Sagem Défense Sécurité
SAFRAN Group

MorphoAccess™ 100 Series

Contactless Card Specification

Produced by Sagem Défense Sécurité

www.sagem.com

Table of content

INTRODUCTION

MorphoAccess™ 110 or 120 terminals allow reading reference templates on a contactless card.

The captured fingerprint can be matched against reference templates contained on a contactless card or extracted from the local database: this mode is called *contactless authentication*.

- On MorphoAccess™ 120, reference templates are stored on a Mifare™ contactless card.
- On MorphoAccess™ 110, reference templates are stored on a *iCLASS*™ contactless card.

Contactless card containing:

- ID
- Templates

In *contactless authentication* the led flashes “blue” to indicate that the terminal is waiting for a card.

Data localization on the card may be specified. Data are stored on the card according to the format detailed in this guide.

CHECK YOUR TERMINAL TYPE: MA120 OR MA110

MorphoAccess™ 120 terminal

Terminal type (read only)	
app/info/type	120

Mifare™ contactless card are supported on MorphoAccess™ **120** terminal.

MorphoAccess™ 110 terminal

Terminal type (read only)	
app/info/type	110

iCLASS™ contactless card are supported on MorphoAccess™ **110** terminal.

Retrieving the “terminal type”

The *GetVersion* ILV command returns the terminal type. Terminal type is also available in the *app.cfg* configuration file in the following entry: *app/info/type.*

You can use the *GetRegistryFile* ILV command to retrieve the *app.cfg* configuration.

You can use the *GetRegistryKey* ILV command to retrieve the *app/info/type* value.

ILV commands are described in *MorphoAccess100 Series Host System Interface.*

CONTACTLESS AUTHENTICATION STRATEGIES

Various recognition modes can be applied depending on the templates localization, the required security level.

These modes can be combined with a local identification (fusion mode).

These modes are :

- Contactless authentication with templates on a contactless card.
- Contactless authentication with templates on local database.
- Contactless authentication based on card mode.

They are descirbed in the *MorphoAccess100 Series User Guide*.

MIFARE™ CARD STRUCTURE [MA120]

A Mifare™ card is defined by a unique serial number.

Mifare™ 1K card

- The 1K card is divided in 16 sectors.
- Each sector is divided in 4 blocks.
- Each block contains 16 bytes of data.
- Data are encoded with two sets of key.
- Key are stored in the last block of each sector.

Mifare™ 4K card

- The 4K card is divided in 40 sectors.
- Sectors 0 to 31 are divided in 4 blocks.
- Sectors 32 to 39 are divided in 16 blocks.
- Each block contains 16 bytes of data.
- Data are encoded with two sets of key.
- Key are stored in the last block of each sector.

Overview

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

Data can be accessed by blocks as follows:

	Block 0	**Block 1**	**Block 2**	**Block 3**
Sector 0	Block 1	Block 2	Block 3	
Sector 1	Block 4	Block 5	Block 6	
...				
Sector 15	Block 46	Block 47	Bloc 48	

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

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

- <B> is the first block number to read,
- <N> is the number of blocks to read (allways 31 in fact),
- <C> selects a security key.

The complete 1K-4K card mapping is described in section Mifare™ Contactless Card Mapping.

iCLASS™ CARD STRUCTURE [MA110]

A *iCLASS*™ card is defined by a unique serial number.

MorphoAccess™110 terminal manage only *iCLASS*™ 16K/2 and 16K/16 HID badges.

iCLASS™ 16K/2 card

This card contains 2 applications. The limit between Application 1 and Application 2 can be defined on the card.

Biometric data require 78 contiguous blocks (624 bytes).

By default, the first block to read is the 19th block, but this value can be modified in the MorphoAccess™110 terminal.

Every block must be protected with the same key.

If a previous application is available in this area, SAGEM application and previous ones must share the same customer key and have to pay attention with different memory location.

iCLASS™ 16K/16 card

This card contains 16 applications.

Biometric data require 78 contiguous blocks (624 bytes).

For 16K/16 the terminal starts the reading process at a given a page. By default the reading begins at page 1.

Every block must be protected with the same key.

Pre personalized 16K16 card often contain “HID Reserved Area” storing a Wiegand identifier: it is possible to copy this identifier in the biometric data structure and to send it on the Wiegand layer. Section iCLASSTM “HID Reserved Area”, describes how to store this identifier in biometric data structure.

