MorphoSmart™ Overview

Version 1.18

MSO OEM

MSO20x/MSO30x

MSO35x

CBM OEM

MSO1300

MSO1350

Copyright notices

Revision History

Revision	Date	Document revision history
1.0	25th February 2004	Document creation
1.1	24th June 2004	Smart Card overview
1.2	16th July 2004	IDENTLITE License overview
1.3	15th December 2004	Some corrections and add MSO CBM
1.4	7th April 2005	Biometric tokens conformity with the X9.84 format Update of hotline phone number
1.5	25th July 2005	Added False Finger Detection Overview for MSO XX1 terminals (Chap. 3)
1.6	22th September 2005	Update of company name.
1.7	20th January 2006	MSO accepts new templates format as ANSI 378 or ISO 19794-2 Modified template numbers. Added information about the biometric coder.
1.8	15th June 2006	Modified hotline number Modified the licenses definition.
1.9	August,17th 2007	Update of company name.
1.10	January 2009	Change uncorrected values in FAR table (2 and 4 threshold) please refer to section Matching Threshold value.
1.11	September 2009	Update hotline mail address
1.12	July 2010	Update company name to Morpho
1.13	April 2011	Upgrade document format
1.14	March 2013	Update hotline address and registered office address
1.15	October 2013	Update product images for CBM from 2014
1.16	December 2013	Update template format
1.17	May 2015	Update footer legal text
1.18	Feb. 2018	Update company's logo

Table of Contents

List of Figures

List of Tables

1 Conventions

This section presents acronyms, abbreviations, measurement units, and conventions used in this document.

1.1 Acronyms and abbreviation

Acronym/Abbreviation	Definition
ILV	Identifier Length Value.
PK	Characteristics points (minutiae) of a fingerprint used by a biometric process.
FAR	False Acceptance Rate: probability that a finger is falsely accepted by the system.
FRR	False Rejection Rate: probability that a correct finger is falsely rejected by the system.

Table 1: Acronyms and Abbreviations

2 Scope

2.1 Identification

This document describes the main functionalities of the MorphoSmart™ and MorphoSmart™ Compact Biometric Module (CBM), and gives an overview on fingerprint and security issues.

3 Fingerprint Basic Knowledge

3.1 About Fingerprints

Fingerprints are permanent and unique. They are formed before birth and last throughout one's life. Classification and systematic matching of fingerprints for different purposes have been in use since the late 19th century.

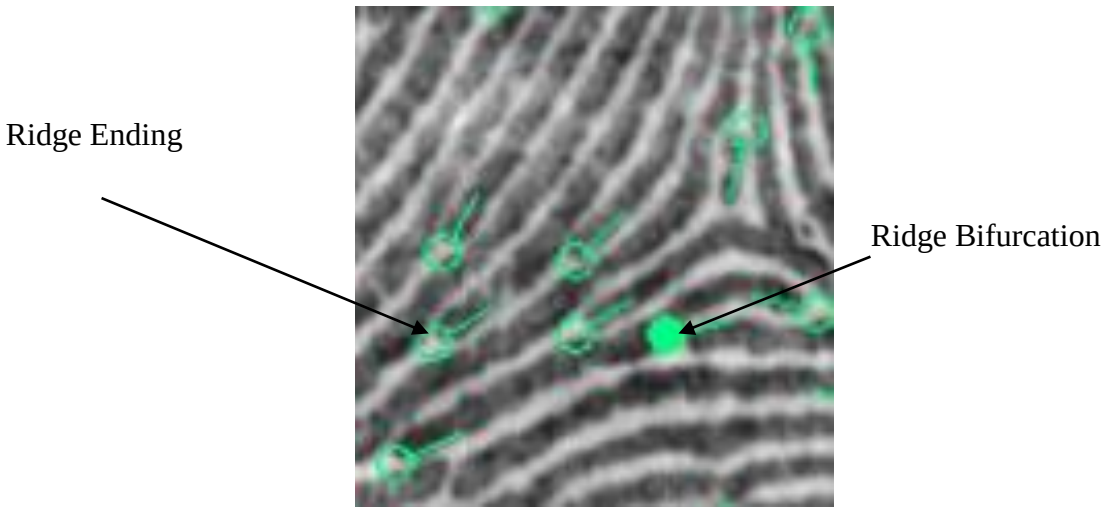

Figure 1: Minutiae are classified in two categories: Ridge ending and bifurcation

