INTERNATIONAL STANDARD

ISO/IEC 18584

First edition
2015-11-15

Information technology — Identification cards — Conformance test requirements for on-card biometric comparison applications

Technologies de l'information — Cartes d'identification — Exigences relatives aux essais de conformité pour les applications de comparaison biométrique sur carte

Reference number
ISO/IEC 18584:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

Introduction

On-card biometric comparison provides a more secure biometric authentication in that the comparison is executed inside the ICC and the biometric reference is never be revealed outside the ICC. ISO/IEC 24787:2010 specifies a set of requirements for implementing biometric comparison inside the ICC. An ICC application that is claimed to be conformant to ISO/IEC 24787:2010, should fulfil a set of requirements that are stated in this International Standard. The requirements established are for both, the ICCs that fully process the on-card biometric comparison, and those using the work-sharing mechanism, as specified in ISO/IEC 24787:2010.

Information technology — Identification cards — Conformance test requirements for on-card biometric comparison applications

1 Scope

This International Standard establishes

— conformance test requirements for using general framework for on-card comparison applications,

— conformance test requirements for using work-sharing mechanism for on-card comparison applications, and

— conformance test requirements to check accomplishment of security policies for on-card biometric comparison that are specified in ISO/IEC 24787:2010.

This International Standard only covers the testing of APDU command and response pairs involved for the ICC that has the capability to perform on-card biometric comparison based on ISO/IEC 24787:2010.

Measuring the performance of on-card biometric comparison algorithms in terms of error rates is not within the scope of this International Standard.

2 Normative references

ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 7816-15, *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*

ISO/IEC 19785-1, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-2, *Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority*

ISO/IEC 19785-3:2007, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19794 (all parts), *Information technology — Biometric data interchange formats*

ISO/IEC 24761:2009, *Information technology — Security techniques — Authentication context for biometrics*

ISO/IEC 24787:2010, *Information technology — Identification cards — On-card biometric comparison*

ISO/IEC 29794-1:2009, *Information technology — Biometric sample quality — Part 1: Framework*

3 Terms and definitions

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

3.1
auxiliary data
data that is dependent on biometric modality and related to the biometric reference but does not include the biometric reference or a biometric sample

EXAMPLE Data such as orientation, scaling, etc.

3.2
biometric (adj.)
of or having to do with biometrics

Note 1 to entry: "biometric" should never be used as a noun.

Note 2 to entry: This definition is derived from SC37 SD2 *Harmonized biometric vocabulary*.

3.3
biometrics
automated recognition of individuals based on their behavioral and biological characteristics

Note 1 to entry: This definition is derived from SC37 SD2 *Harmonized biometric vocabulary*.

3.4
biometric claim
claim that a biometric capture subject is the bodily source of a specified biometric reference

3.5
biometric data
biometric sample or aggregations of biometric samples at any stage of processing, biometric reference, biometric feature or biometric property

Note 1 to entry: This definition is derived from SC37 SD2 *Harmonized biometric vocabulary*.

3.6
biometric data format
structure for representing biometric data

3.7
biometric Information Template
descriptive information regarding the associated biometric data

Note 1 to entry: This definition is derived from ISO/IEC 7816-11:2004.

3.8
biometric product identifier
unique identifier registered with the registration authority in accordance with ISO/IEC 19785-1

3.9
biometric property
descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means

Note 1 to entry: This definition is derived from SC37 SD2 *Harmonized biometric vocabulary*.

3.10
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison

Note 1 to entry: This definition is derived from SC37 SD2 *Harmonized biometric vocabulary*.

3.11
biometric verification system
system that aims to perform the process of confirming a biometric claim

3.12
client application
software executed in the biometric sample acquisition terminal to process a request for comparison that uses the decision obtained from the on-card comparison process

3.13
installation
writing of the required parameters into the non-volatile memory inside the ICC by the card OS executing the installation procedure after the application has been uploaded to the ICC

3.14
integrated circuit(s) cards interface devices
requirements and specifications for USB devices that interface with Integrated Circuit(s) Cards or act as interfaces with Integrated Circuit(s) Cards

Note 1 to entry: This definition is derived from USB Implementers Forum.

