the access is granted.

/app/send ID ethernet/controller on no response	
0 or 1	Let the MA act as controller or not (default is 1, for true).

This key is used only in modes 2 and 3 (TCP connected modes).

Default controller definition

app/send ID ethernet/controller 1 IP	
10.10.161.39	It defines the controller’s IP on the network.
app/send ID ethernet/controller 1 port	
11020	It defines the controller’s port on the network **Note:** Check that your firewall is correctly configured.
app/send ID ethernet/controller 1 timeout	
2000	Timeout used for connection, reading and writing data (at TCP/UDP level) to/from the remote controller. In multiple of 10ms (2000 means 20 seconds)

Alternative controller definition

It is possible to define an alternative controller on the network. This alternative controller is reached when the default controller has not been reached in duration specified by timeout.

To enable the alternative controller, set alternative controller’s IP or port

different from default controller. Both could have the same IP and different ports (same computer) or different IP and same port (several machines).

To disable the alternative controller, set the alternative controller's IP and port to default controller's values.

app/send ID ethernet/controller 2 IP	
10.10.161.39	It defines an alternative destination computer on the network.
app/send ID ethernet/controller 2 port	
11020	It defines the alternative computer port on the network. **Note:** Check that your firewall is correctly configured.
app/ send ID ethernet/controller 2 timeout	
2000	Timeout used for connection, reading and writing data (at TCP/UDP level) to/from the remote controller. In multiple of 10ms (2000 means 20 seconds)
app/send ID ethernet/back to controller 1 timeout	
0 to 7200	When alternative controller is activated, on connection to default controller failure the terminal switches to alternative controller. While the duration of timeout “back to controller 1 timeout” it firstly tries to connect to alternative controller, before switching to default terminal. Value of 0 means that default controller is always reached before alternative controller.

SSL securing

To secure the system with SSL, see *SSL Solution for MorphoAccess®* and the *MorphoAccess® Series Parameters Guide Documentation*.

Message filtering

MorphoAccess® terminal is able to send only certain messages by filtering.

app/failure ID/send ID mask	
0 to 7200	This mask let the administrator select the mask to apply as filter. Setting this key to 255 means all is sent. What can be sent is: - 1: User authorized - 2: User not recognized or authorized - 4: User is not on time (Time and attendance functionality) - 8: Timeout on biometric operation - 16: Fake finger detected (only on MA521) - 32: error - 64: error authent PK (only in authent PK mode) - 128: tamper Alarm detected

For example to send only the user ID when the user is authorized and when the user is not recognized, set this key to 3 (equals to 1 (message “User authorized “) + 2 (message “User not recognized or authorized”)).

Developers can recognize a bit field mask (set in decimal representation in Sagem Sécurité configuration tools).

IP - Message sent by MorphoAccess® terminal when control is OK

Description

This frame is sent to the controller when the user is recognized.

In connected mode (TCP) the server can send a reply to specify a MMI (Man Machine Interface) state. That means that a special state can be set by controller to relay, LED, buzzer and screen text.

Frame sent when control is OK

Identifier value	**0x00**: User ID is sent in ASCII format and control succeeded.	1 byte
Length value	0x0000 + L *+ 1 + 17*	2 bytes
Value (Parameters)	User ID	L bytes
	Attendance Status (T&A only)	*1 byte*
	MA date and hour (T&A only)	*17 bytes*

User ID

User identifier in ASCII. “94066” for example.

Attendance Status (Time & Attendance enabled : MorphoAccess® 500 Series only)

This is an ASCII character defining the transaction performed :

0x49 = ‘ I ’ : IN

0x4F = ‘ O ’ : OUT

0x69 = ‘ i ’ : IN DUTY

0x6F = ‘ o ‘ : OUT DUTY

If Extended Time & Attendance is activated and the pressed key is associated to the “user defined” function, ASCII code of the key is sent.

If Extended Time & Attendance is activated and the key pressed is associated to one of the four standard functions (IN, OUT, Temporary IN, Temporary OUT), the sent code is the one of the above ones.

MA date and hour (Time & Attendance enabled)

A 17 bytes ASCII buffer formatted as follows: “ HH/MM/SS DD:MM:YY”

Example

This frame means user “528610” has been recognized.