Present on your fingers is skin, which is different from that on other areas of your body. This skin is rough or corrugated, consisting of raised portions that are called ***ridges***. These ridges do not run continuously from one side to the other, rather they may curve, end, or divide into two or more ridges (***bifurcation*** and ***endings***). Barring accidental or intentional mutilation, the ridge arrangement is permanent.

Fingerprints can be divided into major ridge pattern type such as Whorls, Loops and Arches etc. Unique characteristics known as ***Minutiae*** identify those points of a fingerprint where the ridges become bifurcation or endings, as illustrated in **Figure 1**. These minutiae are the unique features, which form the basis of any system using fingerprint comparison techniques for identification and verification purposes.

3.2 How does it work?

3.2.1 Image Acquisition

Acquisition is performed with a CMOS camera.

3.2.2 Image Processing and Features Detection

Image processing and features detection is a threefold process:

- First, the software analyzes the grayscale image. The image is then filtered in order to remove 'noise' and obtain the best-binarized image as possible, thereby facilitating the detection of bifurcations, endings and other minutiae characteristics.
- Second, the software uses the binarized image to determine the 'skeleton' of the fingerprint image, thus creating skeletons for ridges and valleys.
- Third, the system produces a minutiae list – biometric template - obtained after analysis of the two skeletons.

The biometric template is a mathematical representation of the original fingerprint based on the analysis of the ridge patterns. The template maximum size is 256 bytes[1] and is used during the matching process to compare it against previously stored templates.

[1] The template size depends on the template format. Please refer to the template description chapter.

3.2.3 Matching

During the verification process, the system does not compare fingerprint images. It compares the minutiae, which were detected while coding the fingerprint image. After processing, the image has a corresponding cloud of minutiae (see **Figure 2**).

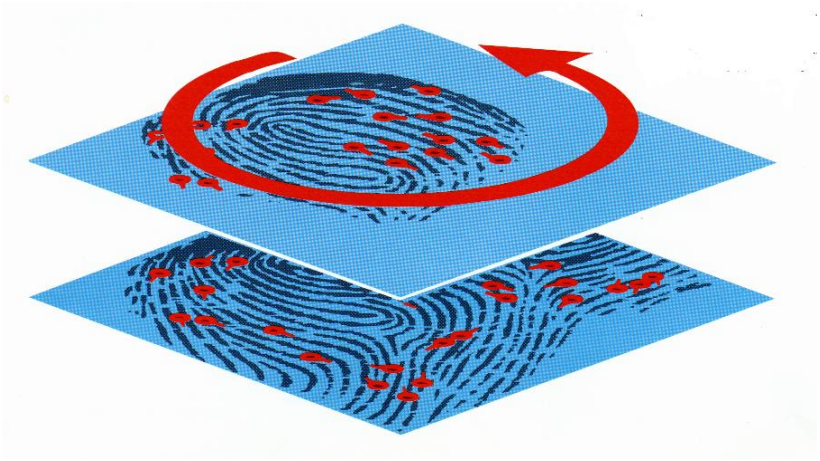

Figure 2: Matching process

The 'cloud' of minutiae for a search fingerprint is compared with the 'cloud(s)' of minutiae corresponding to those fingerprint images stored either in the system permanent database or on an external source such as smart card, 2D bar code, ...etc.

