ELECTRONICS
MICROELECTRONICS
INNOVATIVE PRODUCTS

Understand – Analyse – Design - Evolve

FINGERPRINT MATCH-ON-CARD 3.30

API SPECIFICATIONS

Revision 1.5

30/03/2015

Legal Information

Revision History

Revision	Date	Description
1.0	16/06/2011	First release.
1.1	09/09/2011	Changed value of working buffer size
1.2	07/10/2011	Updated BIT
1.3	07/06/2012	Added legal information and revision history
1.4	28/09/2012	id3 Semiconductors becomes id3 Technologies Some precisions added to the API reference and Use Case.
1.5	30/03/2015	Added FNMR versus FMR table

Table of Contents

1. Introduction 5

1.1. Purpose 5
1.2. Terms and definitions 5
1.3. Symbols and abbreviated terms 5
1.4. References 6

2. Algorithm Description 7

2.1. Main Features 7
2.2. Algorithm Parameters 7
2.3. Matching threshold 7
2.4. FNMR 8

3. C API Reference 9

3.1. Overview 9
3.2. Type Definitions 9
3.3. Predefined Constants 9
3.4. Algorithm configuration 9
3.5. Functions 10

4. Use Case 12

4.1. Enrolment 12
4.2. Verification 12

5. Biometric Data 13

5.1. Biometric Data Format 13
5.2. Biometric Data Template 13
5.3. Biometric Information Template (BIT) 13

6. Ordering Information 16

6.1. Contact us 16

1. Introduction

1.1. Purpose

This document describes the API of the fingerprint on-card comparison implementation designed by id3 Technologies.

1.2. Terms and definitions

For the purpose of this document, the following terms and definitions apply.

Terms	Definitions
Algorithm	A sequence of instructions that tell a biometric system how to solve a particular problem. An algorithm will have a finite number of steps and is tipically used by the biometric engine (i.e. the biometric system software) to compute whether a biometric sample and template match.
Biometric data	Data encoding a feature or features used in biometric verification.
Biometric information template	A constructed data objcet in a card containing information needed by the outside world for a verification process, see ISO/IEC 7816-11.
Comparison	The process of comparing a biometric sample with a previously stored reference template or templates.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.
Extraction	The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template; sometimes called "characterization".
Match / Matching	The process of comparing a biometric sample against a previously stored template and scoring the level of similarity.
Minutiae	Friction ridge characteristics that are used to individualize a fingerprint. Minutiae occur at points where a single friction ridge deviates from an uninterrupted flow. Deviation may take the form of ending, bifurcation, or a more complicated "composite" type.
Template / Reference template	Data, which reprensents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples. NOTE – this term is not restricted to mean only data used in any particular recognition method, such as template matching.

1.3. Symbols and abbreviated terms

For the purpose of this specification, the following abbreviations apply.

BDB	Biometric Data Block
BDT	Biometric Data Template
BIT	Biometric Information Template as defined in ISO/IEC 7816-11
CBEFF	Common Biometric Exchange Formats Framework
DO	Data Object
FMR	False Match Rate
FNMR	False Non Match Rate
PIV	Personal Identity Verification
RFU	Reserved for Future Use

1.4. References

Normative References

[1] ISO/IEC 7816-4:2005 – Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange

[2] ISO/IEC 7816-11:2004 – Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods

[3] ISO/IEC 19794-2:2005 – Information technology – Biometric data interchange formats – Part 2: Finger minutiae data

[4] ISO/IEC 19785-1:2006 – Common biometric exchange formats framework – Part 1: Data element specification

[5] ISO/IEC 24787 CD3 – Identification cards – On-card biometric comparison

NIST

[6] NIST Interagency Report 7477 (Revision I) – MINEX II – Performance of Fingerprint Match-On-Card Algorithms Phase II / III Report (http://fingerprint.nist.gov/minexII)

[7] NIST Interagency Report 7485 – MINEX II – Performance of Fingerprint Match-On-Card Algorithms Evaluation Plan (http://fingerprint.nist.gov/minexII/nistir_7485.pdf)

2. Algorithm Description

2.1. Main Features

id3 Fingerprint Match-On-Card is a finger minutiae comparison algorithm specifically designed and optimized for card-based systems.

