MorphoAccess® SIGMA Family and MorphoWave Compact

Contactless cards Specification

Warning

This manual makes reference to names and products that are trademarks of their respective owners.

Revision History

The table below contains the history of changes made to the present document.

Version	Date	Description
1	November 2016	New documents' refence based on the 2014_0000001408-v6. Remove Mifare® Plus card support
2	March 2017	Replace 5G Series with SIGMA Family Add the MorphoAccess® SIGMA Extreme Series product
3	June 2017	Add template formats ISO19794-2 Finger Minutiae Card Record, Compact Size(AA), DIN_V66400_CS, DIN_V66400_CS_AA and Multimodal (FVP) Add HID Seos® support
4	December 2017	Update company name (IDEMIA)
5	July 2018	Add Mifare® Plus card support Add SmartMX card support (as a DESFire® card) Add HID® DESFire® SE card support Add Morpho*Wave* Compact
6	July 2018	Add DESFire® EV2 card support
7	August 2018	Add iClass Legacy Add limitation, SEOS 16K is not supporting Complete warning about 8 fingers storage
8	November 2018	Limitation about physical type of supported card (added in Introduction chapter) Add SmartMX card full support (Mifare® and DESFire® card) HID PACS Data section creation (added in card structure chapter) Morpho*Wave* Compact, add HID® Card number support for HID Seos® Morpho*Wave* Compact, add HID® Card number support for HID® Mifare® SE and HID® DESFire® SE Morpho*Wave* Compact, add HID® Elite customization support

		Add 0x39 Tag
9	January 2019	Warning in data section
10	April 2019	Firmware MorphoAccess® SIGMA 4.6 evolutions
		Add warning Morpho*Wave* Compact is not supporting data read from HID Seos®
		Add warning in data section about TLV parsing
		Add TLV SECURE_DATA
		Completed supported cards

Table of Content

Table of Figures

Section 1 : Introduction

MorphoAccess® SIGMA Family and Morpho*Wave* Compact, when equipped with a contactless smartcard reader, allow reading reference templates on a contactless card.

Reference templates can be stored on an iClass® contactless card (iClass legacy or iClass SE), a MIFARE® contactless card or a DESFire® contactless card depending on the kind of contactless smartcard reader which equips the terminal.

Please refer to Administration guide to have complete list of contactless validated cards.

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.

Various authentication recognition modes can be applied depending on:

- user's fingerprint templates localization (either local database or user's card)
- touchscreen/keyboard presence on the terminal, for PIN code check
- required security level (biometric check and/or PIN check)
- which entity defined the authentication process (the terminal or the user's card)

MorphoAccess® SIGMA Family and MorphoWave Compact support contactless cards with ID-1 type format (as per ISO/CEI 7810 standard). Other contactless devices like smart keys or tags are not supported.

Section 2 : Card structure

DESFire® card structure

This section concerns only MorphoAccess® equipped with a DESFire® contactless smartcard reader.

A DESFire® card has a unique serial number (the random serial number of DESFire® EV1 cards is not supported).

A DESFire® card (DESFire® EV1) exists in several sizes (2kB, 4kB, 8kB).

A DESFire® card contains "applications" (comparable to a directory). An application is represented by 3 bytes (AID, Application IDentifier).

An application may contain up to 16 files. A file is represented by a number.

A fundamental security key protects the card: PICC_MASTERKEY. This key allows creating / deleting applications on the card.

An application uses a particular key to create/delete files: APPLICATION_MASTERKEY.

Access rights for a file are the following:

- Read,
- Write,
- Read / Write,
- Change Access Rights.

Data access

By default, to read biometric data, the MorphoAccess® will look for the file 0 stored in the application named "BIO" (AID is 0x42 0x49 0x4F in ASCII).

By default, to read biometric data, the Morpho*Wave* Compact will look for the file 0 stored in the application named "WAV" (AID is 0x77 0x41 0x76 in ASCII).

File location

By default, the file 0x00 in dedicated application contains the relevant information. These values can be changed using parameters ***sc_tlv_desfire.aid*** and ***sc_tlv_desfire.fid***.

Features

The DESFire® card reading features can be customized by one configuration parameter (see features details in next sections):

sc.auto_key_update	
1 (Bit 0 - 0x01)	Do not format card before encoding
2 (Bit 1 - 0x02)	Disable keys rotation on the fly

16 (Bit 4 - 0x10)	Disable PICC Master key derivation
32 (Bit 5 - 0x20)	Disable Application keys derivation

NOTE: these values can be used together. For example use the value 17 (0x11) to activate multi-applicative mode.

Card formatting

By default, the DESFire® cards are formatted (completely erased) when they are encoded.

This feature can be disabled to keep another application that can be on the card.

Key rotation

In DESFire® system, the MorphoAccess® terminals are able to perform keys rotation on the fly: when a user presents a card that is encoded with obsolete OLD keys set, the reader will automatically change these keys to the NEW keys set.