3.15
on-card comparison
performing comparison and decision making on an IC card where the biometric reference data is retained on-card in order to enhance security and privacy

3.16
off-card comparison
biometric comparison performed outside the card by the biometric verification system against the biometric reference data stored on the card

3.17
pre-comparison computation
computation procedure executed outside the ICC that requires the (open) on-card auxiliary data to compute meta-data that can be used to speed up the subsequent on-card biometric data comparison process

3.18
work-sharing
splitting the work load of computation of the pre-comparison process between the card and the biometric interfacing device

Note 1 to entry: Work-sharing on-card comparison is one type of on-card comparison.

3.19
system-on-card
complete biometric verification system on a card, including data acquisition, processing and comparison

Note 1 to entry: System-on-card comparison is one type of on-card comparison

3.20
zeroize data
electronically stored data that have been degaussed, erased, or over-written device

Note 1 to entry: This definition is derived from ANSI X9.17 *Financial Institution Key Management (Wholesale)*.

4 Abbreviated terms

AID	application identifier
ADF	application dedicated file
APDU	application protocol data unit
API	application programme interface
AUT	authenticate
BER	basic encoding rules
BIT	biometric information template
CCID	Integrated Circuit(s) Cards Interface Devices
CRT	control reference template
CPU	central processing unit
DF	dedicated file
DF.CIA	dedicated file, cryptographic information application
EF	elementary file
FCI	file control information
FCP	file control parameter
FMR	false match rate
FNMR	false non-match rate
ICC	integrated circuit card
IFD	interface device
MAC	message authentication code
MSE	manage security environment
OID	object Identifier
OS	operating system
RFU	reserved for future use
SW1-SW2	status bytes
TLV	tag length value
UQ	usage qualifier
USB	Universal Serial Bus
WSCP	work-sharing computation protocol
WSR	work-sharing request

5 Test Methodology

5.1 Test assertion

Test assertion is a function to check a given parameter whether can meet the requirement of specification. If the parameter cannot satisfy the criteria of the original specification, the assertion function shall return a negative condition (e.g. Boolean false) indicating "assertion failed" with specific error message. Otherwise, the assertion function shall return a positive condition (e.g. Boolean true) and continue to test for the next criteria. All test results shall be consolidated to generate a report to notify the outcome of the test.

5.2 Test criteria

If the item under test is specified as mandatory, this item under test shall be present as per specification. Two levels of test criteria for the content/value are defined in the document for testing:

— Level 1: The content/value can be tested by following the requirement from the manufacturer.

— Level 2: The content/value shall be tested by following the test requirement/method specified in this document.

6 Conformance test requirements related to data for on-card comparison

6.1 Biometric reference object handling

For testing 7.1.2 biometric reference object handling, the conformance test requirements of relevant part of ISO/IEC 19794- series shall be used to test the biometric data format, unless proprietary biometric data format is explicitly not required for particular operation environment.

6.2 Configuration data (biometric verification)

6.2.1 Data objects for configuration data elements

If configuration data are available and the access rule associated with logical data structures allows retrieval of configuration, the test requirements as shown in Table 1 shall be used.

Table 1 — Test requirements for data objects for configuration data elements

Tag	Length	Valid values	Test Requirement	Mandatory	Test Level	Test result
'80'	1 to 3 bytes	NA	* Maximum size of biometric verification data.	Yes	1	
'81'	1 to 3 bytes	NA	* Minimum size of the biometric reference data.	Yes	1	
'82'	1	'00'-'FF'	* Supported number of biometric templates ('00' – no information given)	Yes	1	
'83'	1	'00'-'FF'	* Flag indicating the possibility of re-enrolment. Only two values: '00': No re-enrolment possible and '01':Re-enrolment possible are allowed, all other values are reserved for future use and shall never be used.	Yes	2	
NOTE 1 "*" denotes that this tag shall be present. The value is provided by manufacturer of the ICC under test.						