It presents the following features and benefits:

- Compliant with ISO/IEC 19794-2 compact card format
- PIV-compliant, certified by NIST in MINEX II program (http://fingerprint.nist.gov/minexII)
- High interoperability with most minutiae extractors
- Invariant to translation and tolerant to rotation up to 16°
- Fast comparison time: < 80 ms
- Easy implementation on any target (native code, single source file, no additional library needed)
- Flexible to specific requirements
- Very low resource requirements (3 kB code, 317 bytes data)
- Template size: < 241 bytes

2.2. Algorithm Parameters

The following parameters apply to the biometric comparison algorithm:

- Maximum number of minutiae expected: **80**
- Minimum number of minutiae required: **0**
- Ordering scheme for minutiae: **Ascending Cartesian y-x**

Note 1: If the number of minutiae exceeds the maximum number processible by the comparison algorithm, then truncation is necessary. The use of minutia quality values for removal is highly recommended.

Note 2: The number of minutiae is a security sensitive parameter and depending on the security policy of the application. The recommended minimum number of minutiae for enrolment is 16 and for verification is 12. These values have an impact on the resistance of minutiae-based biometric recognition system against zero-effort imposter attacks.

2.3. Matching threshold

Matching threshold determines FMR (False Match Rate). It defines the probability to accept false fingerprints (impostors). Since FMR and FNMR (False Non-Match Rate) is in inverse proportion to each other, FNMR will increase with higher matching thresholds.

The matching threshold should be selected according to the following table, depending on the required FMR.

False Match Rate	Matching threshold
1 %	2861
0.1 %	4396
0.01 %	5931
0.001 %	7466
0.0001 %	9001

2.4. FNMR

The following table shows the FNMR at a given FMR with a single finger, as measured and reported by NIST in MINEX II testing (see NISTIR7477, Rev 8, page 31, Algorithm F, Column 7).

FMR	3 * 10-2	10-2	3 * 10-3	10-3	3 * 10-4	10-4
FNMR	2.1%	3.1%	4.5%	6%	8%	10.2%

3. C API Reference

3.1. Overview

This section provides the API reference for C programming language.

The code is designed to be compiled seemlessly for any target chip. However, for proper compilation on ST23 smartcard ICs, the '*ST23*' preprocessor symbol shall be defined in the compilation environment.

3.2. Type Definitions

These types are C-definitions used in the native library.

```
typedef unsigned char   int8;          // signed 8-bit integer
typedef unsigned short  int16;         // signed 16-bit integer
typedef unsigned short  int32;         // signed 32-bit integer
typedef unsigned char   uint8;         // unsigned 8-bit integer
typedef unsigned short  uint16;        // unsigned 16-bit integer
typedef unsigned long   uint32;        // unsigned 32-bit integer
```

3.3. Predefined Constants

The following pre-defined constants give information about the MOC algorithm:

Name	Value	Description
ID3MOC_VENDOR_ID	003Fh	Identifier of the owner of the template matcher (value assigned by the IBIA)
ID3MOC_VERSION	0330h	Algorithm version number
ID3MOC_MIN_MINUTIAE	0	Minimum number of minutiae required
ID3MOC_MAX_MINUTIAE	80*	Maximum number of minutiae expected
ID3MOC_MINUTIA_ORDER	00h	Required ordering scheme for minutiae
ID3MOC_TEMPLATE_SIZE	241*	Maximum size (in bytes) of a biometric template encoded using a proprietary format.
ID3MOC_WORKING_BUFFER_SIZE	317*	Required size (in bytes) of the working buffer used for biometric comparison.

* Reducing the number of minutiae allow to lower the required size of the buffers used for biometric comparison. The following formulas apply:

*ID3MOC_TEMPLATE_SIZE = ID3MOC_MAX_MINUTIAE * 3 + 1*

*ID3MOC_WORKING_BUFFER_SIZE = ID3MOC_MAX_MINUTIAE * 3 + 77*

3.4. Algorithm configuration

The following preprocessor symbols, declared into the compilation environment, allow configuring the algorithm:

Symbol Name	Value	Default Value	Description
ST23	Option enabled if defined	Not defined	Use this option for proper compilation on ST23 smartcard ICs in "small memory" model.