This feature is disabled by default due to security and use reasons. Please do not activate this feature without a full understanding on the consequences for your system.
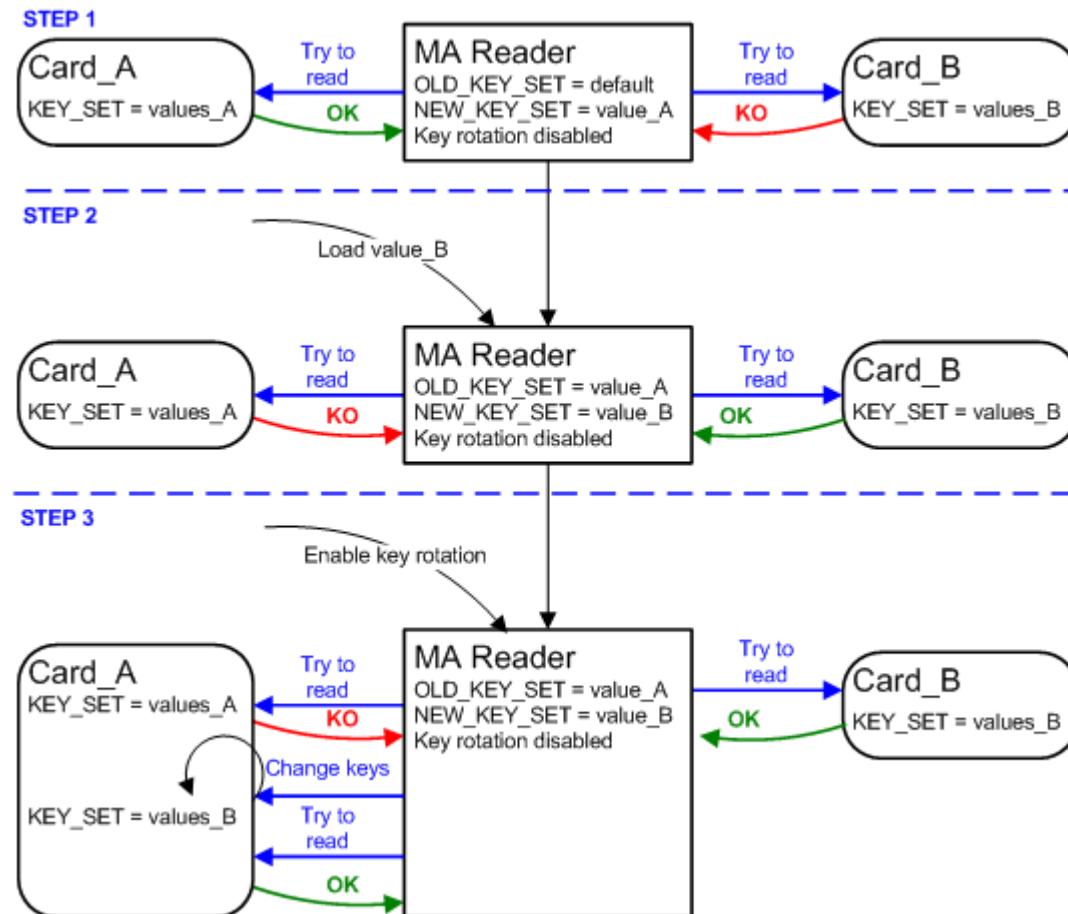
Figure 1 : Full example of key rotation

NOTE: If a card is not encoded with OLD keys of the MorphoAccess®, the terminal cannot do keys rotation.

NOTE: Do not activate this feature for the first key set. In fact, by default the old keys are set to default key value then any card that is encoded with default keys can get the new key set from your system.

Key derivation

By default, card encoding is made with key derivation. That means that the real used key is different for each card.

The keys set into the MorphoAccess® are used as base keys and are diversified by the card's unique identifier.

This is a method for security improvement: the security keys are known only by encoder and reader, and not stored "as is" in the card.

This feature is by default enabled for BIO_FILE_READ_KEY and APPLICATION_MASTER_KEY, and can be disabled for PICC_MASTER_KEY (bit 4 of sc.auto_key_update), BIO_FILE_READ_KEY and APPLICATION_MASTER_KEY (bit 5 of sc.auto_key_update).

PICC_MASTER_KEY derivation should be disabled only to let the card being encoded by another system for multi-applications cards.
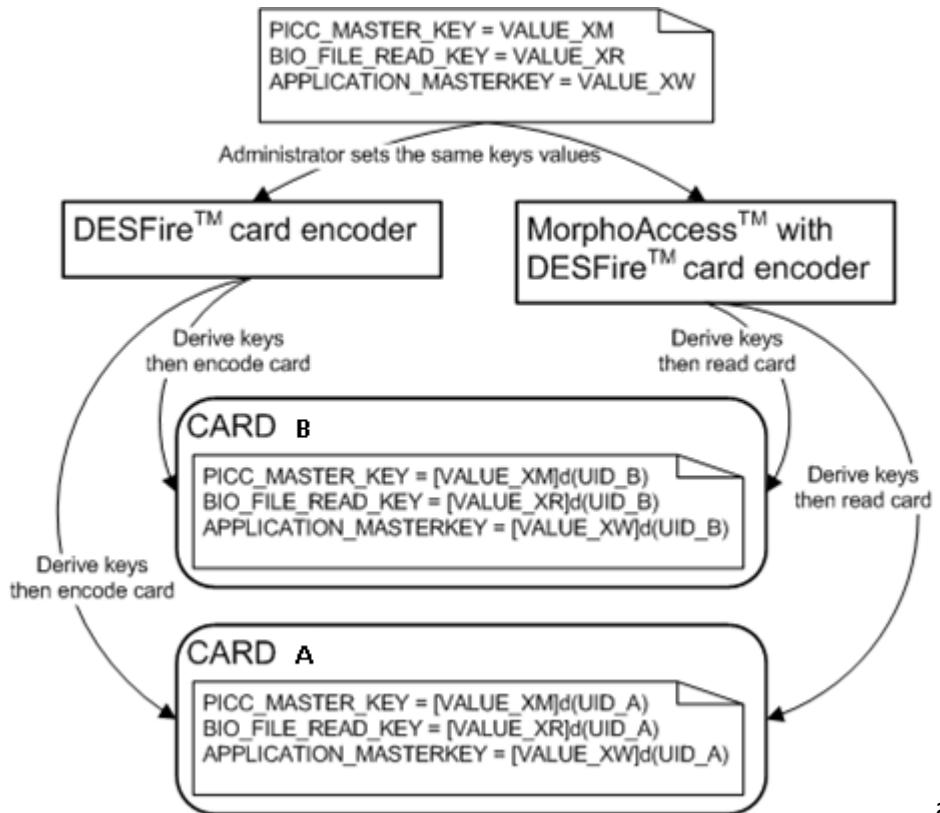
Figure 2 : Key derivation