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9
0x00	0x06	0x00	0x35	0x32	0x38	0x36	0x31	0x30
OK	L = 6 bytes		User identifier: “528610”					

Attendance Status (Time & Attendance enabled)

This is an ASCII character defining the transaction performed :

0x49 = ‘ I ’ : IN

0x4F = ‘ O ’ : OUT

0x69 = ‘ i ’ : IN DUTY

0x6F = ‘ o ‘ : OUT DUTY

If Extended Time & Attendance is activated and the pressed key is associated to the “user defined” function, ASCII code of the key is sent.

If Extended Time & Attendance is activated and the key pressed is associated to one of the four standard functions (IN, OUT, Temporary IN, Temporary OUT), the sent code is the one of the above ones.

MA date and hour (Time & Attendance enabled)

A 17 bytes ASCII buffer formatted as follows: “ HH/MM/SS DD:MM:YY”

Examples

Identification mode: this frame means that identification failed.

Byte 1	Byte 2	Byte 3	Byte 4
0x10	0x01	0x00	0x01
NOK	L = 1 byte		Identification failed

Verification mode: this frame means the user “528610” presented its badge, but biometric verification failed.

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9	Byte 10
0x10	0x07	0x00	0x01	0x35	0x32	0x38	0x36	0x31	0x30
NOK	L = 7 bytes		Verification failed	User identifier: “528610”					

IP - Tamper alarm sent by MorphoAccess® terminal

Description

This frame is sent to the controller when the tamper switch is activated.

The device can send an alarm through IP communication port. It can also play a sound alarm while sending the Alarm ID.

In case of intrusion, the alarm is emitted.

Enabling

To enable tamper alarm, set the key *app/tamper alarm/level* to value:

- **1**: checks alarm state every second, then sends the alarm to the remote controller using IP (see section ***Activation of enhanced TCP features*** in this document) every 15 seconds (default value. See below to modify it),
- **2**: same as level 1 but also emits a sound and a LED red flash every second in case of intrusion.

Sending

The key *app/send ID ethernet/interval* must be set to the duration between IP frames sending (for example, value 1500 (*10ms) means that the alarm will be sent every 15 seconds.

In case of TCP mode, the terminal does not wait for response.

Command: sent frame

Identifier value	**0xC1**: ILV_ALARM_ID.	1 byte
Length value	0x04	2 bytes
Value (Parameters)	Alarm state	4 bytes

Alarm state

IP (TCP/SSL) - Basic MMI Answer (returned by the controller)

Description

On reception of the frame “Control OK” and after checking the user is authorized. The controller returns this frame on the established socket (same connection).

With this response, the relay is switched on only if the key *app/relay/enabled* is enabled. If the key is disabled, nothing happens.

Command: frame returned by the controller to the MorphoAccess®

Identifier value	**0x50**: Access status.	1 byte
Length value	1	2 bytes
Value (Parameters)	Access Granted or Denied	1 byte

Access Granted or Denied

0x00: Access is granted: the MorphoAccess® terminal status LED is green and short beep is emitted. If the relay is activated, it switches on (else stays off).

0xFF: Access is denied: the MorphoAccess® terminal status LED is red and long beep is emitted.

0x01 or any other value: nothing happens. MorphoAccess® terminal goes back in control mode.

Example

This frame means user cannot enter in the zone protected by the MorphoAccess® terminal.

Byte 1	Byte 2	Byte 3	Byte 4

0x50	0x01	0x00	0xFF
AS	L = 1 byte		Access is denied

This frame means user can enter in the zone protected by the MorphoAccess® terminal.

Byte 1	Byte 2	Byte 3	Byte 4
0x50	0x01	0x00	0x00

IP (TCP/SSL) - Enhanced MMI Answer (returned by the controller)

Description

On reception of the frame “Control OK”, the controller could response with this command.

This ILV defines the user interface (LED, buzzer, screen text and relay) in a particular state for a defined time.

The same ILV can be sent “empty”. That means it does not contain an ILV configuration.