DATA ACCESS: MIFARE™ CARD [MA120]

Data localization on the card: first block read

Data read offset on the card	
app/contactless/B	4 – 185 (depending on card size)

By default, contactless read starts at block 4. 31 consecutive blocks are read.

This value can be modified. Setting this value to 9 means that data will be read from block 9 to 38.

This parameter is applied for biometric contactless card and admin contactless card.

31 block are allways read. If authentication fails at a given block the reading is stopped and valid data are extracted.

Authentication strategy

Authentication strategy	
app/contactless/C	1 *key A then B* 2 *key A only* 3 *key B only*

For each sector the terminal stores 2 keys (A and B).

This parameter allows defining the authentication strategy:

- If *app/contactless/C* is set to 1, Mifare™ security key A then B is selected (default)
- If *app/contactless/C* is set to 2, Mifare™ security key A is selected.
- If *app/contactless/C* is set to 3, Mifare™ security key B is selected.

Depending on card type (16K2 or 16K16) read parameters are different. The MorphoAccess™ 110 automatically detects card type.

- On 16K2 cards, biometric data starts at a specific block.
- On 16K16 cards, biometric data starts at a specific page.

Data localization on 16K2 card: first block read

On 16K2 cards the terminal start the reading process at a defined block.

By default, read starts at the 19th block, but this value can be modified in the MorphoAccess™110 terminal.

Data read offset on a 16K2 card	
app/contactless/HID start block	19 - 177

Biometric data require 78 contiguous blocks (624 bytes). Even if data are smaller these blocks will be read: it is highly advised to pad resting blocks to “0x00”.

This parameter is applied for biometric contactless card and admin contactless card.

Data localization on 16K16 card: first page read

On 16K16 cards the terminal start the reading process at a defined page.

By default, read starts at page 1. This value can be modified in the MorphoAccess™110 terminal.

Data read offset on a 16K16 card	
app/contactless/HID start page	1 - 5

Biometric data require 78 contiguous blocks (624 bytes). Even if data are smaller these blocks will be read: it is highly advised to pad resting blocks to “0x00”.

This parameter is applied for biometric contactless card and admin contactless card.

Authentication strategy

Only one key is employed during the read process. It means that the same key must be employed to protect every application aera containing the biometric data.

This key can be changed through Ethernet or using an “Admin card”.

Default factory key value is [01 23 45 67 89 AB CD EF].

It is possible to restore the factory key by setting a congfiguration key to “0”.

HID key status	
app/contactless/HID key valid	1: the key is valid 0: the key is invalid: the key will be reset to its default value.

DATA FILE STRUCTURE

Data storage format

Data are stored in tagged structures (TLV).

Tag	Length	Value
1 byte	2 bytes	L bytes
Data identifier	Value length (Little Endian)	Data

File format

The file will contain a succession of TLV.

TLV_0	TLV_1	TLV_2	…

BIOMETRIC CARD: DATA DEFINITION

Overview

The data card

Tag	Description
ID	*User ID in ASCII*
NAME	*User name in ASCII*
PIN	*User PIN code in ASCII*
PK1	*First compressed minutiae*
PK2	*Second compressed minutiae*
BIOPIN	*This PIN code will replace minutiae.*

ID tag

Value	TAG_ID 0x32
Presence	Mandatory.
Description	This tag contains a unique card identifier. This ID can be used as an index in the local database of the MorphoAccess™. It is sent to the access control system on a positive authentication. This tag holds a length fixed string. Data are then padded with null characters.
Format	ASCII
Length	25 bytes

iCLASS™ cards "HID Reserved Area"

To enhance the MorphoAccess™ 110 integration, it is possible to store Wiegand data in this tag.