When two minutiae clouds are compared, a score is processed. When the score is above a given threshold the two templates are assumed to be from the same finger.

Two types of error can occur in a biometric system, a *False Accept* (hit) and a *False Reject* (no hit):

- A False Accept occurs when two biometric templates which should not match (belong to different people) are determined to match (score higher than the threshold),
- A False Reject occurs when two biometric templates that should match (belong to the same person) are determined not to match (score lower than the threshold).

It is important to notice that the user can adapt the algorithm's performance to his/her requirement simply by adjusting the False Acceptance Rate via the application.

4 MorphoSmart™ Architecture overview

4.1 Scheme

The following figure describes the MorphoSmart™ software architecture:

<table>
<tr><td colspan="5">ILV Interface</td><td rowspan="3">SmartCard Interface</td></tr>
<tr><td>Database</td><td>Module Manager</td><td rowspan="2">Biometric algorithms</td><td>SPILV</td><td>Image</td></tr>
<tr><td colspan="2">File System</td><td>Com</td><td>Sensor</td></tr>
</table>

Figure 3: General MorphoSmart™ Architecture

4.2 File system

The MorphoSmart™ incorporates a specifically designed file system. This file system resides in flash memory. The file system implements the following characteristics:

- File creation / deletion,
- File writing / reading,
- File search,
- Flash garbage collector: file system is resident in flash. When a file is deleted, the available space is not instantaneously retrieved in order to optimize time execution (note: sensitive files are physically erased). In the case the whole flash is fragmented, it would take about 10 seconds (depending on flash fragmentation) to process a whole garbage collector operation. To avoid such a long waiting time, MorphoSmart™ implements an automatic garbage policy: when 90% of the “free” space can be retrieved, part of the garbage collector is performed (<1 second). Thanks to this dynamic policy, commands overhead are not a nuisance.

4.3 Module manager

MorphoSmart™ software has a great modularity. It is designed as a collection of executable packages. In order to have efficient performance, only the used packages are loaded in RAM.

MorphoSmart™ manages different modes (regular mode, download mode...) that use a different collection of packages.

4.4 Database

4.4.1 Generalities

The MorphoSmart™ manages an internal database that stores templates (minutiae) and user attributes (for example name, address ...). This database can be filled during an enrollment (live fingerprint acquisition) or with an already existing compatible biometric database.

A database is a collection of records. Records are a collection of fields.

Each record contains data relative to one enrolled person: his/her minutiae and his/her attributes (for example name, address ...).

Database records contain the following fields:

Field	Description
Index	Unique internal index number (used only internally for optimization purposes),
UserID	User unique identifier that can be freely retrieved from the database,
Template	One-or two-finger minutiae template that cannot be retrieved,
Public data	Field that can be freely retrieved from the database,
Private data	Field that can only be retrieved upon successful biometric identification

Table 2: Database record content

Records are referenced by their UserID.

All fields (UserID and supplementary fields) are managed as byte arrays. If you need to use string, do not forget to manage the ending '\0'.

One-finger and two-finger templates can be freely mixed in the database.

During database creation the programmer specifies:

- Maximum number of records,
- Maximum number of templates per record,
- Maximum number of fields per record,
- Maximum field size (for each field).

The MorphoSmart™ reserves the necessary flash memory during database creation to guarantee that those characteristics can be fulfilled any time.

Once created, it is not possible to modify the database internal structure.

Example:

It is possible to store a login name (public data) and its associated password (private data) in the MorphoSmart™ terminal.

UserID (field0)	Template1	Template2 (optional)	Login (field1)	Password (field2)	Some more public data... (field3)	...

Figure 4: Internal database structure example

In the above example:

- Green: fields that can freely be retrieved from the database,
- Black: fields that can never be retrieved,
- Red: fields that can only be retrieved upon successful biometric identification.