NOTE: A card encoded in one way (for example: enabled derivation) cannot be re-encoded with the other way (without derivation).

Multi-application

By default, the MorphoAccess® will encode cards with derived keys (see section above) and firstly formats the card.

To use the card for different other applications (ex: coffee machines, parking…) from MorphoAccess® access control system, the MorphoAccess® configuration must be changed.

- In multi applicative use:
  o the card has not to be formatted at the beginning of the encoding,
  o and its PICC Master key must not be derived.
- The consequence of multi-application cards is:
  o the PICC_MASTER_KEY is shared between different applications,
  o PICC_MASTER_KEY used for each card is the same,
  o PICC_MASTER_KEY is stored "as is" in all the cards.

Some differences between the two modes are noticeable:

Multi-application mode	Single application mode
PICC_MASTER_KEY is not derived with card UID	PICC_MASTER_KEY is derived with card UID by the Morpho derivation algorithm
Another system can create and manage its own applications	Only the Morpho system can create and manage its own applications
PICC_MASTER_KEY is known by all the systems that manage applications on the card	PICC_MASTER_KEY can be known only by the Morpho system
Lower security level: all the systems know the shared PICC_MASTER_KEY all the cards have the same PICC_MASTER_KEY	Higher security level: only Morpho system knows the PICC_MASTER_KEY each card use a different PICC_MASTER_KEY

Access rights

Card

Key ID	Description
0	PICC_MASTER_KEY

In multi applicative use, if the card is previouly configured to authorize Application creation and deletion without the PICC_MASTER_KEY, it is possible to encode cards with the MorphoAccess® without loading this PICC_MASTER_KEY into the MorphoAccess®.

Application

The "BIO" application will contain two keys. Both could be derived with the card Serial Number (SN) from a master key stored in the MorphoAccess® terminal equipped with a DESFire® contactless smartcard reader. It means that every card has a unique set of keys.

Application master key setting is 0x0B.

ID	B7	B6	B5	B4	B3	B2	B1	B0
APPLICATION_MASTERKEY	0	0	0	0	1	0	1	1

File

Access rights for the biometric file (file 0) use only two keys: BIO_FILE_READ_KEY (1) for reading, and APPLICATION_MASTERKEY (2) for other access rights.

- Read: key BIO_FILE_READ_KEY,
- Write: key APPLICATION_MASTERKEY,
- Read / Write: key APPLICATION_MASTERKEY,
- Change Access Rights: key APPLICATION_MASTERKEY.

File "com mode" is 3 (*enciphered*).

Biometric file	
File ID	0
Com Mode	3
R key	BIO_FILE_READ_KEY (1)
W key	APPLICATION_MASTERKEY (2)
RW key	APPLICATION_MASTERKEY (2)
CAR key	APPLICATION_MASTERKEY (2)

Cards supported as DESFire® cards

MorphoAccess® SIGMA Multi, Morpho*Wave* Compact MD and Morpho*Wave* Compact MDPI are supporting as DESFire® cards:

- DESFire® EV0 (first generation of DESFire® cards, 3DES only)
- DESFIRE® EV1 (3DES and AES, random CSN not supported)
- DESFIRE® EV2 (3DES and AES, random CSN and Delegated Application Management not supported)
- HID® DESFire® SE (PICC_MASTER_KEY unknown, free to create application)

MorphoAccess® SIGMA Multi and Morpho*Wave* Compact MD are supporting as DESFire® cards:

- SmartMX® (dual technology Mifare® and DESFire®, as DESFire® when dedicated profiles are activated)

Mifare® card structure

This section concerns only MorphoAccess® equipped with a Mifare® contactless smartcard reader.

A Mifare® card is defined by a unique serial number of 4 or 7 bytes.

Mifare® 1K

- The 1K card is divided into 16 sectors,
- Each sector is divided into 4 blocks,
- Each block contains 16 bytes of data,
- Data are encoded with two sets of key,
- Keys are stored in the last block of each sector, this last block doesn't contain data.

Mifare® 4K

- The 4K card is divided into 40 sectors,
- Sectors 0 to 31 are divided into 4 blocks,
- Sectors 32 to 39 are divided into 16 blocks,
- Each block contains 16 bytes of data,
- Data are encoded with two sets of key,
- Keys are stored in the last block of each sector, this last block doesn't contain data.

Mifare® Plus card

Mifare® Plus card is a card that can work in different **S**ecurity **L**evels:

- **SL0** is a level used to change the keys in the card
- **SL1** is a level to use the card as a Mifare® Classic card (Mifare® Classic authentication)
- **SL2** is not compatible with MorphoAccess® terminals
- **SL3** is a level to use the card as a Mifare® Plus card (Mifare® Plus authentication)
- It is not possible to go back to a lower security level
- MorphoAccess® terminal will not change security level of a Mifare® Plus card

MorphoAccess® terminal uses 16 bytes 0xFF AES keys as default keys for Mifare® Plus SL3 card support.

