INTERNATIONAL STANDARD

ISO/IEC 24787

Second edition
2018-10

Information technology — Identification cards — On-card biometric comparison

Technologies de l'information — Identification des cartes — Comparaison biométrique sur cartes

Reference number
ISO/IEC 24787:2018(E)

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

Published in Switzerland

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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. This document was prepared by ISO/IEC JTC 1, *Information technology*, SC 17, *Cards and security devices for personal identification*.

This second edition cancels and replaces the first edition (ISO/IEC 24787:2010), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 24787:2010/Cor 1:2013.

The main changes compared to the previous edition are as follows:

— Clause 7 has been restructured; the subclauses have been relocated within the clause:

  — in 7.3.3 (previously 7.1.3), configuration data elements and biometric comparison algorithm parameters have been replaced with biometric functionality information and biometric comparison parameters respectively. Refer to 7.3.3.2 and 7.3.3.3 for more information;

  — in 7.3.4 (previously 7.1.4), the implementation of one biometric reference for multiple applications has been updated. Refer to Annex B for an example of the updated implementation;

— Clause 8 (previously Annex B) has been moved from a normative annex into the main body of the document;

— Clause 9 (previously Clause 8) has been replaced with an outline of the overall work-sharing process;

— previous Annexes A, D, F and H have been removed.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

On-card biometric comparison provides a more secure biometric verification method than one where a biometric comparison is carried outside a secure cryptographic device. Storing biometric reference data in a secure ICC means that the reference is not available at any external interface once it has been stored in the ICC, mitigating the risk of extraction and misuse by an unauthorised party.

ISO/IEC 7816-11 and ISO/IEC 19785-3 cover technologies for off-card and simple on-card biometric comparison. ISO/IEC 17839 covers biometric system-on-card.

This document provides requirements for a biometric comparison methodology suitable for the on-card environment. It also covers the on-card comparison work-sharing techniques that require an intensity exceeding the capabilities of ICCs.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning work-sharing given in Clause 9.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right. The holder of this patent right has assured ISO and IEC that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Exploit Technologies Pte Ltd.,
30 Biopolis Street,
#09-02 matrix,
Singapore 138671

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Information technology — Identification cards — On-card biometric comparison

1 Scope

This document establishes

— architectures of biometric comparison using an ICC,

— on-card biometric comparison, both in sensor-off-card systems and as part of biometric system-on-card,

— work-sharing on-card biometric comparison, and

— security policies for on-card biometric comparison.

This document does not establish

— requirements for off-card biometric comparison,

— requirements for biometric system-on-card (as defined in ISO/IEC 17839), or

— modality-specific requirements for storage and comparison.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

ISO/IEC 19785-3, *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, *Information technology — Security techniques — Authentication context for biometrics*

ISO/IEC 29794 (all parts), *Information technology — Biometric sample quality*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
action
action taken according to the results of the biometric *decision* (3.10)

EXAMPLE In the case of on-card biometric comparison, a change in the security status.

3.2
biometric auxiliary data
data that is dependent on the biometric modality and related to the *biometric reference* (3.7) but does not include the *biometric reference* (3.7) or a biometric sample

EXAMPLE Data such as orientation, scaling, etc.

3.3
biometric comparison parameters
application-level on-card comparison parameters associated with the appropriate enrolled *biometric reference* (3.7)

3.4
biometric data format
structure for representing the biometric data

3.5
biometric functionality information
read-only ICC biometric functionality capability information specified by the provider of the ICC operating system with on-card comparison

3.6
biometric information template
descriptive information regarding the associated biometric data

3.7
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison

Note 1 to entry: A biometric reference is a set of features extracted from the biometric samples during enrolment. This is completely different from the concept of 'template' by the smartcard industry and standards (see ISO/IEC 7816-4), which is a defined structure of the value field of a constructed data object.

[SOURCE: ISO/IEC 2382-37:2017, 3.3.16, modified — The EXAMPLE and Notes to entry of SOURCE has been replaced by the above Note 1 to entry.]

3.8
biometric system-on-card
card-sized device including biometric acquisition, data processing, storage, comparison and *decision* (3.10) to compose a complete *biometric verification* (3.9) system

3.9
biometric verification
process of confirming a biometric claim through biometric comparison

Note 1 to entry: The result of a biometric verification is taken by the ICC in order to make the final *decision* (3.10).

[SOURCE: ISO/IEC 2382-37:2017, 3.8.3, modified — The Note 1 to entry has been replaced.]

3.10
decision
process to compare a similarity score to a predefined threshold to decide whether the biometric claim is from the genuine cardholder or an imposter

3.11
signal processing
image processing
process to extract distinctive biometric properties from a given image or signal

3.12
on-card biometric comparison
comparison and decision making on an ICC where the *biometric reference* (3.7) is retained on-card in order to enhance security and privacy

3.13
off-card biometric comparison
biometric comparison performed outside the ICC by the *biometric verification* (3.9) system against the *biometric reference* (3.7) stored on the ICC

3.14
work-sharing
splitting the computational workload of the comparison process between the ICC and the IFD

3.15
sensor-off-card
sensor located on the IFD outside of an ICC

4 Abbreviated terms

AID	application identifier
APDU	application protocol data unit
BER	basic encoding rules
BHT	biometric header template
CBEFF	common biometric exchange format framework
DF	dedicated file
EF	elementary file
FCI	file control information
FMR	false match rate
ICC	integrated circuit card
IFD	interface device
MAC	message authentication code
PBO	PERFORM BIOMETRIC OPERATION
RFU	reserved for future use
SW1-SW2	status bytes
TLV	tag length value

5 Conformance

a) An on-card biometric comparison system claiming conformance to this document shall be personalized with three sets of data:

   1) biometric reference, as described in 7.3.2;

   2) biometric functionality information, as described in 7.3.3.2;

   3) biometric comparison parameters, as described in 7.3.3.3.

b) Support one biometric reference for multiple applications, as described in 7.3.4.

c) Support retry counter management, as described in 8.2.3.

d) Comply with the requirements set forth in 7.4 to 7.6 for on-card biometric comparison implementations.

e) Comply with the requirements set forth in Clause 9 for work-sharing implementations.

Biometric verification can coexist with other authentication mechanisms, such as PIN. The rules for such coexistence shall comply with ISO/IEC 7816-4.

The handling of biometric data shall comply with ISO/IEC 7816-4 and ISO/IEC 7816-11.

The encoding of biometric data shall comply with ISO/IEC 19785-3 and ISO/IEC 7816-11.

