International Standard

ISO/IEC 24787-1

Information technology — On-card biometric comparison —

Part 1: General principles and specifications

Technologies de l'information — Comparaison biométrique sur cartes —

Partie 1: Principes généraux et spécifications

First edition
2024-06

Reference number
ISO/IEC 24787-1:2024(en)

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

Published in Switzerland

Contents

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

This first edition cancels and replaces ISO/IEC 24787:2018, which has been technically revised. ISO/IEC CD 24787 has been split into two parts: ISO/IEC 24787-1 and ISO/IEC 24787-2.

The main changes are as follows:

- Previous Clause 9 “Work-sharing on-card biometric comparison procedure” and other subclauses related to work-sharing have been moved to ISO/IEC 24787-2.

A list of all parts in the ISO/IEC 24787 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

On-card biometric comparison provides a more secure biometric verification method than one where a biometric comparison is carried out outside a secure cryptographic device. Storing biometric reference data in a secure integrated circuit card (ICC) for on-card biometric comparison 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 unauthorized party.

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

Information technology — On-card biometric comparison —

Part 1: General principles and specifications

1 Scope

This document provides requirements and general principles and specifications for a biometric comparison methodology suitable for the on-card environment.

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, 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 (defined in the ISO/IEC 17839 series),

— work-sharing on-card biometric comparison (defined in ISO/IEC 24787-2), 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 2382-37:2022, *Information technology — Vocabulary — Part 37: Biometrics*

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

ISO/IEC 7816-11:2022, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 19785-3:2020, *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 29794 (all parts), *Information technology — Biometric sample quality*

ISO/IEC 39794 (all parts), *Information technology — Extensible biometric data interchange formats*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and the following apply.

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

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

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

3.1
action
operation taken according to the results of the biometric *decision* (3.9)

EXAMPLE In the case of *on-card biometric comparison* (3.11), the action is a change in the security status.

Note 1 to entry: Specific details of possible actions based on the result of on-card biometric comparison within the integrated circuit card (ICC) are not within the scope of this document.

3.2
biometric auxiliary data
data that is dependent on the biometric modality and related to the *biometric reference* (3.6) but does not include the biometric reference or a biometric sample

EXAMPLE Data such as orientation, scaling, etc.

3.3
biometric comparison parameters
application specific parameters that are required to perform a biometric comparison with the appropriate enrolled *biometric reference* (3.6)

3.4
biometric functionality information
capability information of *on-card biometric comparison* (3.12) provided by the integrated circuit card (ICC) operating system

3.5
biometric information template
descriptive information regarding the associated biometric data

Note 1 to entry: "Biometric template" defined in ISO/IEC 2382-37 is not the same as "biometric information template" as defined in ISO/IEC 7816-11. A biometric template is a set of features extracted from the biometric samples during enrolment. This is completely different from the concept of “template” by the integrated circuit card (ICC) industry and standards (see ISO/IEC 7816-4), which is a defined structure of the value field of a constructed data object.

3.6
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

[SOURCE: ISO/IEC 2382-37:2022, 37.03.16, modified — The EXAMPLE and Notes to entry have been removed.]

3.7
biometric system-on-card
card-sized device including biometric capture, data processing, storage, comparison, *decision* (3.9) and *action* (3.1), to compose a complete *biometric verification* (3.8) system

[SOURCE: ISO/IEC 17839-1:2014, 3.1, modified — Replaced "acquisition" with "capture", deleted "action", deleted Notes 1 and 2 to entry.]

3.8
biometric verification
process of confirming a biometric claim through comparison

Note 1 to entry: Biometric verification is performed through comparison, decision, and action.

[SOURCE: ISO/IEC 2382-37:2022, 37.08.03, modified — Notes 1 and 2 to entry have been replaced by a new Note 1 to entry.]

3.9
decision
process that compares a similarity score to a predefined threshold to decide whether the biometric claim is from the genuine cardholder or an imposter

3.10
image/signal processing
process that extracts distinctive biometric properties from a given image or signal

3.11
modality
combination of a biometric characteristic type, a sensor type and a processing method

Note 1 to entry: Adapted from the definition for the term "mode" in ISO/IEC 2382-37:2022, 37.02.05.

3.12
on-card biometric comparison
comparison and decision making on the integrated circuit card (ICC) where the *biometric reference* (3.6) is retained on-card in order to enhance security and privacy

3.13
off-card biometric comparison
biometric comparison performed outside the integrated circuit card (ICC) by the *biometric verification* (3.8) system against the *biometric reference* (3.6) stored on the ICC

3.14
work-sharing
splitting the computational workload of the comparison process between the integrated circuit card (ICC) and the interface device (IFD)

3.15
sensor-off-card
sensor located on the interface device (IFD) outside of the integrated circuit card (ICC)

3.16
termination
permanent deactivation of an on-card biometric comparison application

4 Abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 7816-11, ISO/IEC 7816-4 and the following apply.

AID	application identifier
APDU	application protocol data unit
BER	basic encoding rules
BHT	biometric header template
BIDO	biometric information data object
CBEFF-3	common biometric exchange formats framework – Part 3 – patron format specifications (ISO/IEC 19785-3)
DF	dedicated file

DO	BER-TLV data object
EF	elementary file
eMRTD	electronic machine-readable travel document
FCI	file control information
FMR	false match rate
ICC	integrated circuit card
IFD	interface device
Len	length
MAC	message authentication code
MF	master file
OID	object identifier
PBO	PERFORM BIOMETRIC OPERATION
PIN	personal identification number
RFU	reserved for future use
SW1-SW2	status bytes
TLV	tag length value
Var	variable

5 Conformance

An on-card biometric comparison system claiming conformance to this document shall follow the requirements in Table 1:

Table 1 — Conformance requirement for on-card biometric comparison systems

No.	Description	Requirement
1	Conform to the requirements set forth in 8.3.1 for encoding of biometric data	Mandatory
2	Support the storage of three sets of data:	-
2a)	Biometric reference, as described in 8.3.2	Mandatory
2b)	Biometric functionality information, as described in 8.3.3.2	Mandatory unless implicitly known by IFD
2c)	Biometric comparison parameters, as described in 8.3.3.3	Mandatory unless implicitly known by IFD for the specific DF
3	Support the usage of one biometric reference by multiple applications, as described in 8.3.4	Optional
4	Support retry counter management, as described in 9.1.3	Mandatory
5	Conform to the requirements set forth in 8.4 and 8.5 for on-card biometric comparison implementations	Mandatory

6 Biometric data handling and encoding

For handling of biometric data, 8.4 specifies the requirements, according to ISO/IEC 7816-11.

For encoding of biometric data, 8.3.1 specifies the requirements, according to ISO/IEC 19785-3 and ISO/IEC 7816-11.

7 Architecture of biometric verification using an ICC

7.1 General

The following subclauses describe four biometric verification architectures using an ICC or an ICC with a biometric verification system. This document only specifies the requirements for the architecture mentioned in 7.3.

While off-card biometric comparison is out of scope for this document, the information in 7.2 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.

Biometric verification can coexist with other authentication mechanisms, such as PIN, as defined in ISO/IEC 7816-4.

7.2 Off-card biometric comparison

Off-card biometric comparison means that the biometric verification is performed on the off-card biometric verification system outside of the ICC. 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 In 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 eMRTD. Then the stored facial image (biometric reference) is retrieved from the eMRTD and facial image recognition (biometric comparison) is executed by the system. When the comparison is successful (the eMRTD holder is verified), the system allows the passage of the eMRTD holder.