Mifare 1K-4K mapping 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 N	Block 46/94	Block 47/95	Block 48/96	

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

IDEMIA 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 (fixed value),
- <C> selects a security key.

Last sector blocks are used for keys as below:

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

In green: 1K card. Only "data block" are count. Block 1, 2, 3 contain card serial number.

Data access

Data localization

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

These values can be modified using parameters ***sc_tlv_mifare.start_block*** and ***sc_tlv_mifare.num_block*** for Mifare® classic and ***sc_tlv_mifare_plus.start_block*** and ***sc_tlv_mifare_plus.num_block*** for Mifare® Plus SL3 card.

These parameters are applied for biometric contactless card and admin contactless card.

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

Authentication strategy

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

The parameters ***sc_tlv_mifare.key_policy*** for Mifare® classic and ***sc_tlv_mifare_plus.key_policy*** Mifare® Plus allow to define the authentication strategy:

Value	Description
1	Try to read card first with Key A then Key B
2	Try to read card with Key A
3	Try to read card with Key B

Mifare® Classic cards use 6 bytes length keys (CRYPTO1 algorithm)

Mifare® Plus cards use 16 bytes length keys (AES algorithm)

Cards supported as Mifare® cards

MorphoAccess® SIGMA Multi, Morpho*Wave* Compact MD and Morpho*Wave* Compact MDPI are supporting as Mifare® cards:

- Standard Mifare® cards, 1K and 4K, with 4 and 7 bytes serial number
- HID® Mifare® SE

MorphoAccess® SIGMA Multi and Morpho*Wave* Compact MD are supporting as Mifare® cards:

- Mifare® Plus card
- SmartMX® (dual technology Mifare® and DESFire®) as Mifare® when dedicated profile is activated. DESFire® detection is activated before Mifare®, by consequence if terminal have access to the 2 section, only data from DESFire® section will be evaluated.

HID PACS data

PACS data definition

Most of HID cards contain a unique ID stored in the HID application section (currently named PACS data): this is available for iClass® Legacy, iClass® SR, iClass® SE, Seos®, Mifare® SE and DESFire® SE. This ID is a Wiegand frame, refer to HID documentation for the Wiegand format.

HID application can be protected by a custom key named 'Elite'. Please refer to the Administration guide to apply the Elite keys to the terminal.

PACS data support

- MorphoAccess® SIGMA iClass is able to read PACS data from iClass® Legacy, iClass® SR, iClass® SE and Seos® cards.

- Morpho*Wave* Compact MDPI is able to read PACS data from iClass® Legacy, iClass® SR, iClass® SE, Seos®, Mifare® SE and DESFire® SE. When Morpho*Wave* Compact MDPI is configured to read PACS data from Mifare® SE or DESFire® SE, it cannot access the Mifare or DESFire section of the card.

- MorphoAccess® SIGMA iClass and Morpho*Wave* Compact MDPI are able to read contactless card with Elite keys, provided they are previously loaded in the terminal.

HID iClass® card structure

This section concerns only MorphoAccess® or Morpho*Wave* Compact equipped with an iClass® contactless smartcard reader. Terminals are supporting iClass® Legacy, iClass® SR and iClass® SE.

iClass® 2K2 card

This card is supported with limitation. Templates can't be stored because the card can't contain enough data.

iClass® 16K2 card

This card contains 2 applications on 16Kb / 2 KB. The limit between Application 1 and Application 2 can be defined on the card.

Each application can be protected with different keys.

Biometric data requires at least 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® terminal.

MorphoAccess® terminal uses the application 2 when encoding 16K2 cards.

iClass® 16K16 card

This card contains 16 applications in 8 pages, each page contains 2 applications.

Each application can be protected with different keys.

Biometric data requires at least 78 contiguous blocks (624 bytes).

For 16K16 cards, the terminal starts the reading process at a given page. By default, the reading begins at page 1.

MorphoAccess® terminal uses the application 2 of used pages when encoding 16K16 cards.

iClass® 32K16 (16K16/16K1) card

This card contains 2 books (book 0 and book 1). Book 0 is like a 16K16 card: it contains 16 applications in 8 pages with 2 applications by page. Book 1 contains only 1 page with 1 application, protected by 1 key.

If MorphoAccess® terminal is configured to use book 0, it encodes application 2 of used pages.

If MorphoAccess® terminal is configured to use book 1, it encodes application 1 of used pages.

iClass® 32K2 (16K2/16K1) card

This card contains 2 books (book 0 and book 1). Book 0 is like a 16K2 card: it contains 2 applications. Book 1 contains only 1 page with 1 application, protected by 1 key.

If MorphoAccess® terminal is configured to use book 0, it encodes application 2.

If MorphoAccess® terminal is configured to use book 1, it encodes application 1.