6 Architecture of biometric comparison using an ICC

6.1 General

The following subclauses define four architectures of biometric comparison using an ICC or an ICC with a biometric verification system. This document only specifies the requirements for architectures mentioned in 6.3 and 6.4.

While off-card biometric comparison is out of scope for this document, the information in 6.2 is presented to enhance the understanding of the relationship between on-card biometric comparison methods covered in this document and off-card biometric comparison methods.

The biometric reference is stored in an ICC prior to the biometric verification execution.

6.2 Off-card biometric comparison

Off-card biometric comparison means the biometric verification is performed on the off-card biometric verification system. The ICC acts as a storage device to store the biometric reference(s) of the cardholder. The process is schematically represented in Figure 1.

The biometric verification system captures a biometric sample for comparison with a biometric reference retrieved from an ICC. The biometric verification system changes its security status based on the result of biometric comparison to perform subsequent transactions.

EXAMPLE Consider an automated border control system. A facial image (biometric reference) is stored in an electronic machine readable travel document (eMRTD). An eMRTD is a passport with an embedded contactless IC as an ICC. When this eMRTD is presented to an automated border control system, mutual authentication is executed between the system and the e-passport. Then the stored facial image (biometric reference) is retrieved from the e-passport and facial image recognition (biometric comparison) is executed by the system. When the comparison is successful (the e-passport holder is verified), the system allows the passage of the e-passport holder.

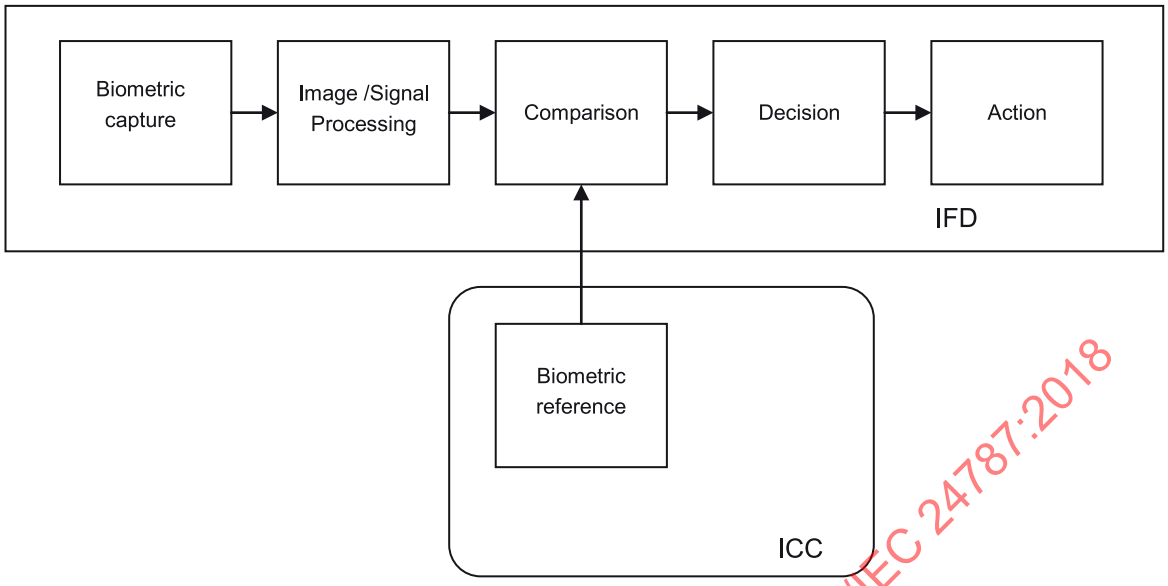

Figure 1 — General architecture for biometric verification using off-card biometric comparison

6.3 On-card biometric comparison (sensor-off-card)

On-card biometric comparison means the biometric verification is performed in the ICC having enough processing power. The process is schematically represented in Figure 2. The capturing of the biometric sample takes place outside the ICC. The enrolment process is the same as or similar to that for off-card comparison.

It is recommended to transfer the biometric data into the ICC using secure messaging (see ISO/IEC 7816-4) between the biometric verification system and the ICC.

NOTE Annex C provides examples of how to implement on-card biometric comparison methods related to the security status of the ICC. Annex D provides information on how security relationships can be implemented in an on-card biometric comparison solution.

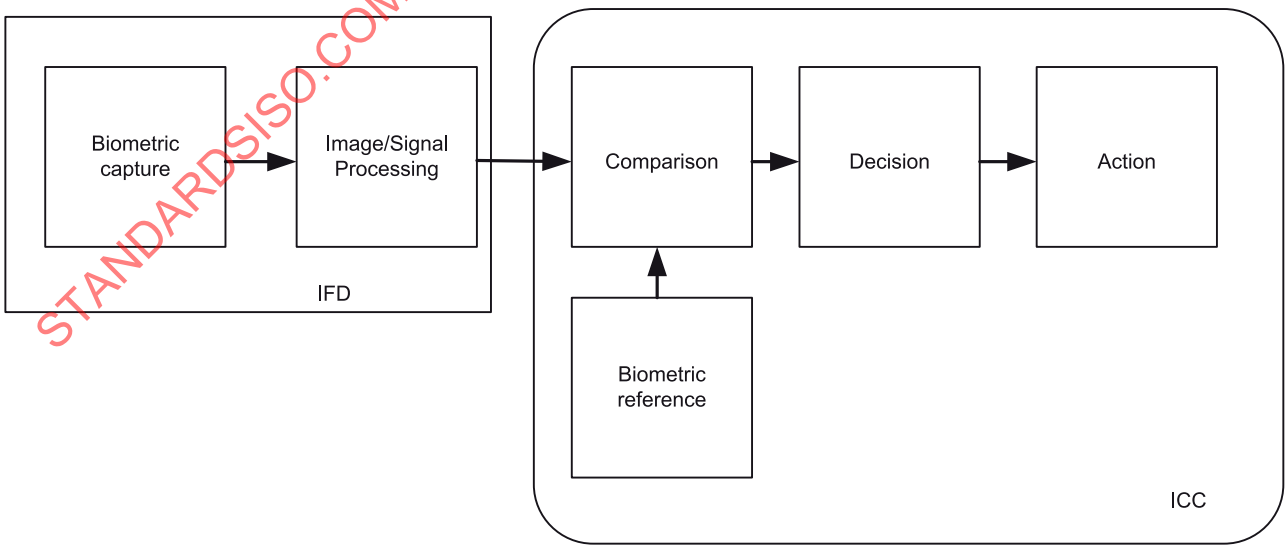

Figure 2 — General architecture for biometric verification using on-card biometric comparison

NOTE Actions taken by the IFD based on the result of biometric on-card comparison within the ICC are not within the scope of this document.