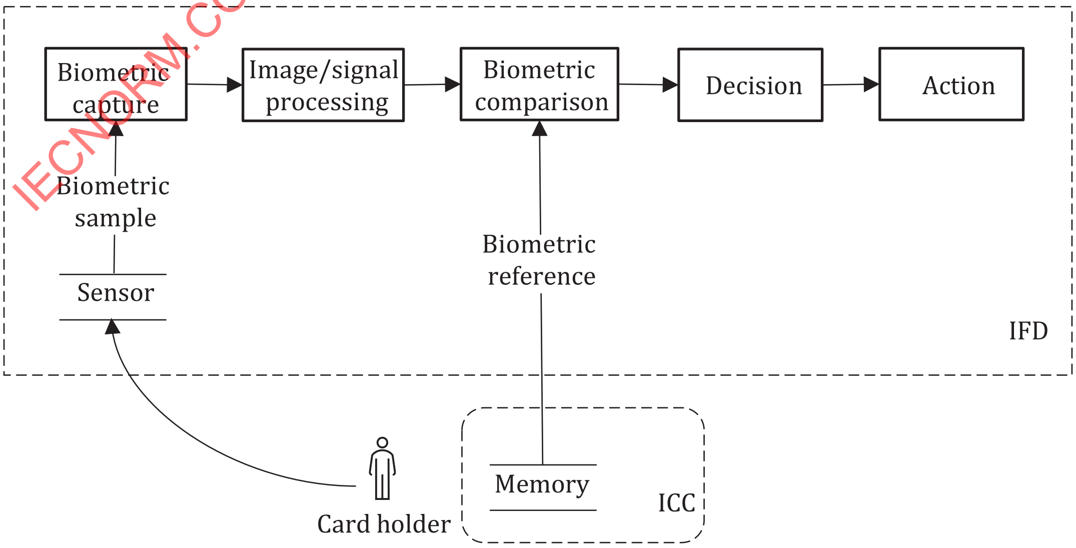


Figure 1 — General architecture of off-card biometric comparison

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

On-card biometric comparison means that 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.

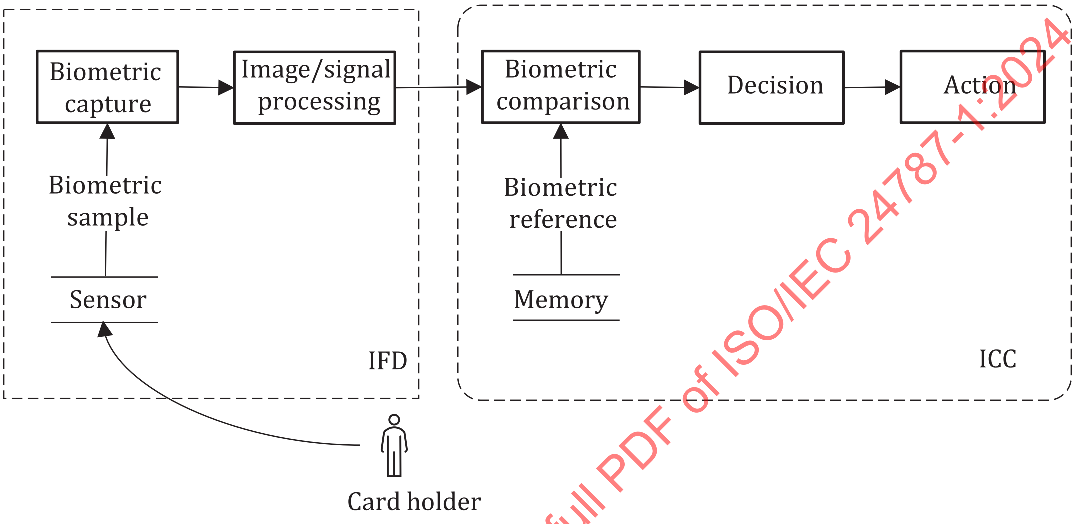


Figure 2 — General architecture of on-card biometric comparison (sensor-off-card)

7.4 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 can be used by an ICC that does not have sufficient processing capability (e.g. long processing time) to execute the entire biometric data comparison.

NOTE 1 The requirements for this architecture for work-sharing biometric verification are specified in ISO/IEC 24787-2. This architecture is only applicable for sensor-off-card.

This biometric comparison process is divided into several sub-processes which are executed in an IFD and on an ICC. Figure 3 shows an example of this process that has one iteration of feedback. Biometric auxiliary data is stored in an ICC and a biometric reference is stored in a 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 can be 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;
  - when such processing is carried out at the ICC side, the biometric reference is used by the ICC if required;

  - when such processing is carried out at the IFD side, the ICC can pass feedback from the previous biometric comparison process to the IFD as input;

- the final process of the biometric comparison procedure is executed on the 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.

This architecture shall be in conformity with ISO/IEC 24787-2 that specifies details of work-sharing on-card biometric comparison.

NOTE 2 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.

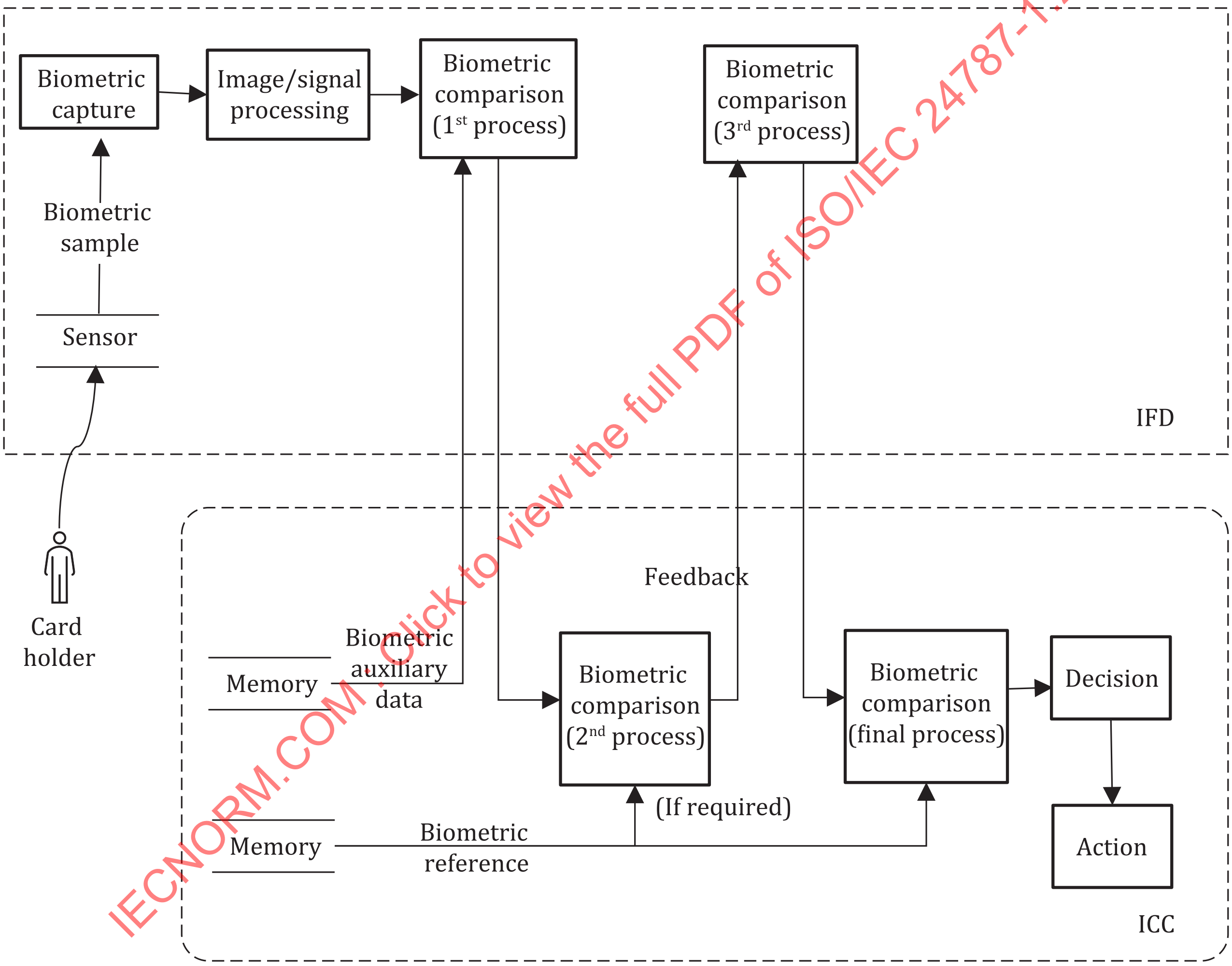


Figure 3 — Example of architecture for work-sharing on-card biometric comparison

7.5 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.