4.4.2 Licenses

The MorphoSmart™ device supports 2 types of license:

- IDENTLITE
- IDENTPLUS

These licenses enable to store more users than in a standard MorphoSmart™ device. Please refer to the *MorphoSmart Host System Interface specifications* document, for full details on this feature, and database size limits of your product.

4.5 Biometric Algorithms

The algorithms supported by MorphoSmart™ are part of MorphoSoft™ product line. These algorithms have been designed for different hardware platforms based on ARM or TMS components.

Since software release 06.03, the MorphoSmart™ is able to manage both juvenile and adult finger images.

This provides a solution with reliable performance to the automatic processing of finger images with small to normal ridges, extending the capability of the terminal by providing access control to a wider range of population. Since the encoding time is longer when the juvenile option is turned on, we offer the possibility to the user set up the terminal either in "Juvenile" mode or in standard mode. When the juvenile mode is turned on, young children can easily be enrolled on the MorphoSmart™.

Unless you have a specific need of enrolling young children or small ridges fingers, Morpho recommends using the default biometric coder.

4.6 Com

For the MorphoSmart™, the Com module is in charge of RS232 or USB management. This separate module allows changing the communication interface easily.

For the MorphoSmart™ CBM the product can be interfaced either using a serial link (Open collector) or a USB connection.

4.7 SPILV

The SPILV module is in charge of the ILV management.

4.8 Image

The MorphoImaging™ optimizes the image quality during acquisition and pre-processing.

4.9 Sensor

The Sensor module drives the CMOS camera.

4.10 ILV Interface

ILV interface is the MorphoSmart™ application interface. A Host system can drive the MorphoSmart™ by sending ILV request.

4.11 Smart Card Interface

The Smart Card Interface is CCID compliant. For more information, please refer to the Universal Serial Bus Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.00 ,March 2001 or to http://www.usb.org.

5 Biometry

5.1 Services

The biometric algorithms implement the following functions:

- **Capture:** a live finger is captured from MorphoSmart™, converted to a numeric template and exported (useful for external storage media: smart card, magnetic strip...),
- **Enrollment:** a live finger is captured from MorphoSmart™, converted to a numeric template and stored in a database,
- **Verify (1 vs 1 up to 20 matching):** a live finger is matched against one up to twenty given reference templates,
- **Identify (1:N matching):** a live finger is matched against the whole database,
- **VerifyMatch (1 vs 1 up to 20 matching):** one candidate template is matched against one up to twenty given reference templates,
- **IdentifyMatch (1:N matching):** one unique candidate template is matched against the whole database.

5.2 Template format

In most of the applications, only PK_COMP should be used.

The following template formats are also managed by the MorphoSmart™:

- *PK_COMP*: compressed standard template. This is the format that should be used in most of the developments. **This is the template that gives the best results.**
- *PK_COMP_NORM*: normalized template format that should only be used when required for compatibility with other existing Morpho systems or for some specific applications. This template is dedicated to systems that need to recognize an adult with a finger enrolled during his/her childhood.
- *PK_MAT_NORM* (little endian): normalized uncompressed template format that should only be used when required for compatibility with other Morpho systems.
- *PK_MAT* (little endian): uncompressed template format that should only be used when required for compatibility with other Morpho systems.
- *ANSI INCITS 378-2004*, to use for compatibilities issues
- *ANSI INCITS 378-2009*, to use for compatibilities issues
- *MINEX A* Specification, to use for compatibilities issues
- *ISO/IEC CD 19794-2* Finger Minutiae Record, to use for compatibilities issues
- *ISO/IEC CD 19794-2* Finger Minutiae Record Version 2011, to use for compatibilities issues
- *ISO/IEC CD 19794-2* Finger Minutiae Card Record, Normal Size, to use for compatibilities issues
- *ISO/IEC CD 19794-2* Finger Minutiae Card Record, Compact Size, to use for compatibilities issues

5.3 Enrollment Requirements

A good quality for the reference template increases biometric performances. For this reason, MorphoSmart™ enrollment consists in three acquisitions. These 3 acquisitions are processed in order to generate a better reference template.