Memory layout

Block Number	Block Description (size = 8 bytes)
0x00	Card Serial Number
0x01	Configuration Block
0x02	e-pulse
0x03	"Debit" Key for Application 1 (Kd)
0x04	"Credit" Key for Application 2 (Kc)
0x05	Application Issuer Area
0x06	HID Application
…	
0x12	
0x13	Application 2 (User Memory)
…	
0x1F (16K16) 0xFF (16K2)	

Figure 3 : Memory layout of 16K2 card or page 0 of 16K16 card

Block Number	Block Description (size = 8 bytes)
0x00	Card Serial Number
0x01	Configuration Block
0x02	e-pulse
0x03	"Debit" Key for Application 1 (Kd)
0x04	"Credit" Key for Application 2 (Kc)
0x05	Application Issuer Area

0x06	Application 1 (User Memory)
…	
0xXX	
0xXX + 1	Application 2 (User Memory)
…	
0x1F	

Figure 4 : Memory layout of pages 1 to 7 of 16K16 card

Data access

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

- On 16K2 cards, biometric data starts at a specific block,
- On 16K16 cards, biometric data starts at a specific page,
- On 32K16 (16K16/16K1) cards, biometric data starts at a specific page of book 0, or at the beginning of book 1.
- On 32K2 (16K2/16K1) cards, biometric data starts at a specific block of book 0, or at the beginning of book 1.

Read data size can be limited using parameter ***sc_tlv_iclass.num_block***.

Pre personalized iClass® card often contain "HID Reserved Area" storing a Wiegand identifier and it is possible to read this area with a MorphoAccess® terminal by configuring ***sc.verify_user_id*** to ***5(HID card number)***

Data access on 16K2 cards

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

By default, read starts at the 19th block, but this value can be modified using parameter ***sc_tlv_iclass.page_offset*** (value from 19 to 177).

Data access on 16K16 cards

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

By default, read starts at page 1. This value can be modified using parameter ***sc.tlv_iclass.page_layout*** (value from 1 to 5).

Data access on 32K16 (16K16/16K1) cards

On 32K16 (16K16/16K1) cards, the terminal can use book 0 and starts the reading process at a defined page like on 16K16 cards.

Additionally, it is possible to configure the terminal to read book 1, using parameter *sc_tlv_iclass.book_number* (value from 0 to 1).

Data access on 32K2 (16K2/16K1) cards

On 32K2 (16K2/16K1) cards, the terminal can use book 0 and starts the reading process at a defined block like on 16K2 cards.

Additionally, it is possible to configure the terminal to read book 1, using parameter *sc_tlv_iclass.book_number* (value from 0 to 1).

HID Seos® card structure

This section concerns only MorphoAccess® SIGMA iClass.

A Seos® card is not defined by a unique serial number but uses a random serial number.

A Seos® card contains "applications" (comparable to a directory). An application is represented by 3 bytes (ADF OID, Application Dedicated File Object IDentifier).

An application may contain up to 8 "data objects" (comparable to a file). A data object is represented by a tag.

Data access

By default, to read biometric data, the MorphoAccess® will read all data objects in an application, starting from the data object **192** stored in the application "**2A8570811E1000070000020000**". These values can be changed using parameters **sc_tlv_seos.adf_oid** and **sc_tlv_seos.first_do_tag**.

Limitations

MorphoAccess® can read only up to 8 successive data objects in the same application.

MorphoAccess® can read only up to 100 bytes per data object.

Terminals are only supporting SEOS 8K (not SEOS 16K).

Warning:

Morpho*Wave* Compact is not able to read data contained in Seos® card.

Section 3 : Data

Data 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$_2$	...

Warning:

Due to the data parsing strategy, TLV should be written in a continuous way and begin at the first byte of the configured reading start address.

There is no mandatory TLV. By consequence, to optimize contactless card reading timings, we recommend to encode only needed data.

Since firmware MorphoAccess® SIGMA 4.6, contactless card data reading is stopped as soon as data don't contain anymore a valid TLV. By consequence, it is not needed anymore to optimize the size of data to read. It is not true for Morpho*Wave* Compact, the complete configured data section will be still read.

User card: data definition

Overview

The user card can contain these elements:

Tag	Value	Description	Products
ID	0x32	User Identifier in ASCII	MorphoAccess® SIGMA Family and MorphoWave Compact
NAME	0x20	User name in ASCII (for screen display)	MorphoAccess® SIGMA Family and MorphoWave Compact
PIN	0x33	User PIN (numeric) code in ASCII (for PIN code check)	MorphoAccess® SIGMA Family and MorphoWave Compact
PKCOMP_1 or BIO_DATA	0x30 0x08	First finger compressed minutiae	MorphoAccess® SIGMA Family and MorphoWave Compact
PKCOMP_2 or BIO_DATA	0x31 0x08	Second finger compressed minutiae	MorphoAccess® SIGMA Family and MorphoWave Compact
BIO_DATA	0x08	Third finger compressed minutiae	MorphoWave Compact only
BIO_DATA	0x08	Fourth finger compressed minutiae	MorphoWave Compact only
BIO_DATA	0x08	Fifth finger compressed minutiae	MorphoWave Compact only
BIO_DATA	0x08	Sixth finger compressed minutiae	MorphoWave Compact only
BIO_DATA	0x08	Seventh finger compressed minutiae	MorphoWave Compact only
BIO_DATA	0x08	Eighth finger compressed minutiae	MorphoWave Compact only
BIOPIN	0x34	This PIN (numeric) code can replace fingerprint check when user's fingerprint cannot be checked (too low number of characteristic points)	MorphoAccess® SIGMA Family and MorphoWave Compact

CARD_MODE	0x35	Authentication process (PIN code check: Yes/No, fingerprint check: Yes/No)	MorphoAccess® SIGMA Family and Morpho*Wave* Compact
EXPIRY_DATE	0x0A	Expiry date of the card	MorphoAccess® SIGMA Family and Morpho*Wave* Compact
BIO_DURESS	0x38	Finger used in case of duress situation	MorphoAccess® SIGMA Family only
BIO ID	0x39	Finger type identification	MorphoAccess® SIGMA Family and Morpho*Wave* Compact
SECURE_DATA	0x0C	Encrypted Data	MorphoAccess® SIGMA Family only

Warning:

Desfire solution is the preferred technology to store biometry of 8 fingers due to much faster performances.