3.5. Functions

3.5.1. id3MOC_Prepare

Description

This function prepares a template to a further comparison process. The input biometric template shall comply with the **ISO/IEC 19794-2 Compact Card format** without appended tags and lengths. The output data is encoded in a proprietary format and its length is equal to the length of the input template plus one byte.

```
uint16 id3MOC_Prepare(
         uint8 * isocc_template,
         uint16 template_size,
         uint8 * output_buffer
);
```

Parameters

isocc_template

[in] Points to a buffer in RAM containing the reference biometric data in ISO/IEC 19794-2 compact card format.

template_size

[in] Supplies the length of the input template. Since each minutia is 3 bytes, the minutiae count is given by *template_size* / 3. The value shall be less than or equal to ID3MOC_MAX_MINUTIAE * 3.

output_buffer

[out] Points to a buffer in RAM that receives the prepared template. The output buffer must be at least ID3MOC_TEMPLATE_SIZE bytes long, which is actually the size of the input template plus one byte.

Returns

The size in bytes of the template transformed into the proprietary format, i.e. *template_size + 1* bytes.

Remarks

For memory saving, the output buffer may start at the same address as the input buffer.

3.5.2. id3MOC_Compare

Description

This function performs the comparison between a probe template and a reference template.

```
uint16 id3MOC_Compare(
         uint8 * working_buffer,
         uint8 * reference,
         uint8 * probe
);
```

Parameters

working_buffer

[in] Points to a buffer in RAM used for the comparison process. The required buffer size shall be at least ID3MOC_WORKING_BUFFER_SIZE bytes.

reference

[in] Points to a buffer in RAM that contains the reference template encoded using the proprietary format. Use the id3MOC_Prepare function to prepare the reference template.

probe

[in] Points to a buffer in RAM that contains the probe template encoded using the proprietary format. Use the id3MOC_Prepare function to prepare the probe template.

Returns

A similarity score value as a short integer in the range [0, 32767]. See Matching threshold for details.

Remarks

Prior to a call to this function, the templates must be prepared using the id3MOC_Prepare function.

4. Use Case

This section describes how the library shall be used on a general use case.

4.1. Enrolment

The template to enroll on the card is generally stored via a PUTDATA command APDU. A javacard applet will manage the APDU reception and forward the template in the data field to an interface library. This interface library will perform the following steps:

1. Retrieve the address of the finger minutiae data in the APDU buffer,
2. Call the id3MOC_Prepare function to prepare the reference template,
3. Store the transformed template into static memory (EEPROM, Flash, etc.).

4.2. Verification

The template to be verified (probe template) is generally sent via a VERIFY command APDU. The interface library will perform the following steps:

1. Retrieve the address of the finger minutiae data in the APDU buffer,
2. Call the id3MOC_Prepare function to prepare the probe template,
3. Copy the reference template from static memory (EEPROM, Flash, etc.) to a buffer in RAM,
4. Allocate a buffer in RAM for the matching process,
5. Call the id3MOC_Compare function to perform the biometric comparison,
6. Analyse the output comparison score and make the final decision (match or no match).

5. Biometric Data

5.1. Biometric Data Format

The data presented to the matcher shall comply with the ISO/IEC 19794-2 compact card format.

- coordinate x (8 bits), unit = 10^{-1} mm
- coordinate y (8 bits), unit = 10^{-1} mm
- minutia type t (2 bits):
  - 00 = other,
  - 01 = ridge ending
  - 10 = ridge bifurcation
  - 11 = reserved for future use
- angle θ (6 bits), unit = 2π/64

x-coordinate	y-coordinate	type t	angle θ
1 byte	1 byte	1 byte	

Notes

- The maximum value for the x and y coordinate is 25.5mm with the compact format.
- Minutia (x, y, theta) triples must be unique.
- ISO 19794-2 compact size minutiae format encodes each coordinate on 8 bits, with one unit = 0.1 mm. As a result, fingerprint minutia must fit into an area of 2.55 x 2.55 cm². If the fingerprint scanner has a larger capture window, it is important that the captured coordinates be shifted to the upper left corner to ensure that no coordinates have an absolute value above 255 when transmitted to the card. Coordinate overflow is not authorized and may result in a false rejection. Coordinate overflow is not checked by the on-card matcher.

5.2. Biometric Data Template

Biometric data may be presented to the card as concatenation of DOs within a Biometric Data Template (BDT).