To obtain the best accuracy, it is strongly recommended to use the fore, the thumb or the middle fingers.

5.4 Matching Threshold value

This parameter can be set to values from 0 to 10. This parameter specifies how tight the matching threshold is. Morpho recommends threshold 5, but according to your application requirements you can adjust this threshold in order to have a more secure control (higher threshold, less false acceptances) or a more comfortable control (lower threshold, less false rejections).

We remind that the better the FAR is, the worse the FRR is, and vice versa. FRR varies from one kind of population to another (FRR is better with people who perform limited manual labor and have good quality fingerprints than with hard manual laborers with damaged fingerprints).

FAR is specified (see table below) to 1-finger mode, 2-finger mode, authentication mode and identification mode.

Threshold scoring values are identified below:

0	Low threshold for test purposes only. There are few rejections, but more false acceptances.
1	FAR < 1 %
2	FAR < 0.5 %
3	FAR < 0.1%
4	FAR < 0.05 %
5	Recommended value. FAR < 0.01 %.
6	FAR < 0.001 %
7	FAR < 0.0001 %
8	FAR < 0.00001 %
9	FAR < 0.0000001 %
10	High threshold for test purposes only. There are very few false acceptances, but many rejections.

Table 3: Relation between Matching Threshold and False Acceptance Rate

6 Graphical User Interface

In order to build friendly user interfaces, the MorphoSmart™ manages asynchronous messages that indicate the current status of a live acquisition.

Asynchronous messages are managed for all live finger acquisition functions: Capture, Enroll, Verify, Identify and DbVerifyAndUpdate. Reception of these messages is performed thanks to callback functions, and is fully customizable. Asynchronous information statuses are:

- Messages to the user (press harder, finger more left, remove finger...),
- The finger number and acquisition number during the enrollment process,
- A low-resolution finger image has been received.

The Graphical User Interface has the possibility to define callbacks during live finger acquisitions. If defined, the callback is processed each time an asynchronous event is received.

Live finger acquisition ends when one of the following events occurs:

- Timeout expiration (timeout could be infinite if required),
- A finger is detected,
- A cancel command is executed.

Figure 5 gives an example of a live finger acquisition workflow managed by a PC.