Table 1 *(continued)*

Tag	Length	Valid values	Test Requirement	Mandatory	Test Level	Test result
'85'	Var	As defined in ISO/IEC 29794-1	Minimum verification data quality supported as defined in the relevant parts of the ISO/IEC 19794 and ISO/IEC 29794- series of standards.	Yes	2	
'86'	1	NA	* Initial value of the retry counter, indicating the supported maximum number of permitted verification attempts.	Yes	1	
'87'	Var	NA	Internal quality restrictions for performing the comparison. The value is depends on particular application.	Yes	1	
'8F'	Var	NA	Proprietary data, application dependent.	No.	1	
'90'	Var	As per Table 3 in ISO/IEC 24787:2010	See Table 3 below	Yes	2	
'A4'	Var	As defined by the registration authority described in ISO/IEC 19785-2	Reserve for future use, Algorithm ID as defined by SC 37.	No	1	
NOTE 1 "*" denotes that this tag shall be present. The value is provided by manufacturer of the ICC under test.						

6.2.2 Biometric comparison algorithm parameters

The requirements for testing data objects to be read from the card encoded in BIT are shown in Table 2.

Table 2 — Test requirements for Data objects for biometric comparison algorithm parameters

Tag	Length	Valid values	Test Requirement	Mandatory	Test Level	Test result
'81'	*	*	Minimum and maximum length of biometric data as defined in the relevant part of the ISO/IEC 19794- series of standards. The content shall follow the relevant part of ISO/IEC 19794- series of standards.	Yes	2	
'82'	*	*	Ordering, if applicable, of the features in the biometric data as defined in the relevant part of the ISO/IEC 19794- series of standards. The content shall follow the relevant part of ISO/IEC 19794- series of standards.	Yes	2	
'83'	*	*	Biometric data handling information as defined in the relevant part of the ISO/IEC 19794- series of standards. The content shall follow the relevant part of ISO/IEC 19794- series of standards.	Yes	2	
NOTE 1 "*" denotes that this variable is defined in the relevant part of ISO/IEC 19794- series of standards. NOTE 2 "**" denotes that this variable is defined in the relevant parts of the ISO/IEC 19794 and ISO/IEC 29794- series of standards.						

Table 2 *(continued)*

Tag	Length	Valid values	Test Requirement	Mandatory	Test Level	Test result
'84'	*	*	Alignment information as defined in the relevant part of the ISO/IEC 19794- series of standards. The content shall follow the relevant part of ISO/IEC 19794- series of standards.	Yes	2	
'85'	**	**	Minimum verification data quality supported (See Table 1). The content shall follow the relevant part of ISO/IEC 19794 and ISO/IEC 29794- series of standards.	Yes	2	
'90'	1	As per Table 3 in ISO/ IEC 24787:2010	See Table 3 below	Yes	2	
'91'	2	'0001' – 'FFFF'	Maximum response time in milli-seconds. A card performing a time-consuming operation has to support proper waiting time extensions according to ISO/ IEC 7816-3.	Yes	2	

NOTE 1 "*" denotes that this variable is defined in the relevant part of ISO/IEC 19794- series of standards.

NOTE 2 "**" denotes that this variable is defined in the relevant parts of the ISO/IEC 19794 and ISO/IEC 29794- series of standards.

The test requirement of authentication and descriptive power as specified in Table 1 and 2 shall follow Table 3.

Table 3 — Authentication type and discriminative power

b7	b6	b5	b4	b3	b2	b1	b0	Meaning	Requirements	Test Level	Test result
						x	x	Authentication type			
						0	0	Comparison on-card	* Shall be the same as specified by the manufacturer	2	
						0	1	Work sharing comparison on-card	* Shall be the same as specified by the manufacturer	2	
						1	0	System-on-card	* Shall be the same as specified by the manufacturer	2	
						1	1	RFU	Shall never be used.		
			x	x	x			FMR claimed			
			0	0	0			No indication given			
			0	0	1			FMR grade 1 (largest)	** shall be the same as specified by manufacturer	2	

NOTE 1 "*" denotes that these bits shall represent the same operation as specified by manufacturer. For example, for comparison on-card, 'b1' = 0 and 'b0' = 1 shall be found.