NAME tag (ignored on MA110 / MA120)

Value	TAG_NAME 0x20
Presence	Ignored on MA110 / MA120.
Description	This tag contains the name of the cardholder. This tag holds a length fixed string. Data are then padded with null characters.
Format	ASCII
Length	20 bytes

PIN tag (ignored on MA110 / MA120)

Value	TAG_PIN 0x33
Presence	Ignored on MA110 / MA120.
Description	User PIN in ASCII. “1234” for example.
Format	ASCII
Length	15 bytes

PK1 tag

Value	TAG_PK_1 0x30
Presence	Mandatory if the control requires a biometric verification.
Description	This tag contains the minutiae of the first enrolled finger according to the PKCOMP170 format.
Format	PKCOMP170, binary.
Length	170 bytes

PK2 tag

Value	TAG_PK_2 0x31
Presence	Mandatory if the control requires a biometric verification.
Description	This tag contains the minutiae of the second enrolled finger according to the PKCOMP170 format.
Format	PKCOMP170, binary.
Length	170 bytes

BIOPIN tag (ignored on MA110 / MA120)

Value	TAG_BIOPIN 0x34
Presence	Ignored on MA110 / MA120.
Description	This tag contains the user BIOPIN code. “4321” for example.
Format	ASCII
Length	15 bytes

CARD MODE tag

Value	TAG_CARD_MODE 0x35
Presence	Mandatory if the control “authent card mode” is enabled.
Description	This tag contains the authentication method to use.
Format	Binary
Length	1 byte
Available values	ID_ONLY 0x01 PKS 0x02

Required tags

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent ID contactless	Yes	No	No	No	No	No
authent PK contactless	Yes	No	Yes	Yes	No	No
authent card mode (ID_ONLY)	Yes	Yes	No	No	No	No
authent card mode (PKS)	Yes	Yes	Yes	Yes	No	No
bypass authentication	Yes	No	No	No	No	No

CHANGING CONTACTLESS KEYS WITH AN ADMIN CARD

Admin Card

An *Admin Card* allows changing contacless keys in the terminal. If current keys in the terminal are K_n, the *Admin Card* allows changing these keys by K_{n+1}.

An *Admin Card* is encoded with K_n (current keys) and contains K_{n+1} (new keys).

The administrator has just to present the *Admin Card* to the terminal: the led flashes green, indicating that the key rotation is successful.

There is no biometric data on the card.

Mifare™ Admin Card [MA120]

Data localization on the card: first block read

Data read offset on the card (first block read)	
app/contactless/B	4 – 185 (depending on card size)

The first block read by MA1XX terminal is the block specified by the *app/contactless/B* key. This setting must be coherent with card size.

MorphoAccess 220, 320 compatibility note !

MA 220/320 terminals allways start reading *admin card* at block 4. MA 120 terminal start reading admin card at a block defined by the *app/contactless/B* key. If this value changes, MA 220/320 admin cards are no more compatible with MA120 terminals.

ADMIN tag

Value	TAG_ADMIN 0x03
Description	This is the unique TLV on the card. The value field contains the new keys for each sector.
Length	480 bytes to change Mifare™ 4K card keys. 192 bytes to change Mifare™ 1K card keys.

Data format: Mifare™ 1K card

New keys are stored in a TLV data structure (see section Data access: MifareTM Card [MA120]).

The value field contains the new key “one after the other”.

For a 1K card we have 16 keys set (A and B): 6bytes x 2 x 16 = 192 bytes.

TLV is stored on 13 consecutive blocks.

6 bytes	6 bytes	6 bytes	6 bytes	…	6 bytes	6 bytes
New KA sector 0	New KB sector 0	New KA sector 1	New KB sector 1		New KA sector 15	New KB sector 15

Data format: Mifare™ 4K card

New keys are stored in a TLV data structure (see section Data access: MifareTM Card [MA120]).

The value field contains the new key “one after the other”.

For a 4K card we have 40 keys set (A and B): 6bytes x 2 x 40 = 480 bytes.

TLV is stored on 31 consecutive blocks.

6 bytes	6 bytes	6 bytes	6 bytes	…	6 bytes	6 bytes
New KA sector 0	New KB sector 0	New KA sector 1	New KB sector 1		New KA sector 39	New KB sector 39

iCLASS™ Admin Card [MA110]

Data localization on a card: first block read

Admin Data are stored at the same place than biometric data (defined by a block on 16K2 card, defined by a page on 16K16 card.) Because the MorphoAccess™ 110 always read 78 contiguous blocks, *Admin Data* must be padded.

ADMIN tag

Value	TAG_ADMIN 0x03
Description	This is the unique TLV on the card. The value field contains the new keys for each sector.
Format	Binary
Length	9 bytes

Data format

The first byte contains the key number: it must be 6.