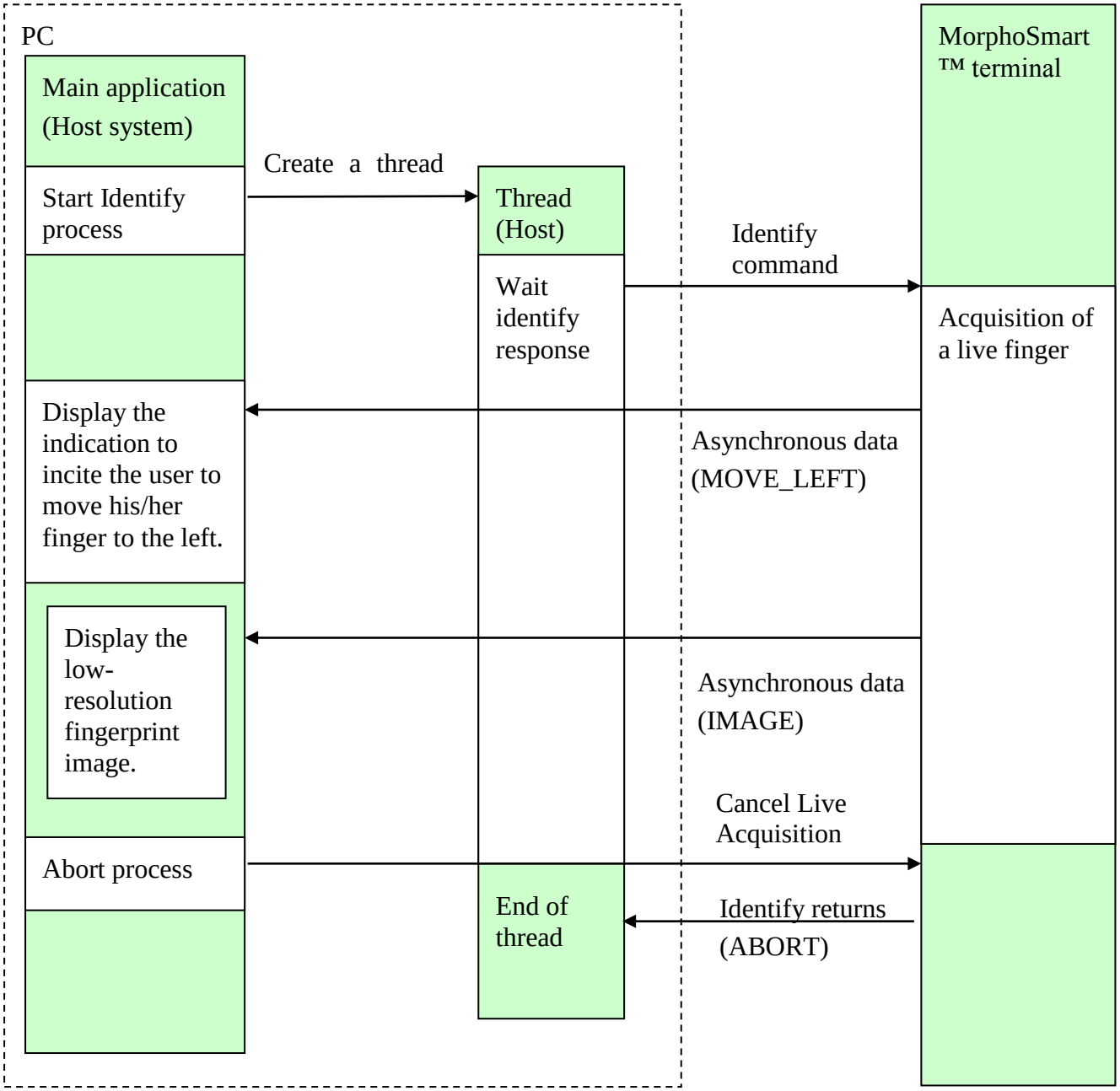

Figure 5: Live acquisition management sample (Identify command)

7 Security

7.1 Overview

A secure MorphoSmart™ includes multiple security protections:

- A secure MorphoSmart™ accepts only the firmware signed by Morpho (firmware integrity).
- During the transport between Morpho and the customer, a secure MorphoSmart™ can't be used. The device is protected with transport keys which enciphered every security data.
- A secure MorphoSmart™ verify a signed template within a X9.84 envelop (template integrity).
- A secure MorphoSmart™ can export a signed template within a X9.84 envelop (template integrity).
- A secure MorphoSmart™ can use two secured protocols security:
  - An offered security protocol:
    - Replay attacks,
    - Integrity insurance (RSA or DSA signature).
  - A tunneling protocol:
    - Mutual authentication,
    - Replay attacks,
    - Integrity insurance (RSA or DSA signature),
    - Confidentiality (3DES encryption).

7.2 Biometric Token

The biometric templates are encapsulated within an X9.84 format (See the norm X9.84 2003 - Biometric Information Management and Security for the Financial Services Industry). Biometric tokens are ASN.1 DER encoded.