6.4 Work-sharing on-card biometric comparison

Work-sharing on-card biometric comparison is similar to on-card biometric comparison except that the comparison process is assisted by external processing. This type of comparison may be used by an ICC that does not have sufficient processing capability (e.g. long processing time) to execute the entire biometric data comparison.

This comparison process is divided into several sub-processes which are executed in an IFD and on an ICC as presented in Figure 3. Biometric auxiliary data is stored in an ICC and a biometric reference is stored in the different portion on the ICC. The biometric auxiliary data can be retrieved from an ICC while the biometric reference cannot. The biometric auxiliary data, which contains the biometric property, is provided for accelerating the biometric comparison.

The outline procedure for work-sharing on-card biometric comparison is:

— before the biometric comparison procedure is started, a biometric verification system on an IFD captures a biometric sample from a cardholder;

— before the biometric comparison procedure, the biometric auxiliary data is retrieved from an ICC;

— a biometric verification system on an IFD starts the first process of the biometric comparison procedure and then triggers the execution of subsequent processes in a daisy chain manner;

— the final process of the biometric comparison procedure is executed on an ICC;

— after the final process of the biometric comparison procedure is done, subsequent processes, such as decision and action, are then executed.

Further details of biometric auxiliary data depend on biometrics modality and are not specified in this document.

NOTE Annex C provides examples of how to implement on-card biometric comparison methods related to the security status of the ICC. Annex D provides information on how security relationships can be implemented in an on-card biometric comparison solution.

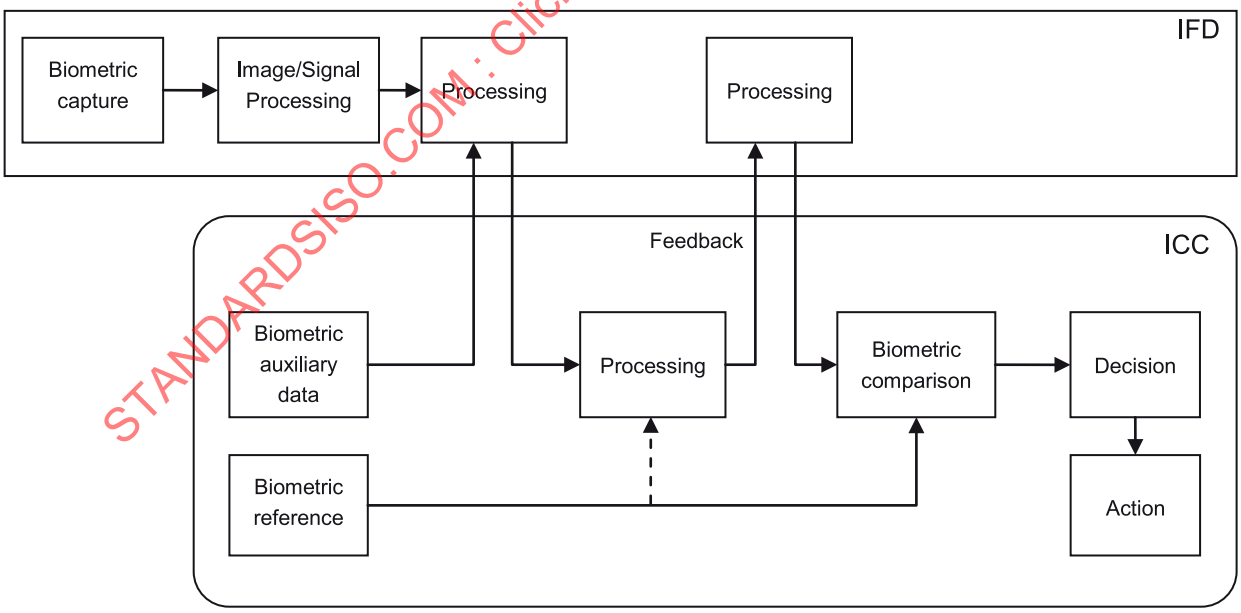

Figure 3 — Example of architecture for work-sharing on-card biometric comparison

6.5 Biometric system-on-card

Biometric system-on-card means that the whole biometric verification process from biometric sample capturing to action is performed on an ICC. The process is schematically represented in Figure 4.

ISO/IEC 17839 specifies details of biometric system-on-card.

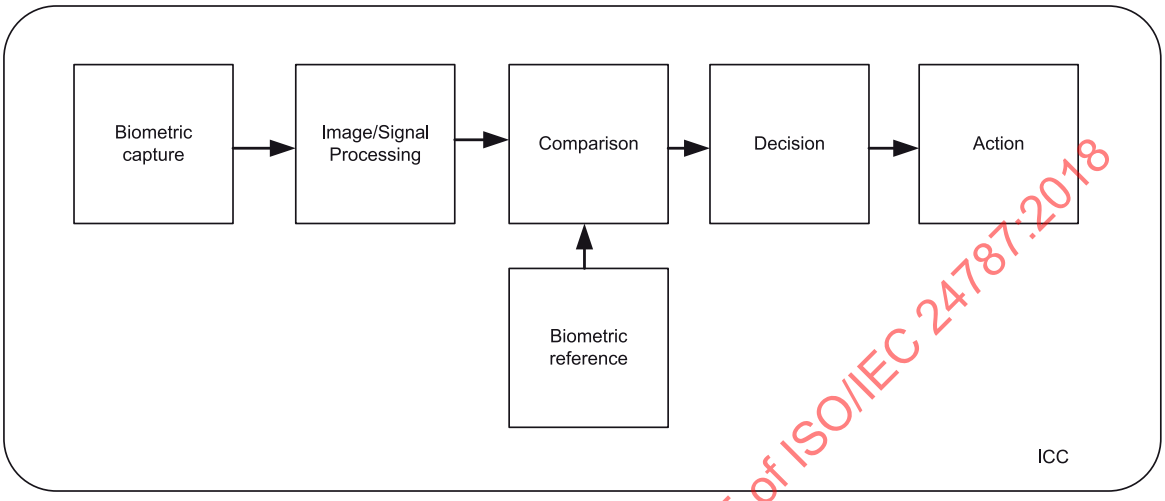

Figure 4 — General architecture for biometric verification using biometric system-on-card

7 Framework for on-card comparison

7.1 General

This clause is applicable to on-card biometric comparison (sensor-off-card) (see 6.3) and work-sharing on-card biometric comparison (see 6.4). It may also be applicable to biometric system-on-card (see 6.5).