The 8 following bytes contain the key binary data.

Data	Byte 0	Key number. Must be 0x06
	Byte 1	New Key[Byte 0]
	Byte 2	New Key[Byte 1]
	…	
	Byte 8	New Key[Byte 7]

CHANGING CONTACTLESS KEYS THROUGH ETHERNET

It is also possible to update contactless keys through the MorphoAccess™ TCP interface.

The *Set Contactless Keys* ILV command allows changing contactless keys from a distant client. Please refer to the *MorphoAccess100 Series Host System Interface* for more information about this feature.

MIFARE™ CONTACTLESS CARD MAPPING

Sector	Block	Block	Block	Block	Block		Block	Block	Size	Real size
0	*1*	*2*	*3*	***Key***					64	48
1	4	5	6	***Key***					128	96
2	7	8	9	***Key***					192	144
…										
14	43	44	45	***Key***					960	720
15	46	47	48	***Key***					**1024**	768
16	49	50	51	***Key***					1088	816
17	52	53	54	***Key***					1152	864
…										
30	91	92	93	***Key***					1984	1488
31	94	95	96	***Key***					2048	1536
32	97	98	99	100	101		111	***Key***	2304	1776
33	112	113	114	115	116		126	***Key***	2560	2016
…										
39	202	203	204	205	206		216	***Key***	**4096**	3456

In green: 1 K card.

Only “data block” are counted. Block 1,2,3 contain card serial number.

iCLASS™ CARD MAPPING

iCLASS™ 16K/2 card

This card contains 2 applications. The limit between Application 1 and Application 2 can be defined on the card.

Biometric data require 78 contiguous blocks (624 bytes).

By default, the first block to read is the 19th block, but this value can be modified in the MorphoAccess™ 110 terminal.

Every block must be protected with the same key.

	Byte number within a block							
Block	0	1	2	3	4	5	6	7
0	Serial Number (64 bits)							
1	Application Limit **XX**	Application 16 bit OTP Area	Block Write Lock	Chip Config	Memory Config		E.A.S	Fuses
2	Secured Stored Value Area							
3	Key 1							
4	Key 2							
5	Application Issuer Area							
6	Application Area 1 (secured by Key 1)							
7								
-								
XX								
XX+1	Application Area 2 (secured by Key 2)							
XX+2								
-								
255								

iCLASS™ 16K/16 card

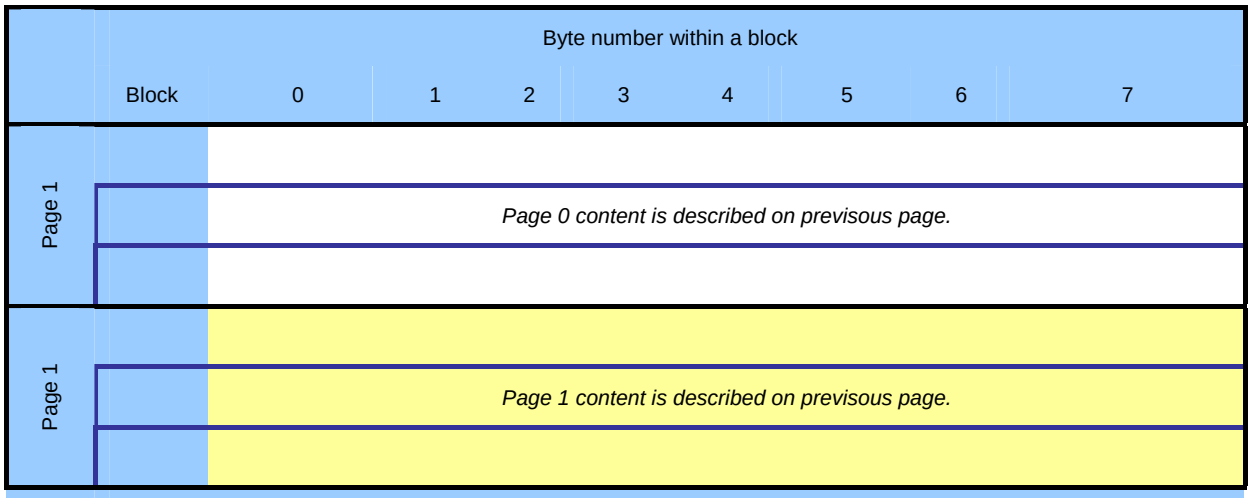
This card contains 16 applications.