7.2.1 ASN.1 syntax

```
BiometricSyntaxSets ::= SEQUENCE SIZE (1..MAX) OF BiometricSyntax {
    BiometricSyntax.integrityObjects = IntegrityObjects ::= SEQUENCE {
        biometricObjects ::= SEQUENCE {
            BiometricObjects ::= SEQUENCE SIZE (1..MAX) OF {
                BiometricObject ::= SEQUENCE {              -- TEMPLATE i
                    BiometricHeader ::= SEQUENCE {
                        version       BiometricVersion      DEFAULT hv1,
                        recordType        RecordType        OPTIONAL,
                        dataType      DataType              OPTIONAL,
                        purpose       Purpose               OPTIONAL,
                        quality       Quality               OPTIONAL,
                        validityPeriod    ValidityPeriod        OPTIONAL,
                        format            Format ::= SEQUENCE {
                                          FormatOwner   IBIA manufacturer OID,
                                          FormatType
                                              SagemFormatType ::= SEQUENCE {
                                                  Version       INTEGER           DEFAULT 0,
                                                  SignerID      OCTET STRING      OPTIONAL,
                                                  ApplicativeData   OCTET STRING  OPTIONAL,
                                                  OrganID       INTEGER           OPTIONAL,
                                                  other OPTIONAL parameters must be defined
                                                      by the application.
                                              } OPTIONAL
```

```
                        } OPTIONAL
                    }
                    BiometricData OCTET STRING (SIZE(1..MAX))
                }
            }
        }
        IntegrityBlock ::= SEQUENCE {
            algorithmID  SignatureAlgorithmIdentifier,  --          dsa-with-sha1          or
    sha1WithRSAEncryption
            signature        OCTET STRING               --   signature   is   performed   on
    BiometricObjects
        }
    }
}
```

7.2.2 Morpho supplementary fields

The field ”BiometricHeader / Format / FormatOwner” identifies the manufacturer (or biometric provider) thanks to an identifier (OID) reserved at the IBIA.

X9.84 lets the possibility to define a manufacturer proprietary structure in the field “BiometricHeader / Format / FormatType”. Morpho proprietary structure is defined as:

```
SagemFormatType ::= SEQUENCE {
        Version             INTEGER                 DEFAULT 0,
        SignerID OCTET STRING               OPTIONAL,
        ApplicativeData     OCTET STRING            OPTIONAL,
        OrganID             INTEGER                 OPTIONAL,
        …other OPTIONAL parameters must be defined by the application.
}
```

Version = Version of this structure. Default value is 0 (v1).

SignerID = Signer identifier. This identifier is the SHA-1 hash of the signer certificate (as proposed within X9.84).

OrganID = Structure that identifies the biometrics organ. This subtype is compliant with 7816-11 definition:

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Subtype
0	0	0	0	0	0	0	0	No information given
		1						Mask, always set to 1 with this representation
						0	1	Right
						1	0	Left
			0	0	0			No meaning
			0	0	1			Thumb
			0	1	0			Pointer finger
			0	1	1			Middle finger
			1	0	0			Ring finger
			1	0	1			Little finger
x	x							RFU (default 0)

Table 4: X9.84 structure, Biometric Organ ID

ApplicativeData = Octet string that is under definition of the application. This string can be reformatted with other structures.

7.2.3 Non redundancy principle

Header of the structure is duplicated within each minutia. Some data such as IBIA manufacturer OID, applicative data and signer identifier are global to the token. In order to avoid application information duplication, only the first object shall contain the format sequence.

7.2.4 Biometric Data

BiometricData field contains a template that represents the extracted biometric characteristics. X9.84 does not provide further indications within this format.

Biometric data are the concatenation of:

- one byte that indicates template format:

Value	Signification
0	PK_COMP v2
1	PK_MAT_NORM. Normalized PK_MAT
2	PK_COMP_NORM. Normalized PK_MAT (little endian)
3	PK_MAT (little endian)
65	ANSI INCITS 378-2004
77	ANSI INCITS 378-2009
108	ISO/IEC CD 19794- Finger Minutiae Card Record Compact Size
109	ISO/IEC CD 19794- Finger Minutiae Card Record Normal Size
110	ISO/IEC CD 19794- Finger Minutiae Record
76	ISO/IEC CD 19794- Finger Minutiae Record Version 2011
111	MINEX A