7.2 Application selection (AID)

The on-card biometric comparison may be implemented as an independent application. In this case, it shall be identified by a standard AID according to ISO/IEC 7816-4. The on-card biometric comparison application may be selected by this standard AID using the object identifier '28 81 C1 53' (i.e. 'E8 28 81 C1 53' + [an application-specific application identifier extension]).

NOTE The standard AID is derived from the standard's document number according to ISO/IEC 7816-4.

7.3 Data for on-card biometric comparison

7.3.1 General

The biometric information template defined in ISO/IEC 7816-11 shall be used for exchanging biometric information with optional biometric reference data. This document defines data objects for the configuration of the biometric verification (biometric functionality information and biometric comparison parameters). These configuration data objects shall be encapsulated in the biometric information template.

An excerpt of the biometric information template as defined in ISO/IEC 7816-11 is provided in Table 1 for the readability of this document.

Table 1 — Excerpt of the biometric information template

Tag	Len	Value						Note
'7F60'	Var	Biometric information template						See ISO/IEC 7816-11.
		Tag	**Len**	**Value**				
		'A1'	Var	Biometric header template (BHT)				DOs other than DO'91', DO'B1' and DO'B2' encapsulated in this template are specified in ISO/IEC 19785-3.
				Tag	**Len**	**Value**		
				'78'	7	Compatible tag allocation authority		Mandatory if 'A1' is present and the tag allocation is explicit.
						Tag	**Len**	**Value**
						'06'	5	'28819A4903'
								Meaning object identifier of ISO/IEC 19785-3. Only if tag allocation is explicit.
				Tag	**Len**	**Value**		
				'70'	Var	Template for nesting CBEFF TLV DOs defined in ISO/IEC 19785-3		Optional.
						Tag	**Len**	**Value**
						'91' or 'B1'	Var	Algorithm parameters
								See Table 3 for DOs encapsulated in DO'B1'. Only if tag allocation is explicit.
				Tag	**Len**	**Value**		
				'91' or 'B1'	Var	Biometric comparison parameters		See Table 3 for DOs encapsulated in DO'B1'. Only if tag allocation is implicit.
				'B2'	Var	Biometric functionality information		See Table 2 for DOs encapsulated in DO'B2'.
		Tag	**Len**	**Value**				
		'5F2E'	Var	Biometric data (primitive)				
		Tag	**Len**	**Value**				
		'7F2E'	Var	Biometric data (constructed)				
				Tag	**Len**	**Value**		
				'81'	Var	Biometric data in primitive binary standardized format		DOs are specified in ISO/IEC 19794.
				'82'	Var	Biometric data in propriety format (primitive)		
				'A1'	Var	Biometric data in constructed standardized format		
				'A2'	Var	Biometric data in propriety format (constructed)		

NOTE While DO'A0' and DO'A1' under DO'7F60' are defined in ISO/IEC 7816-11, DO'A0' is not used and DO'A1' is the biometric header template for this document.

7.3.2 Format of biometric reference

For reasons of biometric reference interoperability, on-card biometric comparison shall use the biometric data format as defined in the relevant part of the ISO/IEC 19794 series.

The biometric data template DO'7F2E' under the biometric information template DO'7F60' shall be used for encapsulating biometric data. The value field of DO'81' or DO'A1' under DO'7F2E' is a biometric

data or a template for biometric data objects in standardized format (See ISO/IEC 7816-11). An example is provided in Annex A.

Compact card formats as described in the relevant parts of ISO/IEC 19794 are recommended.

7.3.3 Data objects in the scope of biometric verification

7.3.3.1 General requirements

Algorithm parameters may either be in the TLV data object format or a set of data elements not in the TLV data object format. The former is encapsulated in DO'B1' under BHT DO'A1' under the biometric information template DO'7F60'. The latter is encapsulated in DO'91' under BHT DO'A1' under the biometric information template DO'7F60'.

7.3.3.2 Data objects for biometric functionality information

The biometric functionality information for biometric verification consists of a set of data objects described in Table 2. Retrieval of biometric functionality information shall be subjected to the associated security attributes. If biometric functionality information is available, it shall be encapsulated in the BHT DO 'A1', which is under the biometric information template DO '7F60'. This biometric functionality information shall be coded when present, within the 'B2' tag of the BHT (see ISO/IEC 7816-11), as shown in Table 2.

Biometric functionality information is established before ICC issuance. This information can be read out of the ICC but cannot be modified during the ICC operational state. In case of multiple biometric modalities supported by the ICC, each biometric modality shall have its own biometric functionality information.

Table 2 — Data objects for biometric functionality information elements

Tag	Length	Valid values	Description
'80'	1-3		Maximum size of the biometric probe in bytes
'81'	1-3		Maximum size of the biometric reference in bytes
'82'	1	'00' – 'FF'	Supported number of biometric references ('00' – no information given)
'83'	1	'00' : No re-enrolment possible '01' : Re-enrolment possible Other values: RFU	Flag indicating the possibility of re-enrolment
'85'	Var	As defined in ISO/IEC 29794-1	Minimum verification data quality supported by the comparison algorithm as defined in the relevant parts of the ISO/IEC 19794 and ISO/IEC 29794 series
'87'	Var		Minimum quality requirements for the biometric probe for performing the comparison, which can be proprietary (e.g. minimum number of fingerprint minutiae required)
'BF'	Var		Proprietary data
'90'	Var	See Table 4	Types of biometric verification and, if applicable, performance of the ICC
'A4'	8	As defined by the registration authority described in ISO/IEC 19785-3	Identification of the comparison algorithm If 'A4' is present, both fields below shall be present

Table 2 *(continued)*

Tag	Length	Valid values			Description
		Tag	Length	Valid values	
		'80'	2		Vendor ID
		'81'	2		Algorithm ID

7.3.3.3 Biometric comparison parameters

While the biometric functionality information is modality-specific, the biometric comparison parameters are application-specific. These biometric comparison parameters should be stored in a biometric information template that contains a reference to the actual biometric data. These parameters can be modified during enrolment. These parameters are related to a biometric reference. In case the ICC allows for multiple applications to share one biometric reference, each application may have its own set of biometric comparison parameters (see 7.3.4). An example is provided in Annex B.