Command

Frame returned by the controller to the MorphoAccess® terminal:

Identifier value	**0x51**: MMI Order.	1 byte
Length value	95	2 bytes
Value (Parameters)	Beep duration	1 byte
	Relay state	1 byte
	Relay duration	1 byte
	LED state	1 byte
	Text line 1	30 bytes
	Text line 2	30 bytes
	Text line 3	30 bytes
	Text duration	1 byte

Beep duration

Duration for beep buzzing in 10ms (value 100 means 1 second). Range = [0, 100]

Relay state

The state applied to the relay:

0 = close

1 = open

2 is no longer used in MorphoAccess® terminal (only close and open are allowed)

Relay duration

Duration of the relay opening in 100ms (value 10 means 1 second). Range = [0, 100]

LED state

The LED state applied during the UI using 0 = LED OFF, 1 = RED LED, 2 = GREEN LED.

The led state will be applied during all the time of the MMI state.

Text duration

Duration of the screen text display in 100 ms (value 10 means 1 second).

Text Line i

NULL terminated strings containing the text to show on screen. Only the 22

Example and recommended values

	Identification succeeded	Identification failed
Beep duration	1	2
Relay state	OPEN (0x01)	CLOSE (0x00)
Relay duration	30	3 (not really used, but must respect the order rule)
Led State	GREEN (0x02)	RED (0x01)
Text duration	45	20

Activation

A configuration entry allows choosing between RS485 and RS422 protocols for sending messages.

app/send ID serial/mode	
0	No link selected.
422	RS422 protocol selected (MorphoAccess® 500 Series only).
485	RS485 protocol selected.

This key (mode) does not enable sending messages on serial link.

The following key activates or not sending messages on serial link.

app/send ID serial/enabled	
0	Messages are not sent.
1	Messages are sent.

Terminal identifier

This parameter allows setting an address defining the MorphoAccess® terminal identifier on the RS485 bus.

app/send ID serial/terminal identifier	
0-255	This value defines a MorphoAccess® on the RS485 bus.

Terminal identifier set to DLE[0x1B], XON[0x11] or XOFF[0x13] is forbidden.

This *Terminal Identifier* can be retrieved in the low layer serial protocol

described in Appendix 2: RS485 Protocol.

Terminal Identifier does not exist for RS422. This field is replaced by the Request Counter field (see Appendix 3: RS422 Protocol).

Serial link settings

It is possible to set the baud rate, the data and stop bits size and to select the parity type.

app/send ID serial/speed
1200, 2400, 4800, 9600, 19200, 28800, 38400, 57600 or 115200 (in bps)

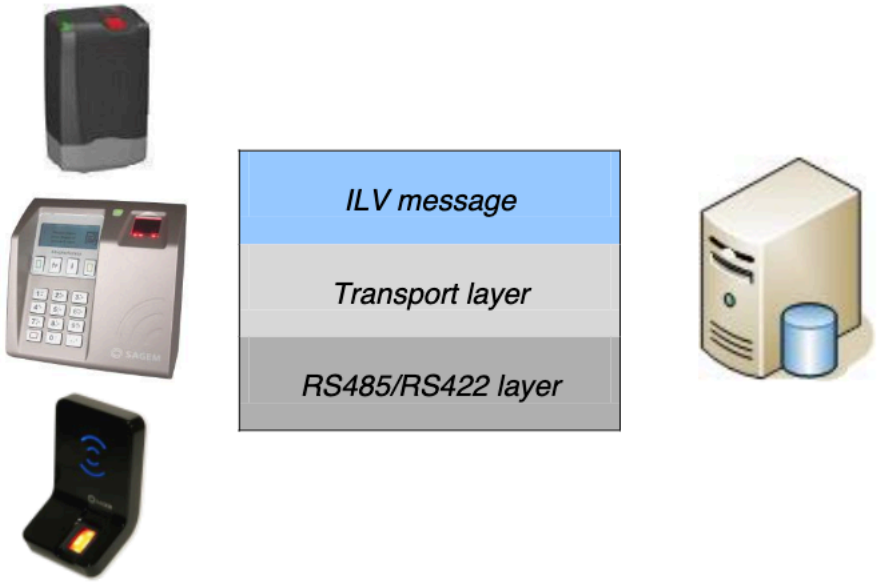
app/send ID serial/databits
7 or 8 (databits).

app/send ID serial/parity	
0	No.
1	Odd.
2	Even.

app/send ID serial/stopbits
1 or 2 (stop bits).