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

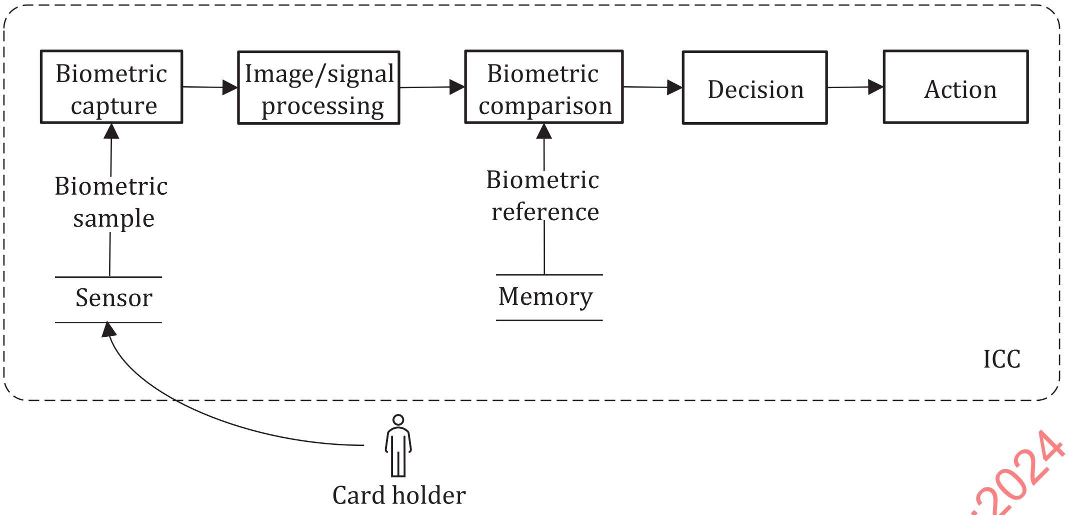


Figure 4 — General architecture of biometric system-on-card

8 Framework for on-card biometric comparison

8.1 General

This clause is applied to on-card biometric comparison (sensor-off-card) (see 7.3) and work-sharing on-card biometric comparison (see 7.4). It can be applied to biometric system-on-card (see 7.5).

8.2 Application selection using AID

The on-card biometric comparison can be implemented as an independent application. In this case, it may 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 01’[1] (i.e. ‘E8 28 81 C1 53 01’ + [an application-specific AID extension]).

NOTE Application-specific AID extension is RFU.

8.3 Data for on-card biometric comparison

8.3.1 General

This document defines data objects for the configuration of the biometric verification (i.e. biometric functionality information and biometric comparison parameters) which can be encapsulated in the biometric information template defined in ISO/IEC 7816-11.

ISO/IEC 7816-11 allows for two types of data encoding, namely explicit tag allocation coding and implicit tag allocation coding. For this document, explicit tag allocation coding shall be used. DO'A1' immediately under the biometric information template shall be used for ISO/IEC 19785-3 and DO'A2' immediately under the biometric information template shall be used for the BIDOs related to on-card biometric comparison. Table 2 specifies a biometric information template using the explicit tag allocation coding specification given in ISO/IEC 7816-11:2022, Table 9 with the inclusion of the DOs defined in this document and ISO/IEC 19785-3:2020, Clause 19. Within this document, tag 'A0' under '7F60' is not considered, making it a requirement to use tags 'A1' and 'A2' for DOs defined by ISO/IEC 19785-3 and this document respectively.

Annex E contains a more comprehensive example of a biometric information template, which includes the data elements defined by ISO/IEC 19785-3 under the biometric header template (BHT) at tag ‘A1’.

[1] This OID used in the standard AID represents ISO/IEC 24787-1 even when the on-card biometric comparison application is in conformity with ISO/IEC 24787-2.

For explicit tag allocation coding, refer to ISO/IEC 7816-11 and ISO/IEC 19785-3:2020, Clause 19.

Table 2 — Biometric information template with DOs defined for on-card biometric comparison

<table>
<tr><th>Tag</th><th>Len</th><th colspan="7">Value</th><th>Presence</th></tr>
<tr><td rowspan="17">‘7F60’</td><td rowspan="17">Var</td><td colspan="7">Biometric information template (see ISO/IEC 7816-11:2022, Table 9)</td><td></td></tr>
<tr><th>Tag</th><th>Len</th><th colspan="5">Value</th><th></th></tr>
<tr><td>‘80’</td><td>1</td><td colspan="5">Algorithm reference for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SE command as defined in ISO/IEC 7816-4</td><td>Optional</td></tr>
<tr><td>‘83’</td><td>1</td><td colspan="5">Reference data qualifier for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SE command as defined in ISO/IEC 7816-4</td><td>Optional</td></tr>
<tr><td>‘A1’</td><td>Var</td><td colspan="5">BIDOs specified by other than ISO/IEC 7816-11
For this document, this DO is reserved for:
BIDOs for CBEFF-3 (ISO/IEC 19785-3:2020, Clause 19)</td><td>Mandatory if any DOs specified in ISO/IEC 19785-3:2020, Clause 19 are present</td></tr>
<tr><td rowspan="10">‘A2’</td><td rowspan="10">Var</td><td colspan="5">BIDOs specified by other than ISO/IEC 7816-11
For this document, this DO is reserved for:
BIDOs for this document</td><td>Mandatory</td></tr>
<tr><th>Tag</th><th>Len</th><th colspan="3">Value</th><th></th></tr>
<tr><td rowspan="3">‘78’</td><td rowspan="3">9</td><td colspan="3">Compatible tag allocation authority</td><td>Mandatory</td></tr>
<tr><th>Tag</th><th>Len</th><th>Value</th><th></th></tr>
<tr><td>'06'</td><td>7</td><td>'28 81 C1 53 01 8F 68'</td><td>Mandatory
OID of this document (1.0.24787.1.2024)</td></tr>
<tr><th>Tag</th><th>Len</th><th colspan="3">Value</th><th></th></tr>
<tr><td rowspan="4">‘70’</td><td rowspan="4">Var</td><td colspan="3">BIDOs specified in this document</td><td>Mandatory</td></tr>
<tr><th>Tag</th><th>Len</th><th>Value</th><th></th></tr>
<tr><td>‘91’ or ‘B1’</td><td>Var</td><td>Biometric comparison parameters
See Table 4 for DOs encapsulated in DO’B1’</td><td rowspan="2">At least one DO with tag ‘91’ or ‘B1’ for biometric comparison parameters or with tag ‘92’ or ‘B2’ for Biometric functionality information shall be present.</td></tr>
<tr><td>‘92’ or ‘B2’</td><td>Var</td><td>Biometric functionality information
See Table 3 for DOs encapsulated in DO’B2’</td></tr>
<tr><th>Tag</th><th>Len</th><th colspan="5">Value</th><th></th></tr>
<tr><td>‘5F2E’ or ‘7F2E’</td><td>Var</td><td colspan="5">Biometric data (primitive/constructed) (see ISO/IEC 7816-11)</td><td>If biometric data is stored in DO’7F60’, either DO’5F2E’ or DO’7F2E’ shall be present</td></tr>
</table>

NOTE The content of this biometric information template contains the tags specified in ISO/IEC 7816-11:2022 Table 9 with additional inclusion of ISO/IEC 24787-1 and ISO/IEC 19785-3:2020 Clause 19 DOs.

8.3.2 Format of biometric data

For reasons of biometric reference interoperability, the formats as defined in ISO/IEC 7816-11 shall be used for biometric data to be sent to the ICC.

If a biometric information template DO'7F60' encapsulates biometric data, either DO'5F2E' or DO'7F2E' shall be used.

Compact card formats as described in the relevant parts of the ISO/IEC 19794 series or the ISO/IEC 39794 series are recommended.

There can be cases where the biometric data (primitive/constructed) are excluded from a biometric information template. One such possible case is when a biometric reference is used by multiple applications (see 8.3.4). Another possible case is when a biometric reference is not retrievable from an ICC with on-card biometric comparison mechanism due to security policy (see 9.2.1).

8.3.3 Specific data objects

8.3.3.1 General

Biometric comparison parameters and biometric functionality information may either be in the TLV data object format or a set of data elements not in the TLV data object format.

When in the TLV data object format, they are encapsulated in DO'B1' and DO'B2' respectively, under the DO'70' within BIDOs DO'A2' included in the biometric information template DO'7F60'.

When in a set of data elements not in the TLV data object format, they are encapsulated in DO'91' and DO'92' respectively, under the DO'70' within BIDOs DO'A2' included in the biometric information template DO'7F60'.