Biometric data require 78 contiguous blocks (624 bytes).

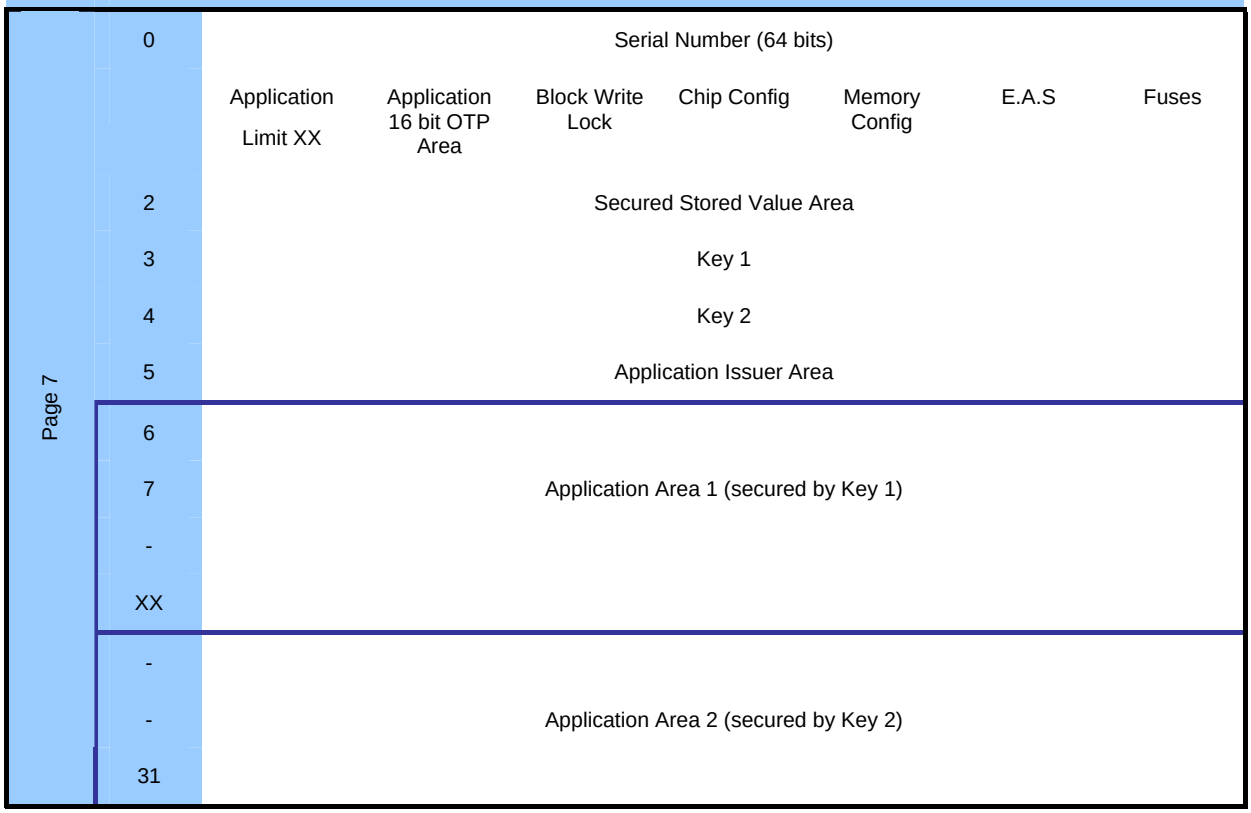
For 16K/16 the terminal starts the reading process at a given a page. By default the reading begins at page 1. This value can be modified in the MA110 terminal.

Every block must be protected with the same key.

	Block	Byte number within a block 0	1	2	3	4	5	6	7
Page 0	0	Serial Number (64 bits)							
	1	Application Limit XX	Application 16 bit OTP Area		Block Write Lock	Chip Config	Memory Config	E.A.S	Fuses
	2	Secured Stored Value Area							
	3	Key 1							
	4	Key 2							
	5	Application Issuer Area							
	6	Application Area 1 (secured by Key 1)							
	7								
	-								
	XX								
	-	Application Area 2 (secured by Key 2)							
	-								
	31								
Page 1									
		Page 1 content is described on next page.							
Page 2 to 6									
Page 7									
		Page 7 content is described on next page.							