Data Format

Remote information is sent on the RS485 or RS422 (MorphoAccess® 500 Series only) serial channel. The transport layer ensures the transmission and ensures frame acknowledgement.



It is possible to send the frame again in case of failure. When using a RS485 serial layer, the terminal uses an anti-collision protocol to prevent collisions on the link.

The RS485 protocol is described in Appendix 2: RS485 Protocol.

The RS422 protocol is described in Appendix 3: RS422 Protocol.

RS485/RS422 - Message format

Messages sent though RS485 or RS422 have the following format named **ILV**.

***ILV** messages*		

Identifier	Length	Value
1 byte	2 bytes	Length bytes
Message identifier	*Message data length (little endian format)*	*Message data*

The application data has three fields:

- **Identifier** called **I**: this is the identifier of the command,

This is an ASCII character defining the transaction performed:

0x49 = ‘ I ’ : IN

0x4F = ‘ O ’ : OUT

0x69 = ‘ i ’ : IN DUTY

0x6F = ‘ o ‘ : OUT DUTY

If Extended Time & Attendance is activated and the pressed key is associated to the “user defined” function, ASCII code of the key is sent.

If Extended Time & Attendance is activated and the key pressed is associated to one of the four standard functions (IN, OUT, Temporary IN, Temporary OUT), the sent code is the one of the above ones.

MA date and hour (Time & Attendance enabled)

A 17 bytes ASCII buffer formatted as follows: “ HH/MM/SS DD:MM:YY”

RS485/RS422 - Message sent when control is NOK

Description

This frame is sent to the controller when the control failed. The format of the ID can be specified.

Command: frame sent

Identifier value	**0x10**: User ID is sent in ASCII format	1 byte
Length value	1+ L	2 bytes
Value (Parameters)	Biometric Error Code	1 byte
	User ID (according to the configuration)	*L bytes*
	Attendance Status (T&A only)	*1 byte*
	MA date and hour (T&A only)	*17 bytes*

Biometric Error Code

Failure: CONTROL_FAILED [0x01]

“Timeout”: CONTROL_TIMEOUT [0x19]

User not in base: LOG_NOT_IN_BASE [0x12]

Generic error: LOG_ IDENT_ERROR [0xFF]

Attendance Status (Time & Attendance enabled)

This is an ASCII character defining the transaction performed:

0x49 = ‘ I ’ : IN

0x4F = ‘ O ’ : OUT

0x69 = ‘ i ’ : IN DUTY

0x6F = ‘ o ‘ : OUT DUTY

If Extended Time & Attendance is activated and the pressed key is associated to the “user defined” function, ASCII code of the key is sent.

If Extended Time & Attendance is activated and the key pressed is associated to one of the four standard functions (IN, OUT, Temporary IN, Temporary OUT), the sent code is the one of the above ones.

MA date and hour (Time & Attendance enabled)

A 17 bytes ASCII buffer formatted as follows: “ HH/MM/SS DD:MM:YY”

User ID

User identifier (returned for a verification only):

“27321” will be 0x32 0x37 0x33 0x32 0x31 in ASCII.

RS422 - Wait for an access controller reply

Description

On RS422 mode, if the control succeeds the MorphoAccess® 500 Series displays the message and sends the ID to a reader (i.e. MK2) that transmits it to a controller (i.e. Blueline). The controller makes a decision on the ID and sends the response and a message (16 characters maximum, one line at a time) back to the reader according to the RS422 data format. Then the reader transmits the same message to the MorphoAccess® 500 Series to display on its screen.

If the control fails the MorphoAccess® terminal behavior is the usual one.

To activate this mode the MorphoAccess® 500 Series must be configured to send an ID on RS422 and to wait a reply from a reader on RS422. (Keys *app/send ID serial/mode at RS422, app/send ID serial/enabled at 1, app/send ID serial/wait reply at 1)*.

app/send ID serial/wait reply	
0	Reply from a controller is not waited
1	Reply from a controller is waited

app/send ID serial/ reply timeout	
5-3600	Timeout (in second) of the reply coming from the reader

app/send ID serial/display duration	
3-3600	Display duration (in second) of the message on the MorphoAccess® 500 Series screen.

EVENTS REMOTE MESSAGES

Since firmware 2.11, all the MorphoAccess® terminals are able to send messages when specific events occurred. Please refer to the MorphoAccess® terminal's User Guide for further details about this feature.