It is not possible to store biometry of 8 fingers using any iClass or SEOS card

User ID tag

TAG_ID	0x32
Presence	Mandatory if terminal is configured to use the biometric user ID.
Description	This tag contains a unique user's identifier (the card holder). 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	24 bytes

Name tag

TAG_NAME	0x20
Presence	Ignored on terminals without screen
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

TAG_PIN	0x33
Presence	Ignored on terminals without screen
Description	User PIN (numeric) code in ASCII. "1234" for example. Used only for PIN code check on MorphoAccess® terminal with keyboard.
Format	ASCII
Length	15 bytes

1st PKCOMP template tag

TAG_PKCOMP_1	0x30
Presence	Mandatory if the control requires a biometric verification, and BIO_DATA is not present.
Description	This tag contains the minutiae of the first enrolled finger according to the PKCOMP170 format. This tag is deprecated, please consider using BIO_DATA instead.
Format	PKCOMP170, binary.
Length	170 bytes

2nd PKCOMP template tag

TAG_PKCOMP_2	0x31
Presence	Mandatory if the control requires a biometric verification, and BIO_DATA is not present.
Description	This tag contains the minutiae of the first enrolled finger according to the PKCOMP170 format. This tag is deprecated, please consider using BIO_DATA instead.
Format	PKCOMP170, binary.
Length	170 bytes

Generic biometric template tag

TAG_BIO_DATA					0x08
Presence	Mandatory if the control requires a biometric verification, and PKCOMP_1 and PKCOMP_2 are not present. This tag can be used twice: for the first and for the second finger.				
Description	This tag contains a TLV formatted structure representing biometric data.				
Format	Generic TLV containing one of these template formats:				

Template Identifier	Description
ID_PKCOMP 0x02	Morpho private format for fingerprint template
ID_PK_FVP 0x81	Morpho private format for fingerprint + vein template

More template formats in Template formats.

For example:

T	TAG_BIO_DATA		08	1 byte
L	Length = 173		AD 00	2 bytes
V	T	ID_PKCOMP	02	1 byte
	L	Length = 170	AA 00	2 bytes
	V	Template data	…	170 bytes

Length	Depends on underlying minutiae format.

BIOPIN tag

TAG_BIOPIN	0x34
Presence	Ignored on terminals without screen
Description	This tag contains the user BIOPIN code. "4321" for example. Can be used only when the MorphoAccess® terminal has a keyboard to replace the fingerprint check by a PIN code check.
Format	ASCII
Length	15 bytes

Card mode tag

TAG_CARD_MODE	0x35
Presence	Mandatory if the "authentication depending on card" access control mode is enabled.
Description	This tag contains the authentication method to use when the terminal lets the card decide.
Format	Binary
Length	1 byte
Available values	0x01 : ID_ONLY (No PIN check, No fingerprint check 0x02 : PKS (No PIN check, with fingerprint check) 0x10 : PIN (with PIN check, no fingerprint check) 0x12 : PIN_THEN_PKS (PIN check, and then fingerprint check)

Whatever is the value of the Card Mode, the terminal searches for the mandatory user's identifier value (ID tag), on the user's contactless card.

Card mode	Access right check process
ID_ONLY	The terminal searches only for user ID value. No fingerprint check, neither PIN code check is performed.
PIN	The terminal searches for the PIN code (PIN tag). Therefore, after reading the card, the PIN code is checked, but no fingerprint check is performed.
PKS	The terminal searches for fingerprints (PKs tags). If there are no fingerprints, it searches for a BIOPIN code (BIOPIN tag). Then, it waits for one user's fingerprint on the sensor, or for BIOPIN code seizure with the keyboard.
PIN_THEN_PK	The terminal searches for a PIN code (PIN tag), and for fingerprints (PKs tags). If there are no fingerprints, it searches for a BIOPIN code (BIOPIN tag). Then it waits for the user's PIN code seizure with the keyboard, then for one user's fingerprint on the sensor or for BIOPIN code seizure (with keyboard).

Expiry date tag

TAG_EXPIRY_DATE		0x0A
Presence	Optional	
Description	This tag contains the expiry date of the card. After this date, the card will be rejected by the terminal.	
Format	Year on 2 bytes Month on 2 bytes Day on 2 bytes Hour on 2 bytes Minute on 2 bytes Second on 2 bytes Example :	
Length	12 bytes	

07 DD	Year: 2013
00 0C	Month: 12 (December)
00 19	Day: 25 (25th)
00 01	Hour: 1
00 1E	Minute: 30
00 32	Second:50

NOTE:

1. Only Date is used during verification.
2. For the infinite expiry date, configure the value of Year, Month and Day to 0.

Duress finger tag (MorphoAccess® SIGMA Family only)

TAG_BIO_DURESS				**0x38**
Presence	Optional. If present and duress check is enabled on terminal, it will be used to know if user is in duress situation.			
Description	This tag contains a TLV formatted structure representing biometric data.			
Format	Generic TLV containing one of these template formats:			

Template Identifier	Description
ID_PKCOMP 0x02	Morpho private format for fingerprint template
ID_PK_FVP 0x81	Morpho private format for fingerprint + vein template

More template formats in [Template formats](#).