Byte number within a block
Block
0
1
2
3
4
5
6
7
Page 1
Page 0 content is described on previsous page.
Page 1
Page 1 content is described on previsous page.

Page 2 to 6


Page 7
0
Serial Number (64 bits)
Application Limit XX
Application 16 bit OTP Area
Block Write Lock
Chip Config
Memory Config
E.A.S
Fuses
2
Secured Stored Value Area
3
Key 1
4
Key 2
5
Application Issuer Area
6
7
Application Area 1 (secured by Key 1)
-
XX
-
-
Application Area 2 (secured by Key 2)
31

ICLASS™ "HID RESERVED AREA"

Reserved area

ICLASS™ 16K16 *Pre Personalized* cards can contain a "reserved area" stored in Application 1 (blocks 6 to 18).

In this area, 18 bytes are reserved to store a *Wiegand Identifier* (26 bits, 32 bits, custom format etc.)

This Identifier can be sent "as is " by the MorphoAccess™.

Activating ID conversion

As the TAG reserved to store the identifier (TAG_ID) on the card can contain only ASCII data, SAGEM DS converts these 18 bytes in 24 characters.

These 24 characters can be sent in the original format through the Wiegand output.

This feature is useful to integrate a MorphoAccess™ 110 in an existing access control system.

First the Wiegand output must be enabled:

Activating the Wiegand output	
app/send ID wiegand/enabled	1

Please refer to *MA100 Series Remote Messages Specification* for more information about the Wiegand output.

In the second place, the "identifier conversion" must be activated:

Activating the "identifier conversion"	
app/ send ID wiegand/HID conversion	1

Once the "HID Conversion" activated other Wiegand format parameters are ignored.

Example

The “HID Reserved Area” contains the following 18 bytes of data:

00 00 00 00 00 00 00 00 00 00 00 00 00 00 **06 02 03 04**

where:

06 02 03 04 = 000001**1**00000001000000011000000100

The first bit set to 1 is a start sentinel. It means that the following frame will be sent through the Wiegand output (26-bits):

1 00000001 0000000110000010 0 (site code 1, identifer 0d386).

To store the “HID Reserved Area” these 18 bytes must be stored on the card using an ASCII 64 characters set.

00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 02 03 04

becomes:

“AAAAAAAAAAAAAAAAAAGAgME”.

This value is stored on the card in the TLV containing the identifer.

If “*HID conversion*” is activated the MorphoAccess™ will send the right identfier (26 bits, site code 1, identifer 0d386).through the Wiegand output.