Internal log file full Message

Description

Once the internal log file is full, the terminal can send a message each time a line is being written in the file.

Message sent

Identifier value	**0x02**: LOGFULL_MESS_ID	1 byte
Length value	0x01	2 bytes
Value (Parameters)	*Response needed*	1 bytes

Response needed

If set to 0x01, the terminal will wait for a response after having sent the message.

If set to 0x00, the terminal will end the communication after having sent the message.

Note1: Even if the response needed is set to one, no specific treatment is made on the response.

Note2: This parameter should be coherent with the terminal configuration.

Message sent

Identifier value	**0x01**: BIOCHG_MESS_ID	1 byte
Length value	1 + m +n	2 bytes
Value (Parameters)	*Response needed*	1 bytes
	TLV Terminal SN	m bytes
	TLV Log File	n bytes

Response needed

If set to 0x01, the terminal will wait for a response after having sent the message.

If set to 0x00, the terminal will end the communication after having sent the message.

Note1: This parameter should be one, because the access control application considers the sending OK, after having received a specific response.

Note2: This parameter should be coherent with the terminal configuration.

TLV Terminal SN

The terminal's serial number at the TLV format:

T	**0x00**: MASN_ID	1 byte
L	X	2 bytes
V	*Terminal SN*	X bytes

TLV Log File

The name of the file containing the biometric changes

T	**0x01**: MALOGFILE_ID	1 byte
L	X	2 bytes
V	*Log File Name*	X bytes

APPENDIX 1: 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.

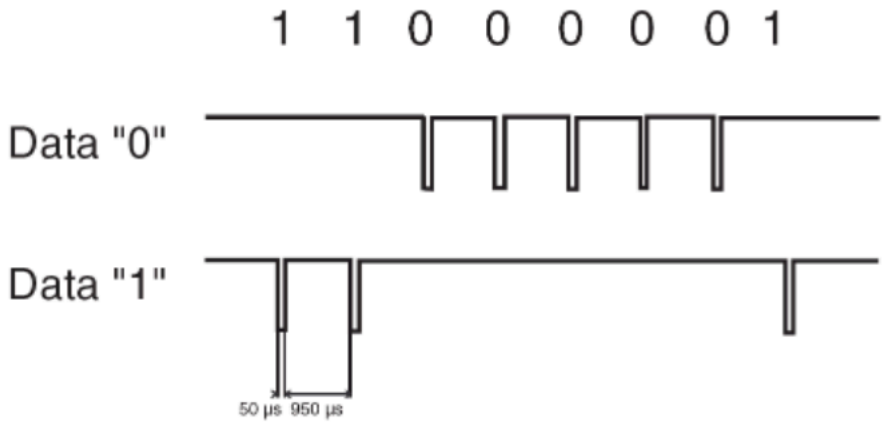
The 16 other bits are data bits.

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



APPENDIX 2: RS485 PROTOCOL

Definition

Data Packet Structure

The packet format is:

STX	ID	TID	DATA	CRC	DLE	ETX
Start Of Packet					End Of Packet	

Abbreviation

Fields name	Definition	Size (Bytes)	Value
<STX>	Start Text	1	**0x02**
<ID>	Packet Identifier	1	**0xE1**
<TID>	Terminal Identifier	1	--
<DATA>	Data value	Up to 1024	--
<CRC>	Transmission error control	2	--
<DLE>	Data Link Escape	1	**0x1B**
<ETX>	End Text	1	**0x03**

The maximum size allowed for a packet is 2 058 bytes:

(STX+ID+DLE+ETX+(TID+DATA+CRC)*2 [if stuffed])

Byte Order

The packet byte order is Little Endian: multi bytes data are sent with Least Significant Byte (LSB) first.

To prevent confusion with the frames sequences <STX><ID> and <DLE><ETX>, every <DLE> byte in the <TID+ Data + CRC> is preceded by an extra <DLE> byte ('stuffing').

Stuffing must be processed before sending a packet and removed ('unstuffed') after receiving the packet.

NOTE: A simple <DLE> <ETX> sequence does not necessarily signify the end of the packet, as these can be bytes in the middle of a data string.

The end of a packet is <ETX> preceded by an odd number of <DLE> bytes.