Tag	**Len**	**Value**				
7F2E	Var.	**Biometric data template**				
		Tag	**Len**	**Value**		
		81	Var.	**Finger minutiae data**		
				Field name	**Size (bits)**	**Range**
				coordinate x	8	[0,255]
				coordinate y	8	[0,255]
				minutia type	2	[0,2]
				minutia angle	6	[0,63]

The minimum and maximum numbers of minutiae supported in the Biometric Data Template are provided in the Biometric Information Template (BIT).

NOTE – The id3 match-on-card implementation does not use additional features such as ridge count data, cores or deltas.

5.3. Biometric Information Template (BIT)

The Biometric Information Template (BIT) provides descriptive information regarding the associated biometric data.

Prior to a verification process, the BIT may be retrieved from a card to correctly compute and structure the biometric verification data (ie. number of minutiae, minutiae order, etc.).

5.3.1. Example of BIT

<table>
<tr><th>Tag</th><th>Len</th><th colspan="8">Value</th></tr>
<tr><td rowspan="11">7F60</td><td rowspan="11">Var.</td><td colspan="8">Biometric information template (BIT)</td></tr>
<tr><td>Tag</td><td colspan="2">Len</td><td colspan="5">Value</td></tr>
<tr><td>A1</td><td colspan="2">Var.</td><td colspan="5">Biometric header template (BHT)</td></tr>
<tr><td></td><td></td><td>Tag</td><td>Len</td><td>Value</td><td colspan="3">Description</td></tr>
<tr><td></td><td></td><td>81</td><td>01</td><td>08</td><td colspan="3">Biometric type (08 = fingerprint)</td></tr>
<tr><td></td><td></td><td>82</td><td>01</td><td>xx</td><td colspan="3">Biometric subtype (finger position) - see table below</td></tr>
<tr><td></td><td></td><td>89</td><td>01</td><td>xx</td><td colspan="3">Impression type – see table below</td></tr>
<tr><td></td><td></td><td>87</td><td>02</td><td>0101</td><td colspan="3">CBEFF BDB format owner registered with IBIA (ISO/IEC JTC1/SC37)</td></tr>
<tr><td></td><td></td><td>88</td><td>02</td><td>0005</td><td colspan="3">CBEFF BDB format type registered with IBIA (ISO/IEC 19794-2 Compact Card Format – Table 16)</td></tr>
<tr><td></td><td></td><td rowspan="3">B1</td><td rowspan="3">07</td><td colspan="4">Biometric matching algorithm parameters</td></tr>
<tr><td></td><td></td><td>Tag</td><td>Len</td><td>Value</td><td>Description</td></tr>
<tr><td></td><td></td><td>81</td><td>02</td><td>0050</td><td>Minimum and maximum numbers of minutiae accepted by the on-card matcher. See ISO/IEC 19794-2 (sub-clause 8.3.3 Table 10).</td></tr>
<tr><td></td><td></td><td>82</td><td>1</td><td>09</td><td>Minutiae order (ascending cartesian y-x). See ISO/IEC 19794-2 (sub-clause 8.3.4 Table 11 and 12)</td></tr>
</table>

5.3.2. Biometric subtype (finger position)

Biometric subtype (finger position) as per ISO/IEC 19785:

Hex value	Finger position
'00'	No information given
'05'	Right thumb
'09'	Right index
'0D'	Right middle
'11'	Right ring
'15'	Right little
'06'	Left thumb
'0A'	Left index
'0E'	Left middle
'12'	Left ring
'16'	Left little

5.3.3. Finger Impression Type

Impression type is used to prevent a false rejection with the on-card matcher when the enrolment template and the verification template have been captured using different types of sensor (e.g. flat scanner vs. swipe) because of associated distortions during fingerprint scanning. In such case, the same finger can be enrolled multiple times, once with each sensor and the on-card matcher shall perform the match of the verification template only with the enrolled template of the same type.

Hex value	Impression type
'00'	Live-scan plain
'01'	Live-scan rolled
'08'	Swipe

6. Ordering Information

6.1. Contact us

id3 Technologies
5, rue de la Verrerie
38120 Le Fontanil-Cornillon
FRANCE

Tel: +33 (0)4 76 75 75 85
Fax: +33 (0)4 76 75 52 30
Internet: http://www.id3.eu
Contact: contact@id3.eu