- the raw template

Example:

Tag (Hex)	Length	Value (Hex)	Signification
30	L		SEQUENCE OF BiometricSyntax.integrityObjects (BiometricSyntaxSets)
A1	L		SEQUENCE IntegrityObjects
A0	**L**		**SEQUENCE biometricObjects**
30	**L**		**SEQUENCE OF BiometricObject (BiometricObjects)**
30	**L**		**SEQUENCE BiometricObject -- FIRST TEMPLATE**
A0	**L**		**SEQUENCE Header**
A6	**L**		**SEQUENCE Format**
A0	**03**		**FormatOwner**
81	**01**	**1D**	**RELATIVE-OID IBIA-owner / Morpho**
A1	**L**		**FormatType : SagemFormatType**
30	**L**		**SEQUENCE FormatType**
81	**L**	**X**	**SignerID**
82	**L**	**X**	**OCTET STRING ApplicativeData**
81	**L**		**OCTET STRING BiometricData**
30	**L**		**SEQUENCE BiometricObject -- SECOND TEMPLATE**
A0	**00**		**SEQUENCE Header (empty)**
81	**L**	**X**	**OCTET STRING BiometricData**
A1	L		SEQUENCE IntegrityBlock
A0	L		SEQUENCE DigitalSignature
A0	L		SignatureAlgorithmIdentifier
06	L	X	OID SignatureAlgorithms (see above)
81	L	X	OCTET STRING Signature

Table 5: X9.84 structure, sample

Data colored in bold blue are signed.

The field ”ApplicativeData” contains the customer data.

The field ”OID SignatureAlgorithms” can have the following values:

Tag	Length	Value	Signification
06	07	2A 86 48 CE 38 04 03	dsa-with-sha1 (DSA algorithm, SHA-1 hash) ⇨ signature is 40 bytes
06	09	2A 86 48 86 F7 0D 01 01 05	sha1WithRSAEncryption (RSA algorithm, SHA-1 hash) ⇨ signature is module size length (128 bytes with RSA1024 bits) ⇨ signature is module size length (256 bytes with RSA2048 bits)

Table 6: X9.84 structure, OID signature

8 Smart Card

When available, the smart card reader functions can directly be accessed through the Microsoft PC/SC layer.

Sample source code of Microsoft Win32 SCard functions calls are given in the 'MSO_Demo' demonstration project included in the MorphoSmart™ SDK package.

For more information please refer to http://www.pcscworkgroup.com.

9 Bibliography

9.1 General information about MSO product family

MorphoSmart™ Overview (ref. SSE-0000080368)

9.2 Integration of EOM modules

MorphoSmart™ module Integration (ref. SSE-0000080364)

MorphoSmart™ CBM module integration (ref. SSE-0000077475)

9.3 Installation of Desktop terminals

MorphoSmart™ Installation (ref: SSE-0000080361)

9.4 ILV Protocol, Description of command

MorphoSmart™ Host System Interface specifications (.chm)

9.5 MorphoSmart™ SDK

MorphoSmart™ SDK Programming guide (.chm)

10 Contacts

10.1 Customer service

Morpho

SAV Terminaux Biométriques

Boulevard Lénine - BP428

76805 Saint Etienne du Rouvray

FRANCE

Phone: +33 2 35 64 53 52

10.2 Hotline and Customer assistance

Morpho

Support Terminaux Biométriques

18, Chaussée Jules César

95520 Osny

FRANCE

hotline.biometrics@idemia.com

Phone: + 33 1 58 11 39 19

(9H00am to 6H00pm French Time, Monday to Friday)

www.biometric-terminals.com

(Login and password are required to access to the private area of the web site).

Registered Office:
11, boulevard Gallieni - 92130 Issy-les-Moulineaux - France

www.idemia.com