CRC Calculation

The type of the CRC is CRC16 V41.

The CRC is computed as a function of the Data part before Stuffing.

The initial value is 0x0000.

Packet Identifier

The packet identifier byte is 0x61.

Terminal Identifier

The terminal identifier byte defines the MorphoAccess® address on the RS485 network.

Frames sequence


replacement

APPENDIX 3: RS422 PROTOCOL (MORPHOACCESS® 500 SERIES ONLY)

Definition

Data Packet Structure

The packet format is:

STX	ID	RC	DATA	CRC	DLE	ETX
Start Of Packet					End Of Packet	

Abbreviation

Fields name	Definition	Size (Bytes)	Value
<STX>	Start Text	1	**0x02**
<ID>	Packet Identifier	1	--
<RC>	Request Counter	1	--
<DATA>	Data value	Up to 1024	--
<CRC>	Transmission error control	2	--
<DLE>	Data Link Escape	1	**0x1B**
<ETX>	End Text	1	**0x03**

The maximum size allowed for a packet is 2058 bytes:

(STX+ID+DLE+ETX+(RC+DATA+CRC)*2 [if stuffed])

Byte Order

The packet byte order is Little Endian: multi bytes data with Least

Significant Byte (LSB) first.

Data

Data are formatted as ILV packets.

Stuffing

Software handshake capabilities (XON-XOFF) are preserved by replacing, in the <RC + Data + CRC>, all XON (0x11) / XOFF (0x13) characters by the couple <DLE> <XON+1> (0x12) or <DLE> <XOFF+1> (0x14).

To prevent confusion with the frames sequences <STX><ID> and <DLE><ETX>, every <DLE> byte in the <RC+ Data + CRC> is preceded by an extra <DLE> byte ('stuffing').

Stuffing must be processed before sending a packet and removed ('unstuffed') after receiving the packet.

Notice that a simple <DLE> <ETX> sequence does not necessarily signify the end of the packet, as these can be bytes in the middle of a data string.

The end of a packet is <ETX> preceded by an odd number of <DLE> bytes.

CRC Calculation

The type of the CRC is CRC16 V41.

The CRC is computed as a function of the Data part before Stuffing.

The initial value is 0x0000.

Packet Identifier

The identifier is formatted as follows:

Bit 7 (MSB)	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0 (LSB)
IN/OUT	First	Last	Reserved 0	Packet Type			

The MSB (Bit 7) is reserved for packet direction. Setting this bit set the direction to IN. Clear this bit to set the direction to OUT.

An OUT packet is a packet sent **by the Host system to the MorphoAccess®** terminal**.**

An IN packet is a packet sent **by the MorphoAccess®** terminal **to the Host system.**

Bit 6 is reserved for Packet Order information. Set this bit when it is the first packet while transmitting a set of packets.

Bit 5 is reserved for Packet Order information. Set this bit when it is the last packet while transmitting a set of packets.

Bit 4 is a reserved bit and must be cleared.

0x4	NACK Packet

Retransmission

In case of NACK reception or Timeout, the transmitter tries to send the same packet again.

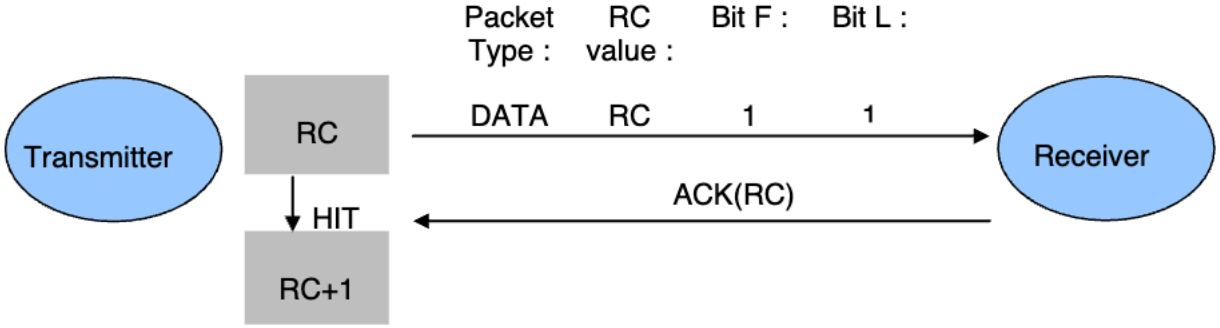
A packet can be retransmitted 3 times. After, another NACK reception or Timeout event leads to ERROR of the transmission.