8.3.3.2 Biometric functionality information

To declare the limiting values for the biometric functionality of each modality on the ICC, biometric functionality information is provided within the DO‘92’ or DO‘B2’ of a biometric information template (see Table 2). The data elements stored in the DO'B2'are defined in Table 3.

The biometric functionality information can be read out of the ICC but cannot be modified during the ICC operational state. Retrieval of biometric functionality information can be subjected to the associated security attributes.

In case of multiple biometric modalities supported within the ICC, the biometric functionality information corresponding to each biometric modality can be specified.

Re-enrolment capability of the ICC is notified by retrieving the DO’83’. According to the value of DO’83’, the ICC shall control re-enrolment of the modality that the DO'83' associated with.

Table 3 — Data objects for biometric modality functionality information elements

Tag	Length	Value	Presence
‘80’	1-3	Maximum length (e.g. number of minutiae) of the biometric probe [a]	Optional
‘81’	1-3	Maximum length (e.g. number of minutiae) of the biometric reference [a]	Optional
‘82’	1	Supported number of biometric references '00': no information given	Optional
‘83’	1	Re-enrolment capability '00': Re-enrolment prohibited '01': Re-enrolment supported Other value: RFU	Optional
‘85’	Var	Minimum verification data quality as defined in ISO/IEC 29794-1, which is supported by the comparison algorithm as defined in the relevant parts of the ISO/IEC 19794 series and the ISO/IEC 29794 series	Optional
‘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)	Optional

Table 3 *(continued)*

Tag	Length	Value	Presence
'8F'	Var	Proprietary data	Optional
‘90’	Var	Biometric verification type and discriminative power (FMR grading) (see Table 5)	Mandatory if SP2 (see 9.2.3) is applied. Optional otherwise.

[a] Each modality may have its own definition of length of the biometric probe/reference. For example, the length for fingerprints is referring to the number of minutiae, while the length for face can be the number of bytes.

NOTE Some or all of the DOs in Table 3 can be made mandatory by a particular application profile.

8.3.3.3 Biometric comparison parameters

While the biometric functionality information is modality-specific, the biometric comparison parameters are both modality-specific and application-specific. These biometric comparison parameters are stored in a biometric information template that belongs to an on-card biometric comparison application. This biometric information template can be linked to the actual biometric data. These parameters can be modified during enrolment. In case the ICC allows for multiple applications to share one biometric reference, each application may have its own set of biometric comparison parameters (if the parameters are different) or may have a common set of biometric comparison parameters in the MF (see 8.3.4). An example is provided in Annex B.

Table 4 and Table 5 define biometric comparison parameters in the biometric information template for on-card biometric comparison (tag '91' or 'B1' under DO'70', which is under the DO'A2').

If the biometric information template contains any biometric comparison parameters, it shall include a parameter for minimum verification data quality for performing comparisons (i.e. DO’85’ in Table 4 in case the parameters are provided in the DO'B1').

Table 4 — Data objects for biometric comparison parameters

Tag	Length	Value	Presence
‘81’[a]	1-3	Minimum and maximum length (e.g. number of minutiae) of the biometric probe [c] This value shall be compatible with the one defined in tag ‘80’ of DO’B2’ (see 8.3.3.2)	Optional
‘82’ [a]	1	Ordering, if applicable, of the features in the biometric probe	Optional
‘83’ [a]	1	Feature handling indicator	Optional
‘84’ [a]	Var	Alignment information	Optional
‘85’ [b]	Var	Minimum verification data quality as defined in ISO/IEC 29794-1, which is supported by the comparison algorithm as defined in the relevant parts of the ISO/IEC 19794 series and the ISO/IEC 29794 series This value shall be compatible with the one defined in tag ‘85’ of DO’B2’ (see 8.3.3.2)	Mandatory
‘90’	1	Biometric verification type and discriminative power This value shall be compatible with the one defined in tag ‘90’ of DO’B2’ (see 8.3.3.2)	Mandatory if SP2 (see 9.2.2) is applied. Optional otherwise.
‘91’	2	Estimation from the ICC of its maximum response time in milliseconds, to be provided to the IFD ‘0001’ – ‘FFFF’	Optional

[a] The value is defined in the relevant part of the ISO/IEC 19794 series.

[b] The value is defined in the relevant parts of the ISO/IEC 19794 series and the ISO/IEC 29794 series.

[c] Each modality may have its own definition of length of the biometric probe/reference. For example, the length for fingerprints is referring to the number of minutiae, while the length for face can be the number of bytes.

NOTE All or some DOs can be made mandatory by a particular application profile.

Table 5 — 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
—	—	—	—	—	—	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.

Table 6 — 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

If the FMR value is higher than FMR grade 1, the FMR grade shall be indicated as “No indication given”.

8.3.4 Use of biometric reference for multiple applications (informative)

8.3.4.1 General

When multiple on-card biometric comparison applications are stored in a single ICC, the data management policy related to biometric comparison can be designed by the location of the data storage and its access control setting.

NOTE 8.3.4.2 through 8.4.3.3 refer to the biometric comparison application(s) while 8.3.4.4 can refer to applications making use of a single and shared biometric comparison application that has common reference and common comparison parameters.

8.3.4.2 Multiple independent biometric comparison applications

If each on-card biometric comparison application uses its own biometric reference, the biometric reference can be stored independently within a DF associated with the on-card biometric comparison application (i.e. an application DF). This DF also stores a biometric information template to provide the biometric comparison parameters of the application as shown in Figure 5. Refer to SP3 for security implementation requirements.

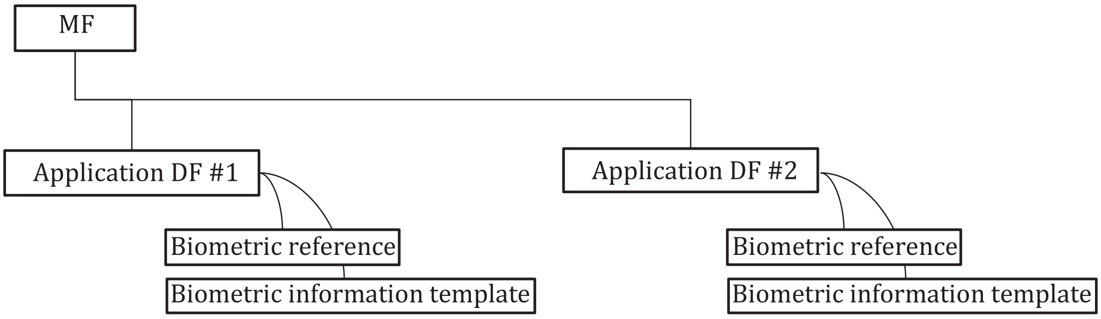


Figure 5 — Application-specific biometric reference management

8.3.4.3 Global biometric reference with application-specific parameters for biometric comparison applications

In case multiple on-card biometric comparison applications share a single biometric reference, the biometric reference can be stored in a MF as a global biometric reference as shown in Figure 6. And if each of the applications manages its biometric comparison parameters independently, each application DF stores its own biometric information template to provide the independent biometric comparison parameters. This biometric information template can also provide information (e.g. link, location, or qualifier) regarding the actual biometric reference.

SP2 specifies the security implementation requirements.

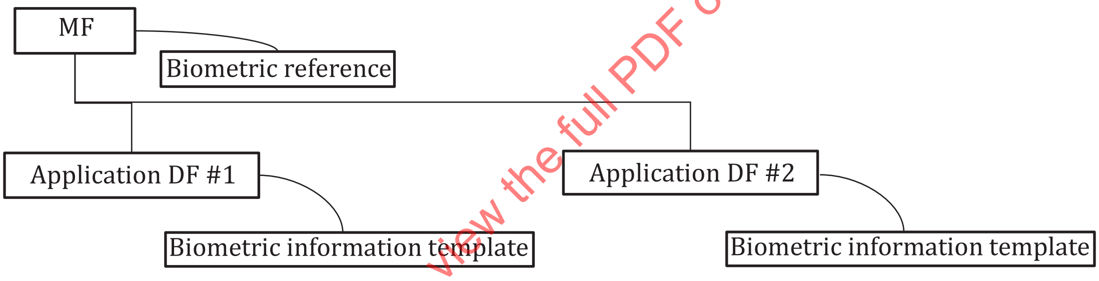

MF
Biometric reference
Application DF #1
Application DF #2
Biometric information template
Biometric information template

Figure 6 — Global biometric reference management with application-specific comparison parameters

8.3.4.4 Global biometric reference with shared parameters for multiple biometric comparison applications

In case multiple on-card biometric comparison applications share both a single biometric reference (i.e. global biometric reference) and a single set of biometric comparison parameters (i.e. global parameters), both the biometric reference and a biometric information template to provide the biometric comparison parameters are stored in an MF. To guide the IFD to access necessary data elements for biometric comparison, each application DF can store its own biometric information template that provides information (e.g. link, location, or qualifier) regarding the actual data elements stored in the MF as shown in Figure 7.