Charcater table

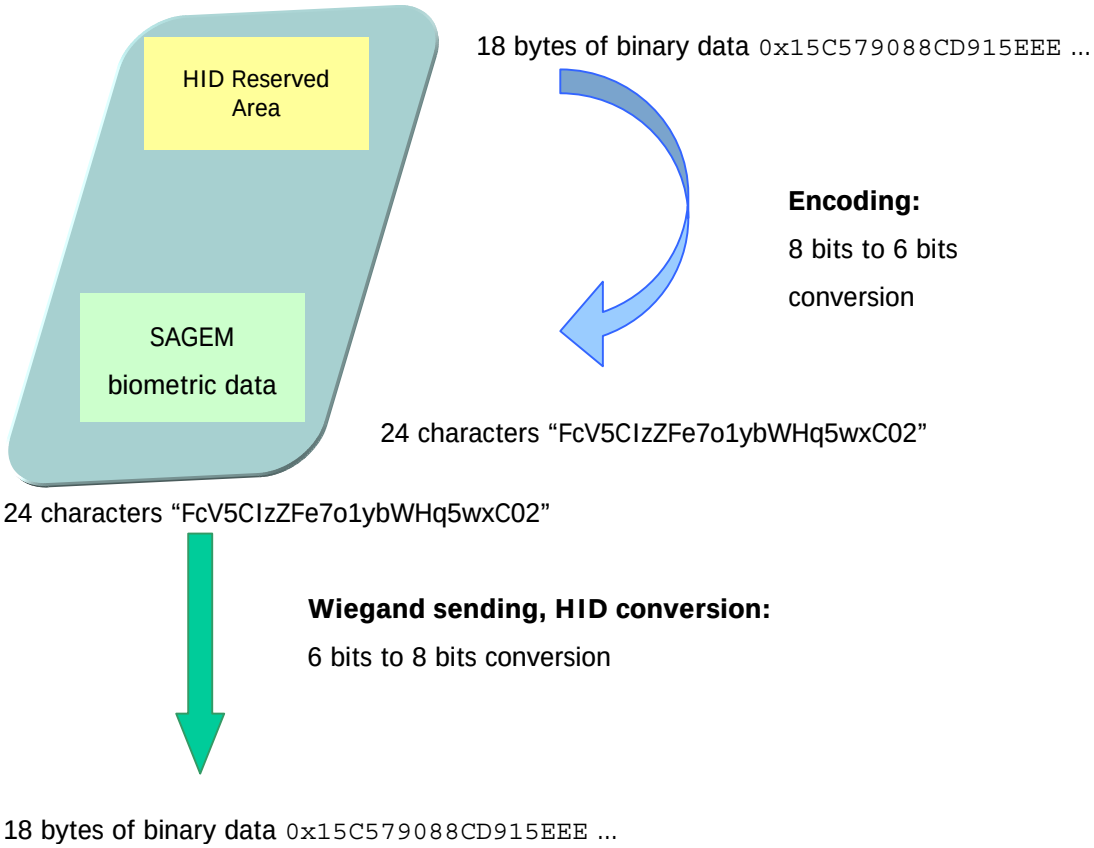
The charcater table is :

"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789 _"

The conversion table (8 bits to 6 bits conversion) is the following:

0	1	2	3	4	…	25	26	27
‘A’	‘B’	‘C’	‘D’	‘E’		‘Z”	‘a”	‘b’
28	…	51	52	53	…	61	62	63
‘c’		‘z’	‘0’	‘1’		‘9’	‘\20‘	‘_’

Synthesis



CONTACTLESS PARAMETERS: SYNTHESIS

Terminal type

Terminal type (read only)	
app/info/type	120 or 110

Card access [MA120]

Data read offset on the card (first block read)	
app/contactless/B	4 – 185 (depending on card size)
Authentication strategy	
app/contactless/C	1 *key A then B* - 2 *key A only* - 3 *key B only*

Card access [MA110]

Data read offset on the card (first block or first page read)	
app/contactless/HID start block	19 - 177
app/contactless/HID start page	1 - 5

Contactless mode

Contactless authentication with templates on card	
app/bio ctrl/authent PK contactless	0-1
Contactless authentication with templates on local database	
app/bio ctrl/authent ID contactless	0-1
Contactless authentication with card mode	
app/bio ctrl/authent card mode	0-1
Disabling biometric control	
app/bio ctrl/bypass authentication	0-1

MORPOACCESS 220 320 COMPATIBILITY [MA120]

Contactless authentication with ID on card, template in local database	
MorphoAccess 320 220 parameter	MorphoAccess™ 120 parameter
/cfg/Maccess/Admin/mode 4	*app/bio ctrl/authent ID contactless 1*

Contactless authentication: Card mode	
MorphoAccess 320 220 parameter	MorphoAccess™ 120 parameter
/cfg/Maccess/Admin/mode 3 */cfg/Maccess/Contactless/without DB mode 0*	*app/bio ctrl/authent card mode 1*

Contactless authentication: Biometric verification	
MorphoAccess 320 220 parameter	MorphoAccess™ 120 parameter
/cfg/Maccess/Admin/mode 3 */cfg/Maccess/Contactless/without DB mode 2*	*app/bio ctrl/authent PK contactless 1*

Contactless authentication: ID “only”, no biometric verification	
MorphoAccess 320 220 parameter	MorphoAccess™ 120 parameter
/cfg/Maccess/Admin/mode 3 */cfg/Maccess/Contactless/without DB mode 1*	*app/bio ctrl/bypass authentication 1*

SAGEM Défense Sécurité

Siège social : Le Ponant de Paris

27, rue Leblanc - 75512 PARIS CEDEX 15 - FRANCE

Société anonyme à directoire et conseil de surveillance

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