Error cases

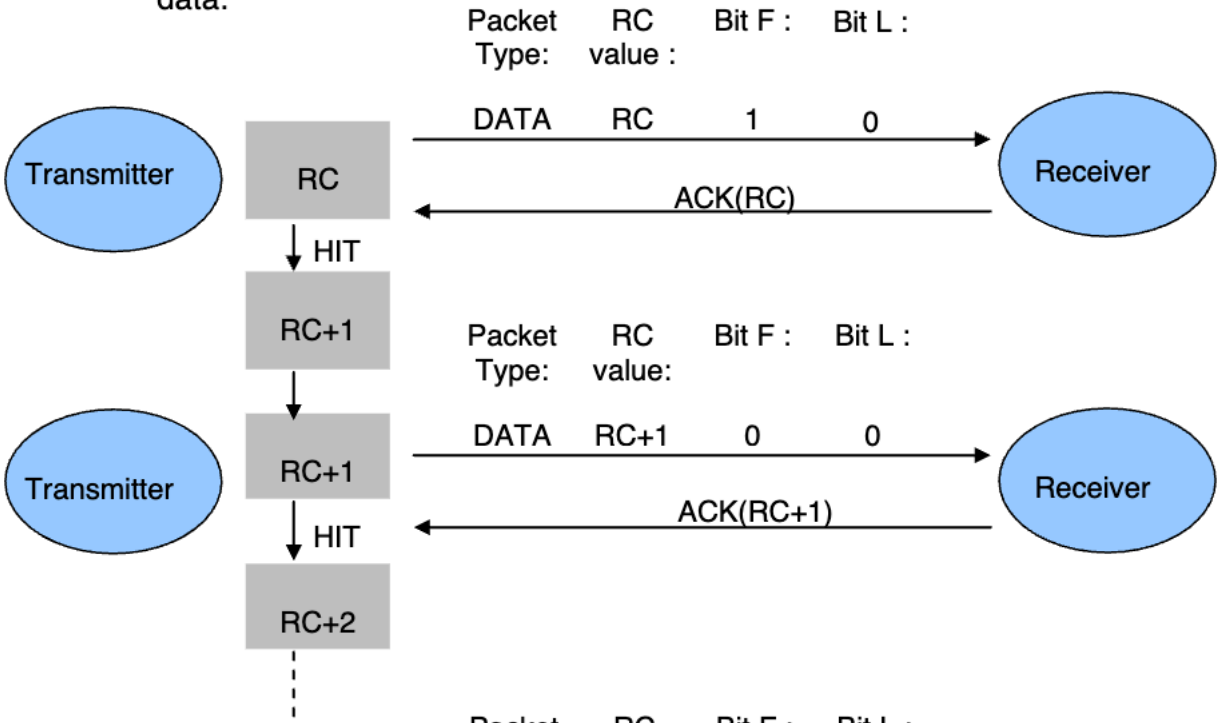
- When a frame is not valid (Bad CRC, Unstuffing error, Rx timeout), the receiver must send a NACK packet.
- When the transmitter is waiting an ACK/NACK packet, all other received packet must be ignored.