SP1 specifies the security implementation requirements.

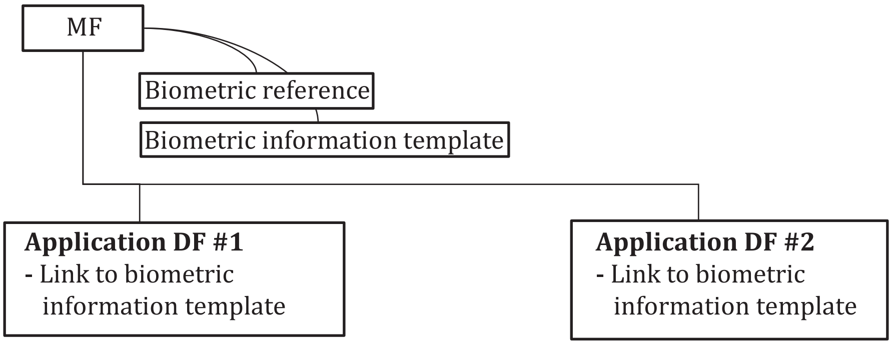

MF
Biometric reference
Biometric information template
Application DF #1
- Link to biometric information template
Application DF #2
- Link to biometric information template

Figure 7 — Global biometric reference management with shared comparison parameters

8.4 Processes

8.4.1 Enrolment and re-enrolment

Enrolment or re-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. The re-enrolment mechanism specified in ISO/IEC 7816-11 can be implemented according to the requirements of the system.

Depending on the capabilities of the ICC, image/signal processing can 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 or re-enrolment to verify the quality of the enrolled data.

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

8.4.2 Biometric verification

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

During biometric verification, the following biometric comparison parameters are included in the process:

a) minimum verification data quality;

b) biometric verification type and discriminative power (if present).

The security status (verification succeeded or failed) can be set as a result of a biometric verification. The biometric verification consists of the biometric comparison and the decision using the biometric comparison parameters. Before the biometric verification is initiated, these biometric comparison parameters are set according to the security level required by the application. A sample APDU for on-card biometric comparison to perform fingerprint verification can be found in Annex A for reference.

8.4.3 Biometric comparison process and decision

8.4.3.1 Biometric comparison process

In case of work-sharing on-card biometric comparison, at least the final process of the biometric comparison shall take place within the ICC. For on-card biometric comparison that does not perform work-sharing, the biometric comparison process shall fully take place within the ICC.

8.4.3.2 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.

8.5 Termination

If termination of an on-card biometric comparison application is supported, the on-card biometric reference pertaining only to such application shall be made inaccessible when it is terminated. A possible way is to set the biometric reference used by the terminated application as the logical erased state.

9 Security policies for on-card biometric comparison

9.1 Minimum security policies for on-card biometric comparison

9.1.1 General

This clause defines the minimum set of security policies for biometric comparison applications.

9.1.2 Minimum security policies

In all cases, the following minimum security policies apply:

a) The ICC shall not send out any biometric reference.

b) A retry counter mechanism shall be implemented according to 9.1.3.

c) In the message exchange, the integrity of data defined in 8.3 for on-card biometric comparison shall be assured. On top of the integrity mechanism provided by the transmission protocol, additional integrity mechanisms shall be added (e.g. the use of secure messaging for achieving integrity).

d) All biometric data shall be enciphered for transmission to the ICC unless the trusted environment is established to keep confidentiality.

e) If the ICC has a mechanism to block the on-card biometric comparison which is triggered by reasons other than the retry counter decrement (e.g. malicious attack detection), the unblocking mechanism should not recover the retry counter because the recovery will provide more biometric attempts to the attacker who has already compromised the unblocking mechanism.

f) In order to re-enrol the biometric reference, the security rules applicable shall be, at least, the equivalent ones as the ones that apply for the enrolment.

9.1.3 Retry counter management

9.1.3.1 General

A retry counter determines if the biometric reference is available to be used for biometric verification.

The following policies are applied:

a) there may be an independent retry counter for each biometric reference, with initial value associated with the biometric reference;

b) if the verification fails, the retry counter shall be decremented by one;

c) if the biometric verification is successful, the retry counter shall be reset;

d) if the retry counter reaches the maximum limit of retries, the biometric reference associated with the retry counter shall be blocked.

ISO/IEC 7816-4 defines key usage and retry counter DOs under key usage template DO'A3' within appropriate Control Parameter Reference Template DO and ISO/IEC 7816-4 maximum usage counter DO'94'and DO'95' and remaining usage counter DO'96' and DO'97' under security parameter template DO'AD' under control parameter data objects DO'62' for the ISO/IEC 7816-4 standard-conformant retry counter management implementation.

If the number of allowed retries is returned, it can be encoded in the status bytes SW1-SW2= '63CX' (where X is the remaining number of retries) of a response to a verification command, or a response to a VERIFY command where the data field is absent according to ISO/IEC 7816-4.

9.1.3.2 Resetting mechanism

The ICC operating system may have a mechanism to reset the retry counter of the on-card biometric comparison. For those cases where blocking of the on-card biometric comparison mechanism has occurred due to reaching the maximum limit of retries, the resetting process shall reset the retry counter. The specific implementation can additionally require a new enrolment.

9.2 Security policies for multiple on-card biometric comparison applications

9.2.1 Taxonomy of biometric comparison applications used in ICC

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

a) 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 the usage of one biometric reference by multiple applications. Applications using the on-card biometric comparison mechanism with such biometric reference shall not change the biometric comparison parameters independently.

b) In an ICC with multiple applications, on-card biometric comparison is used with a single set of biometric comparison parameters (e.g. same FMR grade).

NOTE 1 An ICC with single application can be a particular case, and therefore, SP1 (see 9.2.2) is applied.

c) Using application-specific biometric comparison parameters. This case includes the following situations.

1) Each application has its own biometric reference and related structure including biometric comparison parameters.

2) All applications only share the same biometric reference, but each application has its own biometric comparison parameters, which include for example the different FMR grades. In this case, any changes to biometric comparison parameters for one application shall not affect the ones for the other application.

NOTE 2 The terms “global” and “application-specific” are used in accordance with basic security handling in ISO/IEC 7816-4.

The following subclauses define the minimum security policies, SP1 (see 9.2.2), SP2 (see 9.2.3) and SP3 (see 9.2.4). Table 6 lists the data domain comparison among security policies.

Table 6 — Data domain comparison among security policies

	Biometric reference	Biometric comparison parameter	Retry counter
SP1	Shared Global	Shared Global	Shared Global
SP2	Shared Global	Each App has own copy	Each App has own copy
SP3	Each App has own copy	Each App has own copy	Each App has own copy

9.2.2 Security policy for universal verification mechanism (SP1)

For those applications where the biometric reference is to be used as a universal verification mechanism as shown in Figure 8, there is no need for several sets of biometric comparison parameters. To implement it, the following configuration is applied:

— A single set of biometric reference and retry counter is shared by multiple applications.

- A single set of biometric comparison parameters is shared by multiple applications.

For this configuration, the following security policy applies:

- None of the applications shall change the biometric comparison parameters independently unless it has a privilege.