NOTE 2 "**" denotes that these bits shall represent the same descriptive power as specified by manufacturer.

Table 3 *(continued)*

b7	b6	b5	b4	b3	b2	b1	b0	Meaning	Requirements	Test Level	Test result
			0	1	0			FMR grade 2	** shall be the same as specified by manufacturer	2	
			0	1	1			FMR grade 3	** shall be the same as specified by manufacturer	2	
			1	0	0			FMR grade 4	** shall be the same as specified by manufacturer	2	
			1	0	1			FMR grade 5	** shall be the same as specified by manufacturer	2	
			1	1	0			FMR grade 6 (smallest)	** shall be the same as specified by manufacturer	2	
			1	1	1			RFU	Shall never be used.		
x	x	x						RFU	Shall never be used. These bits may be set to zero.	1	

NOTE 1 "*" denotes that these bits shall represent the same operation as specified by manufacturer. For example, for comparison on-card, 'b1' = 0 and 'b0' = 1 shall be found.

NOTE 2 "**" denotes that these bits shall represent the same descriptive power as specified by manufacturer.

6.2.3 Biometric product identifier

Biometric product identifier shall be an integer within the range 1 to 65535 and should be registered with the registration authority according to ISO/IEC 19785-1. '0' shall never be used as identifier.

6.3 Sharable Interface for multiple applications

6.3.1 File control parameter

The file control parameter (FCP) shall be tested according to ISO/IEC 7816-4.

6.3.2 Access rules

Access rules shall be tested according to ISO/IEC 7816-4.

6.4 Retry counter management

The following Table 4 shall be used to test the retry counter management.

Table 4 — Checklist for retry counter management

List	Test Requirement	Mandatory	Test Level	Test result
1	The cardholder of biometric comparison process shall be under the control of a retry counter which determines if the verification process may continue to be used with a given biometric reference.	Yes	2	
2	An initial value of the retry counter shall be associated to the on-card biometric reference.	Yes	2	
3	This association may be encoded using ISO/IEC 7816-15 sub-class attributes assigned to a Biometric Data Info Object as defined in ISO/IEC 7816-15.	No	2	
4	If the verification fails, the retry counter shall be decremented by one and an error status that contains the remaining attempts shall be returned by the application.	Yes	2	
5	The number of allowed retries may be encoded in the status bytes SW1-SW2 = "63CX" (where X is the remaining number) of a response to a VERIFY command where the data field is absent according to ISO/IEC 7816-4.	No	1	
6	A successful verification of the biometrics reference shall reset the associated retry counter to its initial value.	Yes	2	

7 Conformance test requirements for standard processes for on-card biometric comparison

7.1 Standard Processes

7.1.1 Application identifier (AID) for on-card biometric comparison

If biometric comparison is implemented as an independent application, the application identifier shall be generated as per ISO/IEC 7816-4:2013, 8.2.1.2 and Annex A.

NOTE 1 The AID is derived from the standard's object identifier according to ISO/IEC 7816-4:2013, 8.2.1.2 and Annex A.

7.1.2 Read biometric reference data

This operation shall never be supported, no matter using specific APDU command or reading from file.

7.1.3 Enrolment

This operation shall be supported. The biometric terminal shall be able to store biometric reference into the ICC using the mechanism specified in ISO/IEC 7816-11. Test verification can be used to verify the biometric reference is correctly stored inside the ICC.

7.1.4 Verification

This operation shall be supported. The biometric terminal shall be able to send biometric data to the ICC using the mechanism specified in ISO/IEC 7816-11. The returned bytes shall not contain the biometric comparison score.

7.1.5 Termination of on-card comparison application

The on-card logical data structure containing biometric reference data pertaining only to such application shall be made inaccessible and the data may be "zeroize" inside the card.