Typical Transactions workflow

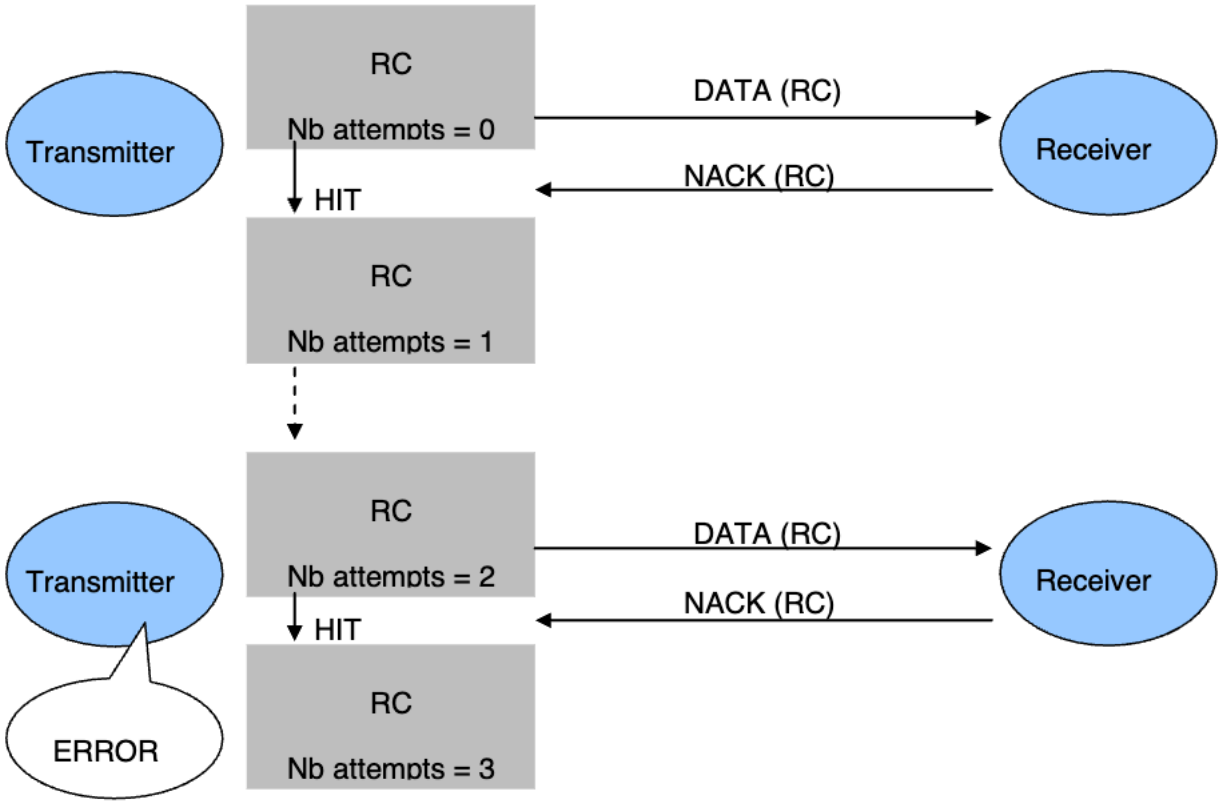
Emission of a data packet that contains less than 1 024 bytes of effective data:



Emission of a data packet that contains more than 1 024 bytes of effective data:



An Error occurred while transmitting the data packet:



Examples

User “094066” has been recognized by a MorphoAccess® terminal.

STX	ID	RC	Data: ILV									CRC	CRC	DLE	ETX
02	61	XX	00	06	00	*30*	*39*	*34*	*30*	*36*	*36*	CE	D1	1B	03

User “62487” has been recognized by a MorphoAccess® terminal.

STX	ID	RC	Data: ILV								CRC	CRC	DLE	ETX
02	61	XX	00	05	00	*36*	*32*	*34*	*38*	*37*	A0	AA	1B	03

Identification failed on MorphoAccess® terminal.

STX	ID	RC	Data: ILV				CRC	CRC	DLE	ETX
02	61	XX	10	01	00	01	B6	3C	1B	03

APPENDIX 4 - ISO 7811/2 - 1995 - TRACK 2 DATACLOCK FORMAT

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	"7"
8	0 0 0 1-0	"8"
9	1 0 0 1-1	"9"
10 (Ahex)	0 1 0 1-1	Unused character
11 (Bhex)	1 1 0 1-0	Start sentinel (start character)
12 (Chex)	0 0 1 1-1	Unused character
13 (Dhex)	1 0 1 1-0	Field separator
14 (Ehex)	0 1 1 1-0	Unused character
15 (Fhex)	1 1 1 1-1	End sentinel (stop character)

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).

SUPPORT

Customer service

Sagem Sécurité
SAV Terminaux Biométriques
Boulevard Lénine - BP428
76805 Saint Etienne du Rouvray
FRANCE
Phone: +33 2 35 64 53 52

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

Sagem Sécurité

SAFRAN Group

Head office: Le Ponant de Paris

27, rue Leblanc - 75512 PARIS CEDEX 15 - FRANCE