For example:

T	**TAG_BIO_DURESS**		38	1 byte
L	Length = 173		AD 00	2 bytes
V	T	ID_PKCOMP	02	1 byte
	L	Length = 170	AA 00	2 bytes
	V	Template data	…	170 bytes

Length	Depends on underlying minutiae format.

Secure Data tag

TAG_SECURE_DATA	0x0C
Presence	Optional
Description	This tag contains encrypted other TLV. It could contain any type and any number of TLV. Data are protected using an AES 128 bits key. This is recommended protection for unsecured contactless technology.
Format	Binary
Length	Depend of content

Admin card: data definition

Overview

An Admin Card allows changing contactless 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 current keys (K_n) become old keys (K_{n-1}).

The administrator has just to present the Admin Card to the terminal: a message indicating that the key rotation is successful will be displayed on the screen.

There are 3 types of Admin Card:

- ADMIN card:
    - lets the user change the MIFARE® Classic keys (or iClass® keys for MorphoAccess® terminals equipped with an iClass® contactless smartcard reader),
    - the card is a MIFARE® Classic card (or an iClass® card),
    - is compatible with all the MorphoAccess® terminal that are able to read MIFARE® Classic cards (or an iClass® cards).

- ADMIN_MIFARE_PLUS_SL3 card:
    - lets the user change the MIFARE® Plus keys,
    - the card is a MIFARE® Plus card,
    - is compatible with all the MorphoAccess® terminal that are able to read MIFARE® Plus cards.

- ADMIN_DESF_DES3 card:
    - lets the user change the DESFire® 3DES keys,
    - the card is a DESFire® 3DES card,
    - is compatible with all the MorphoAccess® that are able to read DESFire® cards.

- ADMIN_DESF_AES card:
    - lets the user change the DESFire® AES keys,
    - the card is a DESFire® AES card,
    - is compatible with all the MorphoAccess® that are able to read DESFire® cards.

Due to security level, a MIFARE® card is not able to change DESFire® keys, and a DESFire® 3DES card is not able to change DESFire® AES keys.

NOTES:

- If the ADMIN tag is present, the other tags (including ADMIN_DESF_DES3 tag) will be ignored.

- If the ADMIN_DESF_DES3 tag is present, the other tags will be ignored.
- If the ADMIN_DESF_AES tag is present, the other tags will be ignored.

DESFire® 3DES Admin Card

This section concerns only MorphoAccess® terminals equipped with a DESFire® contactless smartcard reader.

TAG_ADMIN_DESF_DES3		0x04
Presence	Other tags are ignored	
Description	The value field contains the new keys.	
Format	1 byte	Version of 3DES PICC_MASTER_KEY
	16 bytes	New 3DES PICC_MASTER_KEY key
	1 byte	Version of 3DES APP_WRITE_KEY
	16 bytes	New 3DES APP_WRITE_KEY key
	1 byte	Version of 3DES BIO_FILE_READ_KEY
	16 bytes	New 3DES BIO_FILE_READ_KEY key
Length	3 * (1 + 16) bytes	

DESFire® AES Admin card

This section concerns only MorphoAccess® terminals equipped with a DESFire® contactless smartcard reader.

TAG_ADMIN_DESF_AES		0x09
Presence	Other tags are ignored	
Description	The value field contains the new keys.	
Format	1 byte	Version of AES PICC_MASTER_KEY
	16 bytes	New AES PICC_MASTER_KEY key
	1 byte	Version of AES APP_WRITE_KEY
	16 bytes	New AES APP_WRITE_KEY key
	1 byte	Version of AES BIO_FILE_READ_KEY
	16 bytes	New AES BIO_FILE_READ_KEY key
Length	3 * (1 + 16) bytes	

Mifare® Classic Admin card

This section concerns only MorphoAccess® terminals equipped with a MIFARE® contactless smartcard reader.

TAG_ADMIN		**0x03**
Presence	This is the unique TLV on the card.	
Description	The value field contains the new keys for each sector.	
Format	The value field contains the new key "one after the other". For a 1K card there are 16 keys sets (A and B) For a 4K card there are 40 keys sets (A and B)	
	6 bytes	New KA sector 0
	6 bytes	New KB sector 0
	6 bytes	New KA sector 1
	…	…
	6 bytes	New KA sector 15 (1K) or sector 39 (4K)
	6 bytes	New KB sector 15 (1K) or sector 39 (4K)
Length	480 bytes to change MIFARE® 4K card keys (6 bytes x 2 x 40).	
	192 bytes to change MIFARE® 1K card keys (6 bytes x 2 x 16).	

iClass® Admin card

This section concerns only MorphoAccess® terminals equipped with an iClass® contactless smartcard reader.

TAG_ADMIN		**0x03**
Presence	This is the unique TLV on the card.	
Description	The value field contains the new keys for each sector.	
Format	The value field contains 9 keys sets, defined by an index, key 1 (8 bytes) and key 2 (8 bytes)	
	1 byte	Key index
	8 bytes	New Key 1
	8 bytes	New Key 2
	1 byte	Key index
	8 bytes	New Key 1

8 bytes	New Key 2
…	…
1 byte	Key index
8 bytes	New Key 1
8 bytes	New Key 2

where Key index is:

- 0 for Book 0 Page 0
- 1 for Book 0 Page 1
- …
- 7 for Book 0 Page 7
- 8 for Book 1

Length	153 bytes(2 x 8 +1) x 9).