Table 3 and Table 4 define biometric comparison parameters in the biometric information template for on-card biometric comparison (tag '91'/'B1' under the BHT which is DO'A1' in ISO/IEC 19785-3:2015, Table 3).

Table 3 — Data objects for biometric comparison parameters

Tag	Length	Valid values	Description
'81'	*	*	Minimum and maximum length of the biometric probe This value shall be compatible with the one defined in tag '80' of DO 'B2' (see 7.3.3.2)
'82'	*	*	Ordering, if applicable, of the features in the biometric probe
'83'	*	*	Feature handling indicator
'84'	*	*	Alignment information
'85'	**	**	Minimum verification data quality supported (see Table 2) This value shall be compatible with the one defined in tag '85' of DO 'B2' (see 7.3.3.2)
'90'	1	see Table 4	Biometric verification type and algorithm strength This value shall be compatible with the one defined in tag '90' of DO 'B2' (see 7.3.3.2)
'91'	2	'0001' – 'FFFF'	Estimation from the ICC of its maximum response time in milliseconds, to be provided to the IFD
NOTE 1 "*" denotes that this variable is defined in the relevant part of the ISO/IEC 19794 series. NOTE 2 "**" denotes that this variable is defined in the relevant parts of the ISO/IEC 19794 and ISO/IEC 29794 series.			

On-card biometric comparison may require security attributes to be fulfilled as described in Clause 8.

Table 4 — Biometric verification type and discriminative power (FMR grading)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
—	—	—	—	—	—	x	x	Biometric verification type
—	—	—	—	—	—	0	0	On-card biometric comparison
—	—	—	—	—	—	0	1	Work-sharing on-card biometric comparison
—	—	—	—	—	—	1	0	Biometric system-on-card
[a] This value is provided to enable the system designer to set different comparison levels for different applications with the specific on-card biometric comparison product.								

Table 4 *(continued)*

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
—	—	—	—	—	—	1	1	RFU
—	—	—	x	x	x	—	—	FMR[a] claimed
—	—	—	0	0	0	—	—	No indication given
—	—	—	0	0	1	—	—	FMR grade 1 (largest)
—	—	—	0	1	0	—	—	FMR grade 2
—	—	—	0	1	1	—	—	FMR grade 3
—	—	—	1	0	0	—	—	FMR grade 4
—	—	—	1	0	1	—	—	FMR grade 5
—	—	—	1	1	0	—	—	FMR grade 6 (smallest)
—	—	—	1	1	1	—	—	RFU
x	x	x	—	—	—	—	—	RFU

[a] This value is provided to enable the system designer to set different comparison levels for different applications with the specific on-card biometric comparison product.

A manufacturer shall declare the FMR value for their stated grading. Table 5 is an example of an FMR grading scale.

Table 5 — Example for the FMR grading

FMR grade	FMR
1	≤0,1 %
2	≤0,01 %
3	≤0,001 %
4	≤0,000 1 %
5	≤0,000 01 %
6	≤0,000 001 %

7.3.4 One biometric reference for multiple applications

One biometric reference for multiple applications may require for each application to have its own biometric comparison parameters. For this requirement, a biometric reference may be excluded from a biometric information template DO'7F60'. A file reference DO'51' indicating a biometric reference may be encapsulated in a biometric data template DO'7F2E' under the biometric information template DO'7F60'. An example is provided in Annex B.

7.4 Processes

7.4.1 Enrolment

Enrolment is the process through which a biometric reference is created and stored. The enrolment mechanism specified in ISO/IEC 7816-11 shall be implemented.

Depending on the capabilities of the ICC, signal processing may be split between the IFD and the ICC. In all cases, all biometric data shall be transferred to the ICC through a secure and trusted channel or in a trusted environment, guaranteeing cardholders' privacy. It is recommended to perform a verification test after enrolment to verify the quality of the enrolled data.

Guidance on the enrolment of the biometric data onto the ICC is contained in ISO/IEC 7816-11.

7.4.2 Biometric verification

The biometric verification mechanism specified in ISO/IEC 7816-11 shall be implemented.

7.4.3 Comparison process and result output

7.4.3.1 Comparison process

In case of work-sharing on-card biometric comparison, the last portion of the comparison process takes place within the ICC. In any other cases, the comparison process shall fully take place within the ICC.

7.4.3.2 Decision

The decision is the result of the comparison between the biometric comparison similarity score of given biometric data and a predefined threshold to achieve the desired security level. If the score is not less than the predefined minimal matching score threshold, the biometric verification is successful.

7.5 Biometric comparison parameter management

This subclause defines the policies for managing the biometric comparison parameters and related mechanisms. The following policies shall be followed.

a) The biometric comparison parameters shall define a parameter for internal quality requirements for performing comparisons.

b) The access rules for the use case of one biometric reference for multiple applications, especially for the context of different configurations (in particular FMR grade as defined in Table 5), shall be defined before the first biometric verification.

c) The following biometric comparison parameters as described in 7.3.3.3 shall be considered in order to determine the authenticity during the biometric verification:

   i) minimum quality for verification;

   ii) biometric verification type and discriminative power.

d) The security levels that can be achieved as a result of a positive biometric verification should be obtained from both the biometric functionality information and the biometric comparison parameters. The IFD shall select the security level that is required by its application before initiating the biometric verification.

e) The biometric comparison parameters described in this subclause shall not be changed during the on-card biometric verification.

7.6 Termination

When terminating an on-card biometric comparison application, the on-card biometric reference pertaining only to such application shall be made inaccessible. A possible way is to set a biometric reference as the logical erased state.

8 Security policies for on-card biometric comparison

8.1 General

This clause defines the minimum set of security policies for ICC applications using on-card biometric comparison. As explained below, different approaches can be considered, and although some of the policies can be common to all, there are other policies that are specific for certain approaches.

Within this subclause, an overview to the different approaches is provided. Those different approaches can be classified as:

a) Using biometric comparison parameters as global (categorised into SP1 as in 8.3). This includes the following situations.

   1) ICC with a single application that uses on-card biometric comparison.

   2) ICC with multiple applications that use on-card biometric comparison with a single set of biometric comparison parameters (i.e. same FMR grade, same retry counter, etc.).

b) Using application-specific biometric comparison parameters (categorised into SP2 as in 8.4). This case includes the following situations.

   1) Each application has its own biometric reference structure, including the biometric reference and biometric comparison parameters such as retry counter, FMR grade and maximum value for the retry counter etc.