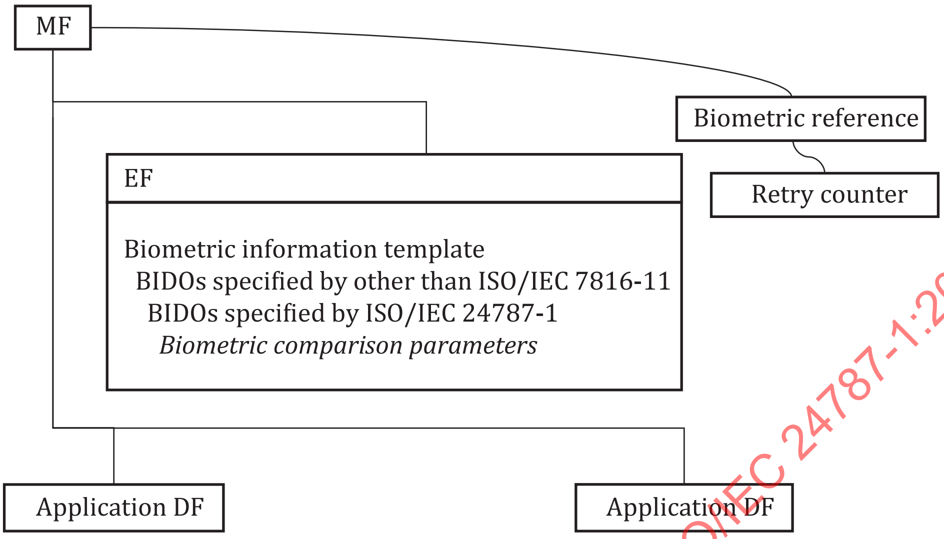

MF
Biometric reference
Retry counter
EF
Biometric information template
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric comparison parameters
Application DF
Application DF

Figure 8 — Using global biometric comparison parameters with shared biometric reference and retry counter

9.2.3 Security policy for shared biometric reference with independent verification mechanism (SP2)

In the case of an ICC the applications request an independent control of the on-card biometric comparison but share the same biometric reference as shown in Figure 9. To implement it, the following configuration is applied:

- A single set of biometric reference and retry counter is shared by multiple applications.
- Each application has its own set of biometric comparison parameters.

For this configuration, the following security policy applies:

- 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.

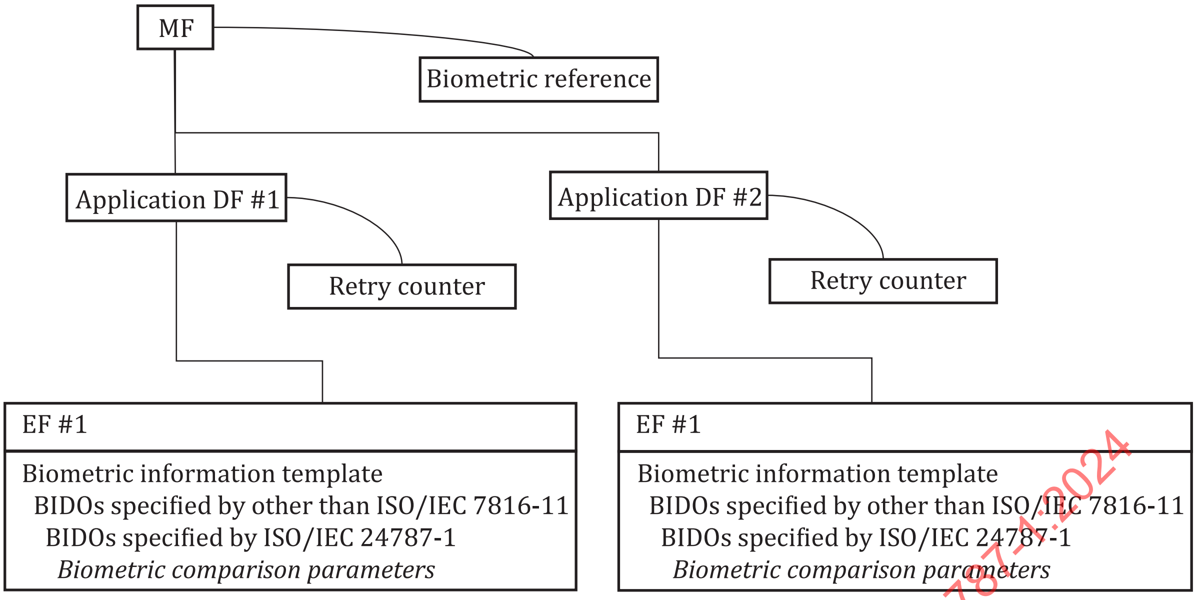

MF
Biometric reference
Application DF #1
Retry counter
Application DF #2
Retry counter
EF #1
Biometric information template
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric comparison parameters
EF #1
Biometric information template
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric comparison parameters

Figure 9 — Using application specific biometric comparison parameters with shared biometric reference and retry counter

9.2.4 Security policy for independent applications (SP3)

Figure 10 shows the security policy (SP3) using application specific biometric comparison parameters with different biometric reference and retry counter. In this case, each application can have its own security policy. The developer may reference 9.1 to implement the security policies to suit the requirements for the application.

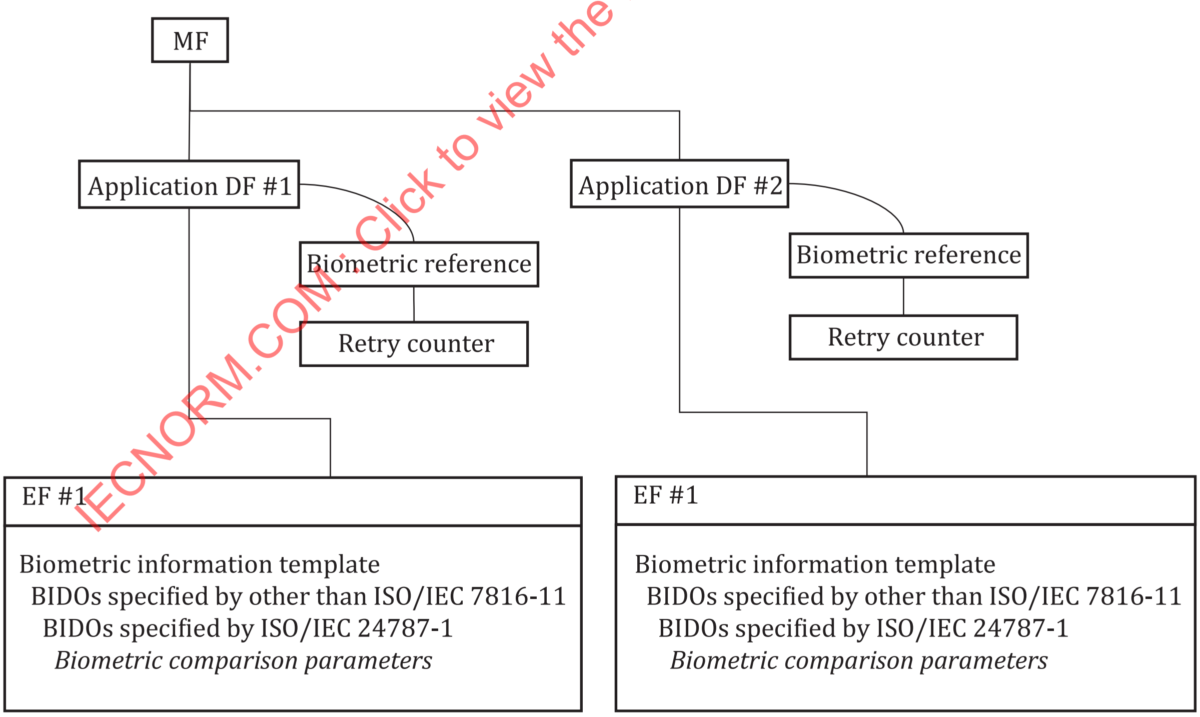

MF
Application DF #1
Biometric reference
Retry counter
Application DF #2
Biometric reference
Retry counter
EF #1
Biometric information template
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric comparison parameters
EF #1
Biometric information template
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric comparison parameters

Figure 10 — Using application-specific biometric comparison parameters with different biometric reference and retry counter

Annex A
(informative)

Sample APDU for on-card biometric comparison

Although PBO command is dedicated to performing biometric related operations, this annex provides another example of how to implement the on-card biometric comparison by a conventional command defined in ISO/IEC 7816-4. The VERIFY command is possible to send fingerprint minutiae data (i.e. biometric probe) to the ICC, which is structured as in Table A.1.

Table A.1 — Example of Command APDU structure for on-card biometric comparison

Field	Value
CLA	‘00’
INS	‘20’ or ‘21’[a]
P1	‘00’
P2	‘00’
Lc	Length of command data field. Where length < 255.
Data	Verification data [a]
Le	Absent

NOTE 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.