Mifare® Plus Admin card

This section concerns only MorphoAccess® terminals equipped with a MIFARE® contactless smartcard reader.

TAG_ADMIN_MIFARE_PLUS_SL3		**0x0B**
Presence	This is the unique TLV on the card.	
Description	The value field contains the new keys for each sector.	
Format	The value field contains the new key "one after the other". For a 1K card there are 16 keys sets (A and B) For a 4K card there are 40 keys sets (A and B)	
		16 bytes	New KA sector 0
		16 bytes	New KB sector 0
		16 bytes	New KA sector 1
		…	…
		16 bytes	New KA sector 15 (1K) or sector 39 (4K)
		16 bytes	New KB sector 15 (1K) or sector 39 (4K)
Length	1280 bytes to change MIFARE® 4K card keys (16 bytes x 2 x 40). 512 bytes to change MIFARE® 1K card keys (16 bytes x 2 x 16).	

Section 4 : Annexes

Template formats

Templates to store using BIO_DATA tag or BIO_DURESS tag are also in TLV format.

PKCOMP V2

T	0x02	1 byte
L	Template length	2 bytes
V	Template data	N bytes (max. 256)

PKMAT

T	0x03	1 byte
L	Template length	2 bytes
V	Template data	512 bytes

ANSI 378-2004

T	0x3F	1 byte
L	Total length	2 or 4 bytes
V	0x40	1 byte
	0x02	2 bytes
	Finger to use	1 byte
	Use all fingers	1 byte
	0x41	1 byte
	Template length	2 or 4 bytes
	Template data	N bytes

Finger to use: numeric value that selects only one of the fingerprints included in the minutiae record. The value in this field is ignored when the "Use all fingerprints" field is set to 0x01.

- 0x00 selects first fingerprint (recommended value for a single fingerprint minutiae record)
- 0x01 selects the 2nd fingerprint
- ...
- N selects the N+1 fingerprint

Use all fingers: numeric value that defines how many fingerprints have to be used within the minutiae record:

- 0x00: use only one fingerprint, the one selected by the "Finger to use" field (recommended value for a single fingerprint minutiae record).
- 0x01: use all the fingerprints available in the minutiae record.

Warning: Morpho*Wave* Compact doesn't accept template with multiple fingers.

ISO19794-2 Finger Minutiae Card Record, Compact Size

T	0x3F	1 byte
L	Total length	2 bytes
V	0x40	1 byte
	0x02	2 bytes
	0x00	1 byte
	0x00	1 byte
	0x6C	1 byte
	Template length	2 bytes
	Template data	N bytes

ISO19794-2 Finger Minutiae Card Record, Normal Size

T	0x3F	1 byte
L	Total length	2 or 4 bytes
V	0x40	1 byte
	0x02	2 bytes
	0x00	1 byte
	0x00	1 byte
	0x6D	1 byte
	Template length	2 bytes
	Template data	N bytes

ISO19794-2 Finger Minutiae Record

T	0x3F	1 byte
L	Total length	2 bytes
V	0x40	1 byte
	0x02	2 bytes
	Finger to use	1 byte
	Use all fingers	1 byte
	0x6E	1 byte
	Template length	2 or 4 bytes
	Template data	N bytes

Finger to use: numeric value that selects only one of the fingerprints included in the minutiae record. The value in this field is ignored when the "Use all fingerprints" field is set to 0x01.

- 0x00 selects first fingerprint (recommended value for a single fingerprint minutiae record)
- 0x01 selects the 2nd fingerprint
- …
- N selects the N+1 fingerprint

Use all fingers: numeric value that defines how many fingerprints have to be used within the minutiae record:

- 0x00: use only one fingerprint, the one selected by the "Finger to use" field (recommended value for a single fingerprint minutiae record).
- 0x01: use all the fingerprints available in the minutiae record.

Warning: Morpho*Wave* Compact doesn't accept template with multiple fingers.

ISO19794-2 Finger Minutiae Card Record, Compact Size(AA)

T	0x3F	1 byte
L	Total length	2 or 4 bytes
V	0x40	1 byte
	0x02	2 bytes
	0x00	1 byte
	0x00	1 byte
	0x7F	1 byte
	Template length	2 bytes
	Template data	N bytes

Minex A (MorphoAccess® SIGMA Family only)

T	0x3F	1 byte
L	Total length	2 bytes
V	0x40	1 byte
	0x02	2 bytes
	0x00	1 byte
	0x00	1 byte
	0x6F	1 byte
	Template length	2 bytes
	Template data	N bytes

PKLITE

T	0xCC	1 byte
L	Template length	2 bytes
V	Template data	N bytes

DIN_V66400_CS (MorphoAccess® SIGMA Family only)

T	0x3F	1 byte
L	Total length	2 bytes
V	0x40	1 byte
	0x02	2 bytes
	0x00	1 byte
	0x00	1 byte
	0x7D	1 byte
	Template length	2 bytes
	Template data	N bytes

DIN_V66400_CS_AA (MorphoAccess® SIGMA Family only)

T	0x3F	1 byte
L	Total length	2 bytes
V	0x40	1 byte
	0x02	2 bytes
	0x00	1 byte
	0x00	1 byte
	0x7E	1 byte
	Template length	2 bytes
	Template data	N bytes

MULTIMODAL (FVP)

T	0x81	1 byte
L	Template length	2 bytes
V	Template data	N bytes

Head office :

IDEMIA

2, place Samuel de Champlain

92400 Courbevoie France

www.idemia.com