   2) All applications only share the same biometric reference, but each application has its own biometric comparison parameters, which include the different FMR grades, retry counter, etc. In this case, any changes to biometric comparison parameters will only apply to the ones for the specific application.

NOTE The terms 'global' and 'application-specific' are used in accordance with basic security handling in ISO/IEC 7816-4.

The following subclauses define the common security policies, the SP1 policies, and the SP2 policies.

8.2 Common security policies for on-card biometric comparison

8.2.1 Minimum security policy

In all cases the following minimum security policies apply.

— No application shall be allowed to send the biometric reference outside the ICC.

— A retry counter mechanism shall be implemented according to 8.2.3.

— The integrity of all data exchanged regarding on-card biometric comparison shall be assured.

— All biometric data shall be enciphered for transmission to the ICC, to assure confidentiality in accordance to ISO/IEC 24761. The use of ISO/IEC 24761 is further specified in ISO/IEC 7816-11.

— The ICC operating system may have a mechanism to unblock the on-card biometric comparison. If such is the case, the unblocking process shall reset the retry counter. The specific implementation may additionally require a new enrolment.

8.2.2 Security requirements and biometric reference management policy

Security requirements are:

a) the biometric reference not including biometric auxiliary data and biometric comparison parameters stored in an ICC shall not be read;

b) in order to update the biometric reference, the security rules applicable for enrolment shall apply;

c) retry counter management shall be applied to the biometric verification;

   1) there may be an independent retry counter for each biometric reference;

2) there may be an independent retry counter for each application (i.e. if one retry counter is expired, the retry counters for other applications referring to the same biometric data remain unchanged);

d) the cardholder of the 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.

8.2.3 Retry counter management

Retry counter management defines the policies for managing the retry counter mechanisms. The policies are:

a) an initial value of the retry counter shall be associated to the on-card biometric reference;

b) 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;

c) 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 or PBO command where the data field is absent according to ISO/IEC 7816-4 and ISO/IEC 7816-11;

d) if the biometric verification is successful, the retry counter is reset.

8.3 Security policies (SP1) for global biometric comparison parameters

For those applications where the biometric reference is to be used as a universal verification mechanism, there is no need for several sets of biometric comparison parameters related to one biometric reference for multiple applications. The following policies shall apply.

— For ICCs with multiple applications conducting on-card biometric comparison using the same biometric reference, if any application using the biometric reference is a high security application, unique biometric comparison parameters shall be used by all applications and a single retry counter associated to the biometric reference shall be used.

— None of the applications using the on-card biometric comparison mechanism with such biometric reference shall change the biometric comparison parameters independently.

— A single retry counter is used. That retry counter shall comply with the management as specified in 8.2.3.

8.4 Security policies (SP2) for application-specific biometric comparison parameters

In the case of an ICC whose applications request an independent control of the on-card biometric comparison, but share the same biometric reference, the following policies apply:

— Each application that uses on-card biometric comparison shall have its own set of biometric comparison parameters, including, at least:

  — verification type and strength;

  — retry counter, managed as indicated in 8.2.3.

Any application can change its biometric comparison parameters as desired, without modifying any of the biometric comparison parameters of the other applications which share the same biometric reference.

9 Work-sharing on-card biometric comparison procedure

The following requirements are applied to work-sharing on-card biometric comparison.

— Biometric auxiliary data for work-sharing on-card biometric comparison is stored separately from a biometric reference. For example, biometric auxiliary data is stored in a working EF (Elementary File) and a biometric reference is stored in an internal EF defined in ISO/IEC 7816-4.

— Biometric auxiliary data may be read from an ICC according to the needs of work-sharing on-card biometric comparison.

— The biometric reference should be managed based on security policies.

Figure 5 illustrates the outline of the work-sharing on-card biometric comparison procedure.

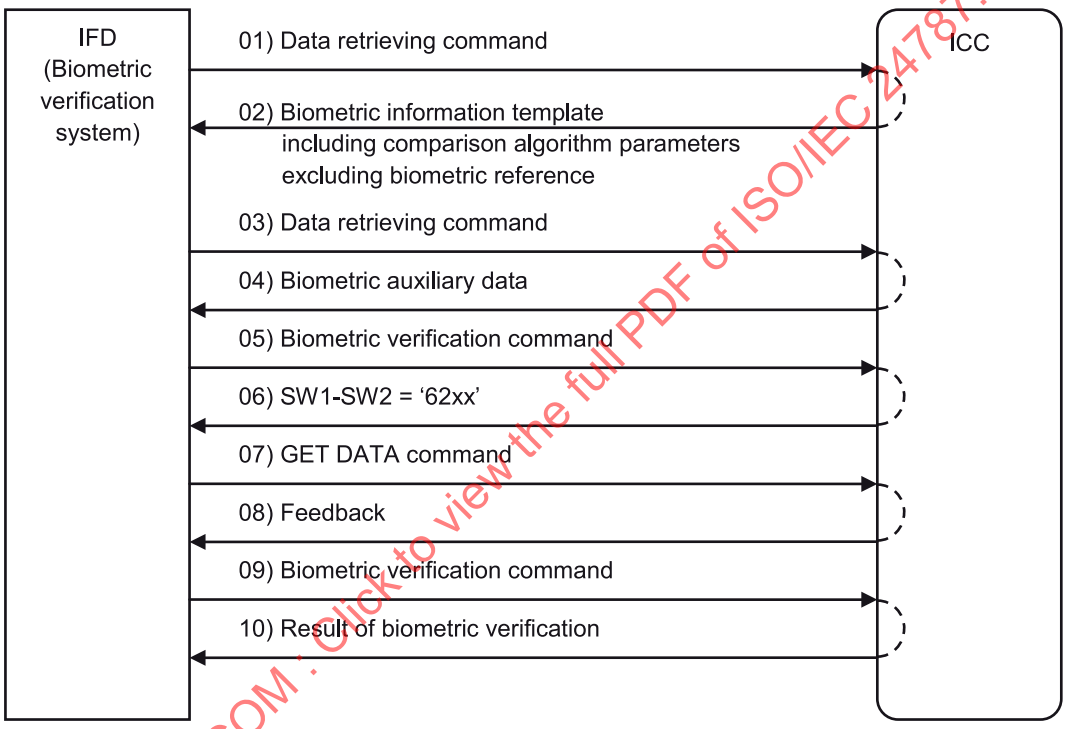

Figure 5 — Command-response APDU exchange for the work-sharing procedure

The following sequence is the outline of the work-sharing procedure.