7.2 Comparison process and result output

7.2.1 Comparison process and result

The comparison process shall take place within the card. The follow checklist shall be used for testing:

a) Test vectors of positive and negative verifications shall be used for testing.

b) If the comparison result of a biometric data are successful, the SW1 and SW2 in the VERIFY response APDU shall be '90 00'.

c) Otherwise, SW1-SW2 shall comply with ISO/IEC 7816 error codes.

8 Conformance test requirements for work-sharing mechanism using WSR protocol

8.1 Biometric reference for work-sharing mechanism

In work-sharing mechanism, the biometric data which is stored during enrolment can be divided into two portions: secured portion and open portion. The secured portion, which is a biometric reference, shall not be sent out to the biometric verification system/IFD. The auxiliary data (open) portion, which contains the biometric property, can be sent out using WSR protocol for processing by biometric interfacing device to speed up the processing time. The secured portion and auxiliary data (open) portion shall be encoded inside the BIT as mandated portion and proprietary portion respectively as per respective part of ISO/IEC 19794-2 and ISO/IEC 7816-11. See Annex A for the checklist to verify the biometric data template for work-sharing mechanism.

8.2 Command and response bytes for work-sharing

In order to support work-sharing using WSR protocol, the ICC shall support the APDU commands and responses which are specified in ISO/IEC 7816-4:2005, 8.6 "Card-originated byte strings". The following checklist in Table 5 shall be used to check whether the ICC has the capability to perform WSR operation.

Table 5 — Checklist a for WSR protocol

List	Test Requirement	Mandatory	Test Level	Test result
1	The ICC shall support "Card-originated byte strings" as per ISO/IEC 7816-4:2005, 8.6.	Yes	2	
2	The ICC shall support VERIFY command as per ISO/IEC 7816-11:2004, 5.2	Yes	2	
3	The ICC shall support '62/64 XX' response bytes to initiate work-sharing as per ISO/IEC 7816-4:2005, 5.1.3.	Yes	2	
4	The IFD shall recognize the response byte '62/64 XX' as initiation of work-sharing as per ISO/IEC 7816-4:2005, 5.1.3.	Yes	2	
5	The IFD shall support GET DATA command (00 CB 00 00 XX) to retrieve the intermediate data/open template from the ICC for work-sharing computation as per ISO/IEC 7816-4:2005, 7.4.2.	Yes	2	
6	The IFD shall support PUT DATA command (00 DB 00 00 YY...) to send back the computed intermediate data to the ICC as per ISO/IEC 7816-4:2005, 7.4.3.	Yes	2	
7	Upon receiving the PUT DATA command and intermediate data from the IFD, the ICC shall be able to continue the execution of biometric comparison as per ISO/IEC 7816-4:2005, 7.4.3.	Yes	2	
8	Upon the situation where additional WSR operations are required, the ICC shall be able to initiate extra WSR procedures.	Yes	2	
9	Upon completion of biometric comparison, if the comparison result of a biometric data are successful, the SW1 and SW2 in the VERIFY response APDU shall be '90 00'. Otherwise, SW1-SW2 shall comply with ISO/IEC 7816 error codes.	Yes	2	
10	Use test vectors to check for both positive and negative verifications of given biometrics.	Yes	2	

8.3 Work-sharing management

This cause shall be used for testing ICC that supports the work-sharing procedure discover.

8.3.1 Unique Identifier

If the ICC supports work-sharing management, a unique object identifier shall be used to let the biometric verification system accept the WSR request during biometric comparison process. The following 8.3.2 and 8.3.3 shall be used to check the work-sharing management.

8.3.2 Work-sharing procedure discovery

To discover the existence of WSR capability inside an ICC using a unique object ID, the IFD shall read the information from a DIR file or to retrieve using a standard GET DATA. The following test criterion shall be used to check the capability of discovery mechanism:

1. The card shall return object identifier in the constructed version of the proprietary data (tag '73') within the application template (tag '61') to be read in a DIR file or recovered by a standard GET DATA:

OID: '00' 'CB' '2F' '00' '02' '5C' '00' '00'

8.3.3 Work-sharing procedure operation

Selecting a protocol WSR protocol inside the ICC may be supported by manufacturer. For selecting a WSR protocol compliant with 8.1 specified in ISO/IEC 24787, the IFD shall send an odd ENVELOP command encapsulating the object identifier of the WSR protocol to the ICC. The checklist in Table 6 shall be used for testing.