[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 can be implicitly known. The recommended way is to hold a biometric information template that can publicly be read out of 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 data template;

— ‘5F2E’ biometric data;

— ‘81’ or ‘A1’ biometric data with standardized format (primitive/constructed);

— ‘82’ or ‘A2’ biometric data with proprietary format (primitive/constructed).

If sending a minutiae data set with the standardized format to the ICC, the data field is encoded as in Table A.2.

Table A.2 — Example of structure for minutiae data with standardized format

<table>
<tr><th>Tag</th><th>Len</th><th colspan="3">Value</th></tr>
<tr><td rowspan="3">'7F2E’</td><td rowspan="3">Var</td><td colspan="3">Biometric data template</td></tr>
<tr><th>Tag</th><th>Len</th><th>Value</th></tr>
<tr><td>'81'</td><td>Var</td><td>Biometric data with standardized format (primitive)
Minutiae data set</td></tr>
<tr><td colspan="5">NOTE The reason for using the tag '7F2E' is because the value field contains biometric data as a data object. The 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 byte string.</td></tr>
</table>

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

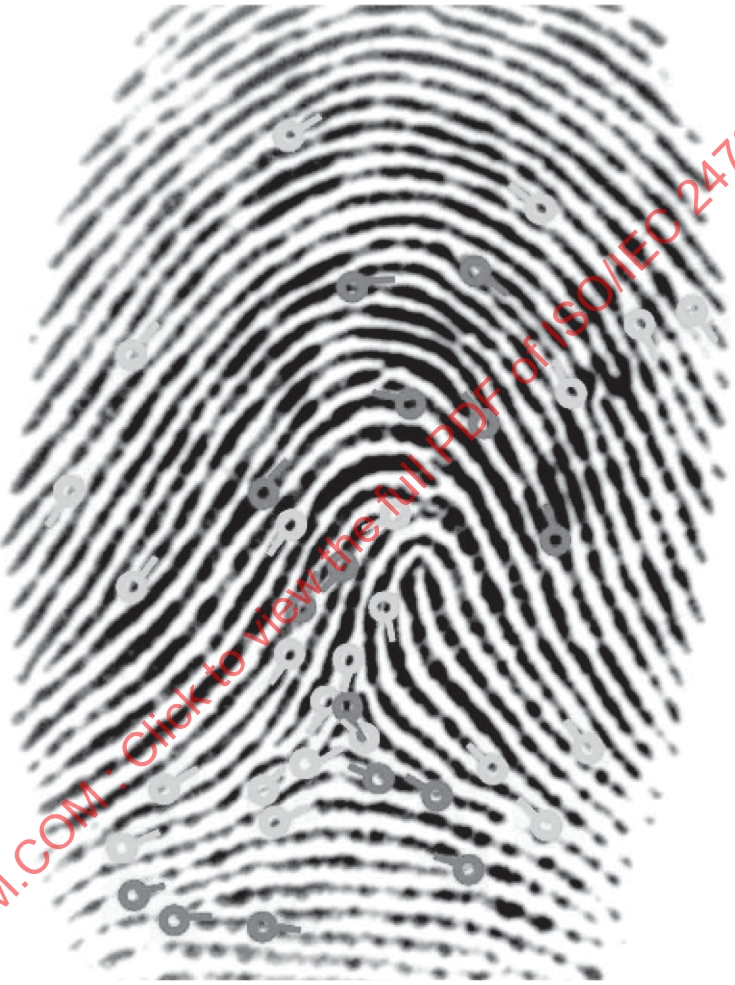


Figure A.1 — Fingerprint image with minutiae positions

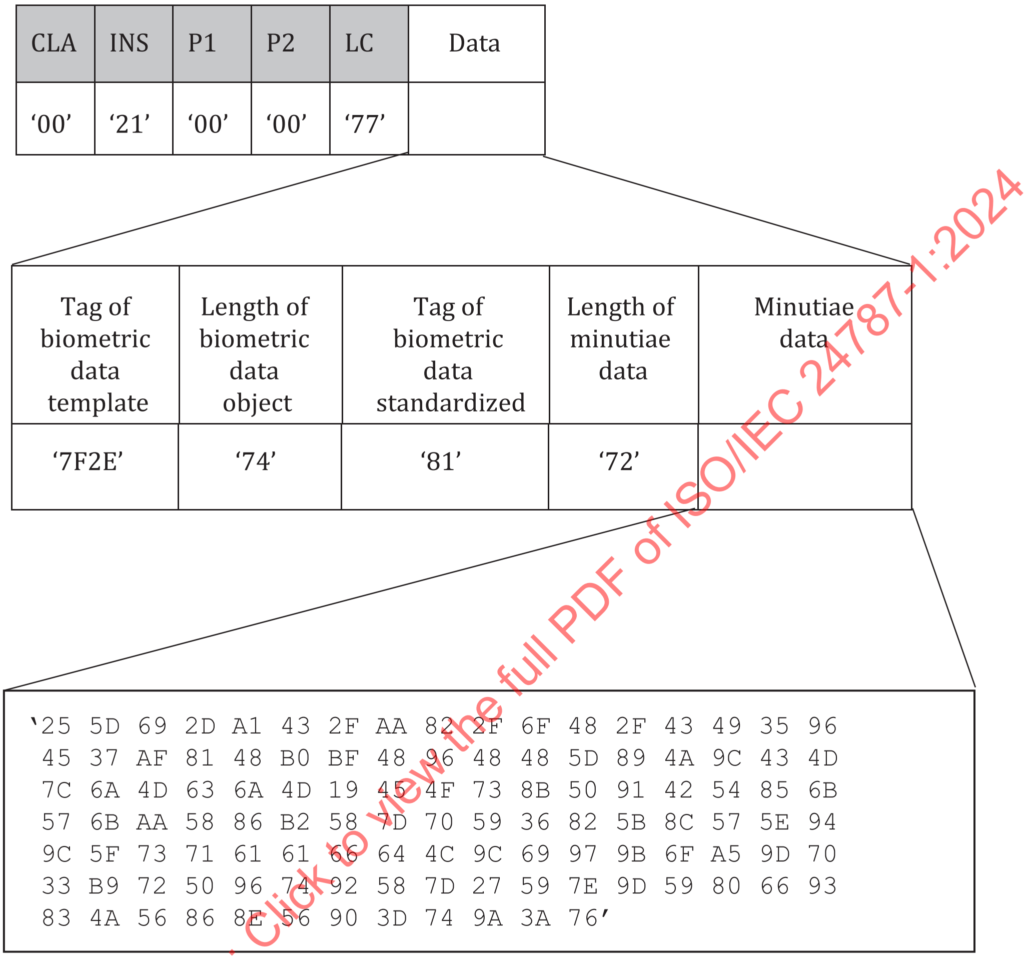
The minutiae are scaled to metric units and compressed into the compact card format for on-card biometric comparison use. This results in the following data (hexadecimal):

```
‘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 × 38 = 114 bytes, hexadecimal ‘72’.

The data added to the above structure results in the following command shown in Figure A.2.



CLA	INS	P1	P2	LC	Data
‘00’	‘21’	‘00’	‘00’	‘77’	

Tag of biometric data template	Length of biometric data object	Tag of 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 can 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.

The command messages written in this annex do not encipher the biometric data. These messages can be used in a trusted environment or in a secure messaging mechanism (e.g. ENVELOPE command) for confidentiality.

Annex B
(informative)

Example for implementation of global biometric reference

B.1 General

When "global biometric reference" (see ISO/IEC 7816-11) is adopted, an enrolled biometric reference can be registered immediately under the MF and such biometric reference is shared by multiple on-card biometric comparison applications under the MF. For this global biometric reference, the MF stores a biometric information template within an EF to introduce to an IFD about the detailed information of this biometric reference. The biometric information template provides a biometric functionality information of the global biometric reference (see Table 2).

According to the policy of such applications, biometric comparison parameters are stored in different places. This annex provides sample implementations of SP2 (see 9.2.3) to introduce useful methods of linkage from the application to a distant data element.

B.2 Generic structure for global biometric reference

The biometric reference under the MF is accessible globally from application DFs under the MF, and it is accessed by specifying a biometric reference qualifier that shows the link to this biometric reference as illustrated in Figure B.1.

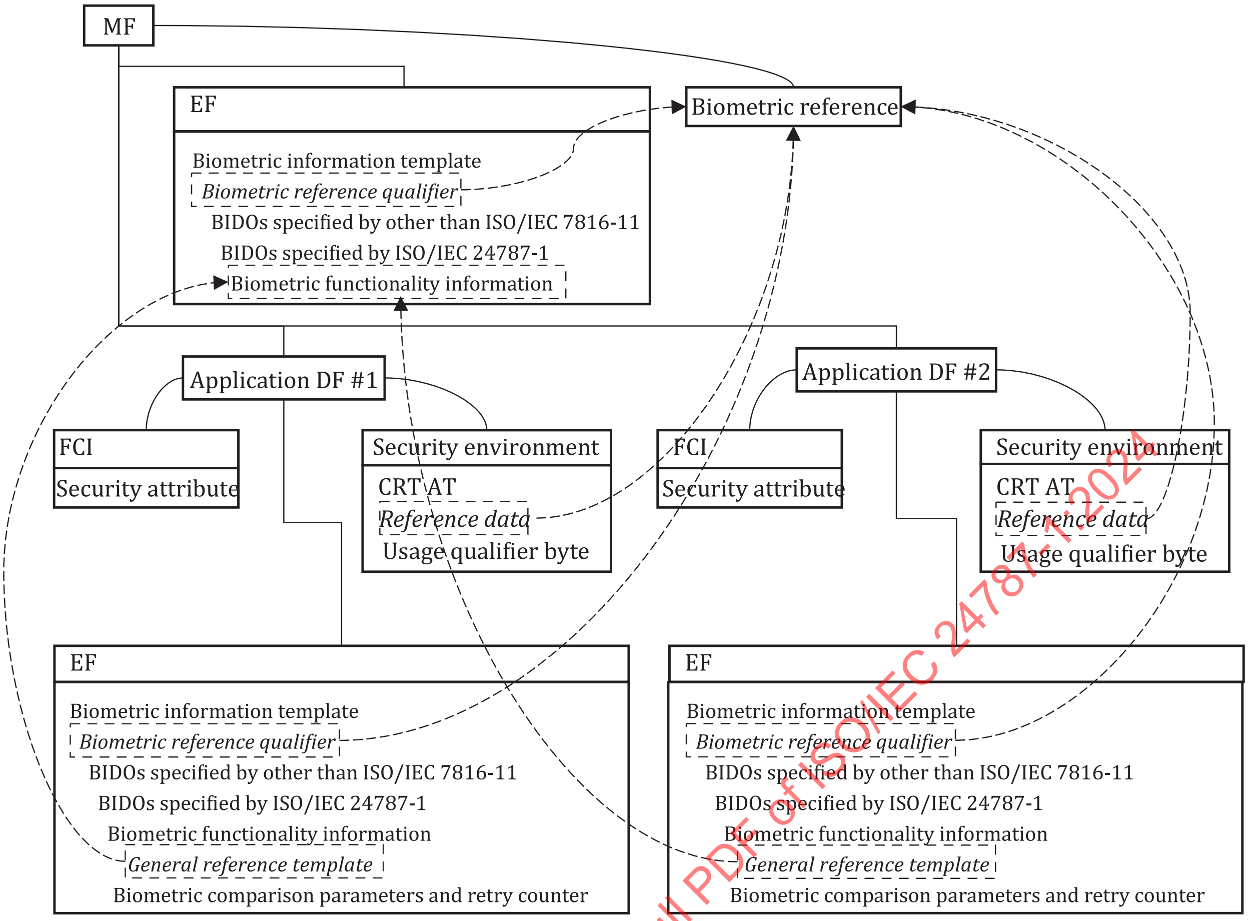

MF
EF
Biometric information template
Biometric reference qualifier
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric functionality information
Biometric reference
Application DF #1
FCI
Security attribute
Security environment
CRT AT
Reference data
Usage qualifier byte
Application DF #2
FCI
Security attribute
Security environment
CRT AT
Reference data
Usage qualifier byte
EF
Biometric information template
Biometric reference qualifier
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric functionality information
General reference template
Biometric comparison parameters and retry counter
EF
Biometric information template
Biometric reference qualifier
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric functionality information
General reference template
Biometric comparison parameters and retry counter

Figure B.1 — Example of generic structure for global biometric reference

Two application DFs are stored immediately under the MF, and each of the application DFs is hosting a different on-card biometric comparison application. When an IFD initiates one of the applications, the application DF is selected and a biometric information template is retrieved from its EF (see Table B.1).