01) An ICC receives a data retrieving command (e.g. READ BINARY) for extracting the biometric information template excluding the biometric reference.

02) An ICC returns the biometric information template for checking parameters.

03) An ICC receives a data retrieving command, e.g. READ BINARY for extracting biometric auxiliary data.

04) An ICC returns auxiliary data for processing with a biometric sample.

05) An ICC receives a biometric verification command requiring work-sharing on-card biometric comparison (e.g. PBO), and then starts the work-sharing on-card biometric comparison process.

06) An ICC returns status bytes as '62xx' indicating 'xx' bytes of feedback available according to card-originated byte string specified in ISO/IEC 7816-4.

07) An ICC receives GET DATA for extracting feedback.

08) An ICC returns feedback.

09) An ICC receives PBO with continuing biometric comparison, then starts biometric comparison, decision and action.

10) An ICC returns status bytes indicating the result of the biometric verification.

Annex A
(informative)

Sample APDU for on-card biometric comparison

In order to see examples on the use of the PBO command, refer to ISO/IEC 7816-11.

Without the use of the PBO command, this Annex provides examples of how to implement the on-card biometric comparison.

Table A.1 is a construction of a sample APDU according to current standards.

The VERIFY command APDU is used to send a fingerprint minutiae template to the ICC. It has the following structure.

Table A.1 — Command APDU structure

CLA	INS	P1	P2	Lc	Data
'00'	'20' or '21'[a]	'00'	'00'	Length	Lc Bytes of data

NOTE 1 The Le field is empty, because no response data is returned for VERIFY in ISO/IEC 7816-4. Only the status bytes are returned to the IFD.

NOTE 2 The biometric in-use is indicated inside the biometric information template.

[a] INS code '20' is used if the data field contains transparent plain data while INS code '21' indicates that the data field is BER TLV-encoded.

The data field contains the verification data. The ICC's capabilities may be implicitly known. The recommended way is to hold a biometric information template that can publicly be read off the ICC with a GET DATA command using tag '7F60' and gives the outside world information on the ICC's capabilities, for example, support of on-card biometric comparison, what data format and format type is expected and whether the ICC wants the minutiae ordered or not. Details on the biometric information template are found in ISO/IEC 7816-11 and ISO/IEC 19785-3.

The biometric probe in the command data field should be BER-TLV-coded. The following tags are relevant for encoding:

— '7F2E' biometric reference;

— '5F2E' biometric data;

— '81'/'A1' biometric data with standardized format (primitive/constructed);

— '82'/'A2' biometric data with proprietary format (primitive/constructed).

If sending a standard minutiae data set to the ICC, this encodes to the data field in Table A.2.

Table A.2 — Data fields for standard minutiae

Tag biometric data	Length of data object	Tag biometric data standardized	Length of minutiae data	Minutiae data
'7F2E'	L+2	'81'	L	

NOTE In Table A.2, the reason for using the tag '7F2E' is because the value field contains a constructed biometric data object. The constructed biometric data object begins with the tag '81', followed by the actual biometric data value. Another potential implementation is to use the tag '5F2E' to encapsulate biometric data as a primitive object explicitly.

Figure A.1 shows a fingerprint image with the minutiae positions marked.

Figure A.1 — Fingerprint image with minutiae positions

The minutiae are scaled to metric units and compressed into the compact card format for on-card biometric comparison use. This results in the following data (hexadecimal):

'25 5D 69 2D A1 43 2F AA 82 2F 6F 48 2F 43 49 35 96 45 37 AF 81 48 B0 BF 48 96 48 48 5D 89 4A 9C 43 4D 7C 6A 4D 63 6A 4D 19 45 4F 73 8B 50 91 42 54 85 6B 57 6B AA 58 86 B2 58 7D 70 59 36 82 5B 8C 57 5E 94 9C 5F 73 71 61 61 66 64 4C 9C 69 97 9B 6F A5 9D 70 33 B9 72 50 96 74 92 58 7D 27 59 7E 9D 59 80 66 93 83 4A 56 86 8E 56 90 3D 74 9A 3A 76'

Format type 6 of format owner '0101' from ISO/IEC 19794-2 was used to encode the minutiae excluding any extended data. The minutia positions are at the ridge skeleton bifurcation points and the ridge skeleton end points. This is in analogy with ground truth as used by a manual fingerprint examiner and common practice with most vendors of fingerprint algorithms. Every minutia is represented by a triplet

of bytes. The first minutia has horizontal position '25', vertical position '5D', type ridge end bifurcation and orientation 205° are stored in '69'.

A total of 38 minutiae were detected, which results in a total minutiae size of 3 x 38 = 114 bytes, hexadecimal '72'.

The data added to the above structure results in the following command.

CLA	INS	P1	P2	Lc	Data
'00'	'21'	'00'	'00'	'77'	

Tag Biometric reference	Length of Data Object	Tag Biometric Data Standardized	Length of minutiae data	Minutiae data
'7F2E'	'74'	'81'	'72'	

'25 5D 69 2D A1 43 2F AA 82 2F 6F 48 2F 43 49 35 96 45 37 AF 81 48 B0 BF 48 96 48 48 5D 89 4A 9C 43 4D 7C 6A 4D 63 6A 4D 19 45 4F 73 8B 50 91 42 54 85 6B 57 6B AA 58 86 B2 58 7D 70 59 36 82 5B 8C 57 5E 94 9C 5F 73 71 61 61 66 64 4C 9C 69 97 9B 6F A5 9D 70 33 B9 72 50 96 74 92 58 7D 27 59 7E 9D 59 80 66 93 83 4A 56 86 8E 56 90 3D 74 9A 3A 76'

Figure A.2 — Structure of APDU for on-card biometric comparison

Total command:

'00 21 00 00 77 7F 2E 74 81 72 25 5D 69 2D A1 43 2F AA 82 2F 6F 48 2F 43 49 35 96 45 37 AF 81 48 B0 BF 48 96 48 48 5D 89 4A 9C 43 4D 7C 6A 4D 63 6A 4D 19 45 4F 73 8B 50 91 42 54 85 6B 57 6B AA 58 86 B2 58 7D 70 59 36 82 5B 8C 57 5E 94 9C 5F 73 71 61 61 66 64 4C 9C 69 97 9B 6F A5 9D 70 33 B9 72 50 96 74 92 58 7D 27 59 7E 9D 59 80 66 93 83 4A 56 86 8E 56 90 3D 74 9A 3A 76'

There are other possibilities to encode the minutiae and to construct the command. Optional features or proprietary data may be used.