Table 6 — Checklist a for Work-sharing procedure operation

List	Test Requirement	Mandatory	Test Level	Test result
1	The ICC shall support odd ENVELOPE command as specified in ISO/IEC 7816-4. (e.g. '00' 'C3' '00' '00' < Lc > '06' < Lc-2 > < object identifier of the WSR protocol of the ICC under test >)	Yes	2	
2	If the object ID specified in the ENVELOPE command matches with the object ID registered inside the card, the card shall return normal operation '90' '00' response bytes. Upon receiving normal operation, the corresponding WSR protocol as specified by the object ID shall be selected inside the ICC. The above 8.2 shall be applied to test the operation of WSR protocol.	Yes	2	
3	If the object ID specified in the ENVELOPE command does not match with the object ID registered inside the card, the ICC card shall return response bytes SW1-SW2 from the ICC shall comply with ISO/IEC 7816 error codes.	Yes	2	

9 Conformance test requirements s for security policies for on-card biometric comparison

9.1 Common security policies (CSP) for on-card biometric comparison

In all cases, the common security policies which are the minimum security policies shall apply. The following checklist shall be used for testing.

Table 7 — Checklist for Work-sharing procedure operation

List	Test Requirement	Mandatory	Test Level	Test result
1	No application shall be allowed to send the biometric reference outside the ICC. (see ISO/IEC 24787:2010, 7.2.2).	Yes	2	
2	The policies specified in ISO/IEC 24787:2010, 7.1.5 shall be used to implement the retry counter mechanism.	Yes	2	
3	A secure messaging shall be established prior to any of the operations related to the biometric reference (enrolment, re-enrolment and verification) (see ISO/IEC 7816-4).	Yes	2	
4	All data exchanged regarding the on-card biometric comparison shall be authenticated for its integrity.	Yes	2	
5	All Biometric data to be exchanged between the card and the IFD shall be enciphered (see ISO/IEC 24761:2009).	Yes	2	
6	The unblocking process for the on-card biometric comparison shall "zeroise" the biometric reference in the ICC, and request for a new enrolment.	No	1	
NOTE	All the clauses mentioned in Table 10 are specified in ISO/IEC 24787:2010.			

9.2 Security policies (SP1) for global comparison configuration data

For those applications where the biometric reference is to be used as a global verification mechanism, there is no need to establish a double indirection for determining a comparison configuration. Table 8 shall be used to check the security policies SP1.

Table 8 — Checklist for SP1 – global configuration data

List	Test Requirement	Mandatory	Test Level	Test result
1	For cards with multiple applications with on-card biometric comparisons using the same biometric reference, if any application using the biometric reference is a high security application, a unique threshold should be used by all applications and a single retry counter associated to the biometric reference shall be used (see 7.2.8 in ISO/IEC 24787:2010, bullet a).	Yes	2	
2	All configuration data are linked to the biometric reference. In particular:			
	— The verification threshold	Yes	2	
	— The maximum amount of verification retries	Yes	2	
	— The retry counter	Yes	2	
	— All parameters for the comparison algorithm	Yes	2	
3	None of the applications using the on-card biometric comparison mechanism with such biometric reference can change the configuration data independently	Yes	2	
4	When the retry counter reaches zero, the on-card biometric comparison mechanism is blocked, and therefore all applications using such biometric reference for verification will not be able to execute those operations protected by the on-card biometric comparison.	Yes	2	
5	A successful verification of the biometrics reference resets the associated retry counter to its initial value, no matter which of the applications have carried out the successful verification.	Yes	2	

9.3 Security policies (SP2) for local comparison configuration data

In the case of a card whose applications request an independent control of the on-card biometric comparison, but shares the same biometric reference, Table 9 shall be used for testing security policies SP2.