An application profile should give guidance to these options to ease the implementation of interoperable applications using technology from a variety of vendors.

Annex B
(informative)

Example of one biometric reference for multiple applications

This annex provides an example of the structure of one biometric reference for two different applications. Each application has its own biometric information template DO'7F60' defined in ISO/IEC 7816-11 including its own biometric comparison parameters. These biometric information templates also have biometric data template DO'7F2E' defined in ISO/IEC 7816-11. A biometric reference is not encapsulated in these biometric data templates but a file reference DO'51' defined in ISO/IEC 7816-4 is encapsulated for indicating one biometric reference.

Table B.1 indicates an example of the structure for a biometric information template.

Table B.1 — An example of the structure for a biometric information template

Tag	Len	Value				Note
'7F60'	Var	Biometric information template				See ISO/IEC 7816-11
		Tag	**Len**	**Value**		
		'A1'	Var	Biometric header template (BHT)		
				Tag	**Len**	**Value**
				'B1'	Var	Biometric comparison parameters
				'B2'	Var	Biometric functionality information
		Tag	**Len**	**Value**		
		'7F2E'	Var	Biometric data template		
				Tag	**Len**	**Value**
				'51'	Var	File reference

This example uses the file structure defined in ISO/IEC 7816-4 for hosting applications and storing application data. Figure B.1 illustrates an example of a file structure of one biometric reference for two applications. The overview of this figure is below.

— The biometric reference is stored in the internal EF (Elementary File) for protecting under the MF (Master File) and this is referred from two different applications by using the file reference DO'51' encapsulated in its own biometric information template stored in the EF for each application.

— Two DFs (Dedicated File) are under the MF and each DF hosts an application having the biometric verification functionality.

— Each working EF for retrieving under each application DF stores an application-dependent biometric information template. Each application may provide its own biometric comparison parameters.

— The FCI (File Control Information) is provided to each EF storing the application-dependent biometric information template. The FCI associated to the EF may include security attributes. Security attributes may indicate security conditions for executing each command to this EF, e.g. READ BINARY and VERIFY.

— The file reference DO'51' is encapsulated in each application-dependent biometric information template. The absolute path to the file is encapsulated in the file reference DO'51' and it identifies

the EF storing the biometric reference. This absolute path is a concatenation of the file identifier from the MF to the objective EF.

The MF, DF, internal/working EF, FCI, security attribute, security condition, file reference and absolute path are defined in ISO/IEC 7816-4.

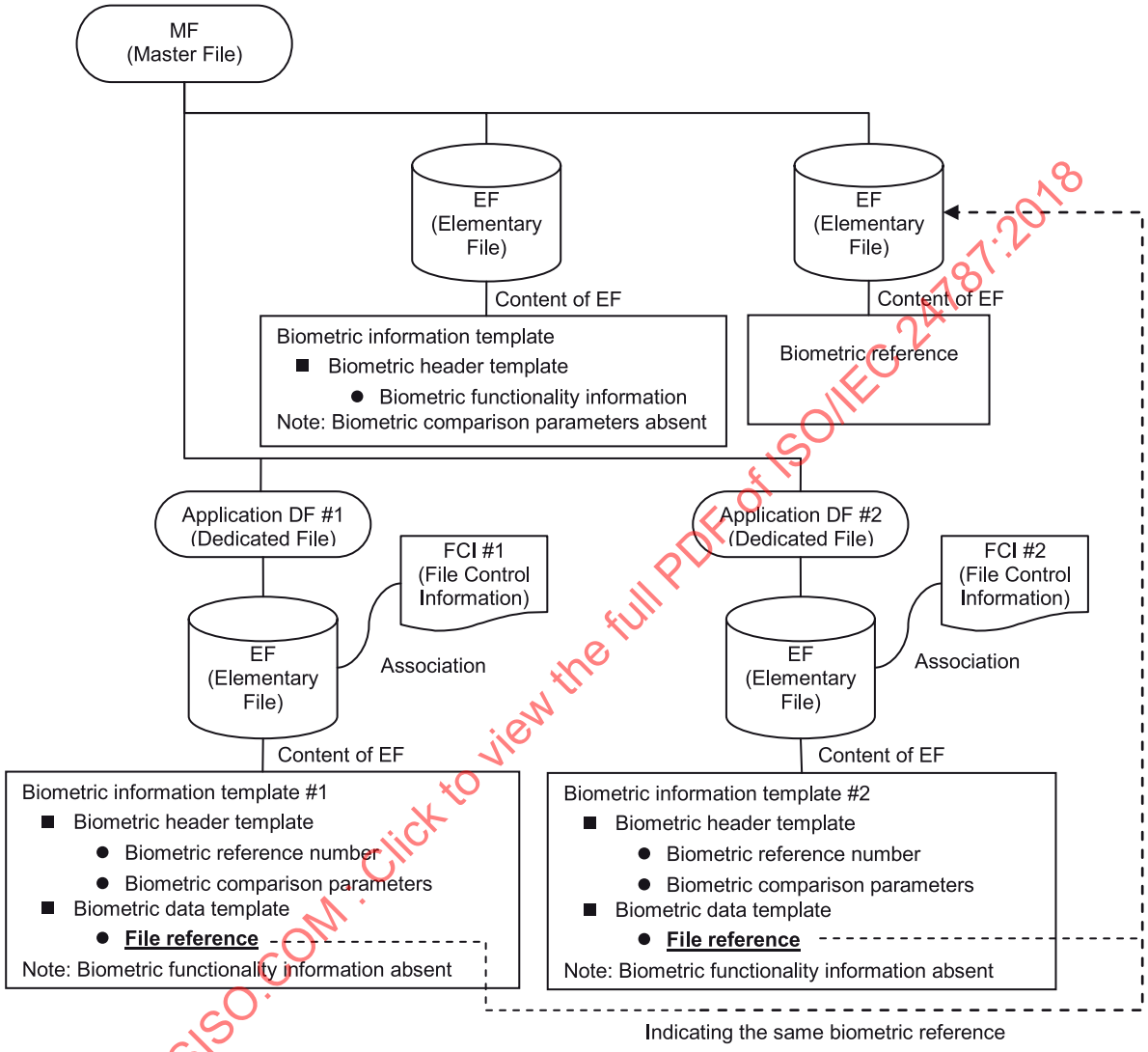

Figure B.1 — Example of file structure of one biometric reference for two applications