The biometric information template provides a biometric reference qualifier that shows a link to the global biometric reference to where the biometric information template is based. The biometric information template also provides a biometric functionality information that holds a general reference template (see ISO/IEC 7816-4). This general reference template specifies the location of the actual biometric functionality information about the global biometric reference stored under the MF. Due to this location provided by an application DF, an IFD becomes possible to retrieve the actual biometric functionality information beforehand to prepare for biometric verification.

Table B.1 — Biometric information template for global biometric reference sharing

Tag	Len	Value								
'7F60'	Var	Biometric information template								
		Tag	Len	Value						
		'83'	1	Biometric reference qualifier						
		'A2'	Var	BIDOs specified by other than ISO/IEC 7816-11						
				Tag	Len	Value				
				'78'	9	Compatible tag allocation authority				
						Tag	Len	Value		
						'06'	7	OID of this document '28 81 C1 53 01 8F 68' (1.0.24787.1.2024)		
				Tag	Len	Value				
				'70'	Var	BIDOs specified in this document				
						Tag	Len	Value		
						'91' or 'B1'	Var	Biometric comparison parameters (Applied within application DF, see 8.3.3.3)		
						'92' or 'B2'	Var	Biometric functionality information (Applied within MF, see 8.3.3.2)		
						'B2'	Var	Biometric functionality information (Applied within application DF)		
								Tag	Len	Value
								'60'	Var	General reference template

Prior to the preparation, an IFD becomes aware that the biometric information template is the appropriate one to be evaluated by matching the biometric reference qualifier value with the one in CRT AT of the security environment, and also by checking the value of usage qualifier byte in CRT AT specifying "User authentication, biometry based (AT)" (see ISO/IEC 7816-4). The SEID where identifies the security environment (see ISO/IEC 7816-4) is provided as one of the security attributes from the FCI associated with an application DF.

B.3 Global biometric reference shared through file reference DO

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 the actual biometric data template which contains the biometric reference qualifier and biometric reference data.

Table B.2 indicates an example of the structure for a biometric information template.

Table B.2 — Example of biometric information template for global biometric reference shared through file reference DO

Tag	Len	Value			Note
‘7F60’	Var	Biometric information template			See ISO/IEC 7816-11
		Tag	Len	Value	
		‘A1’	Var	BIDOs specified by other than ISO/IEC 7816-11 BIDOs for CBEFF-3	Mandatory if any DOs specified in ISO/IEC 19785-3 are present
		Tag	Len	Value	
		‘A2’	Var	BIDOs specified by other than ISO/IEC 7816-11 BIDOs for this document	

Table B.2 *(continued)*

Tag	Len	Value							Note
				Tag	Len	Value			
				’78’	9	Compatible tag allocation authority			
						Tag	Len	Value	
						‘06’	7	‘28 81 C1 53 01 8F 68’	OID of this document (1.0.24787.1.2024)
				Tag	Len	Value			
				‘70’	Var	BIDOs specified in this document			
						Tag	Len	Value	
						‘91’ or ‘B1’	Var	Biometric comparison parameters	Where applicable (see Figure B.2)
						‘92’ or ‘B2’	Var	Biometric functionality information	Where applicable (see Figure B.2)
		Tag	Len	Value					
		‘7F2E’	Var	Biometric data template					
				Tag	Len	Value			
				‘51’	Var	File reference			Indicating the location of the file that stores the actual biometric reference

This example uses the file structure defined in ISO/IEC 7816-4 for hosting applications and storing application data. Figure B.2 illustrates an example of a file structure where one biometric reference is shared by two applications. The following is the overview of Figure B.2:

- The biometric reference is stored in the internal EF for protecting under the MF 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 dedicated files (DFs) 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 file control information (FCI) is provided to each EF storing the application-dependent biometric information template. The FCI associated to the EF may include security attributes. Security attributes can 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 file reference DO’51’ points to the actual biometric data template which contains the biometric reference qualifier and biometric reference data.

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

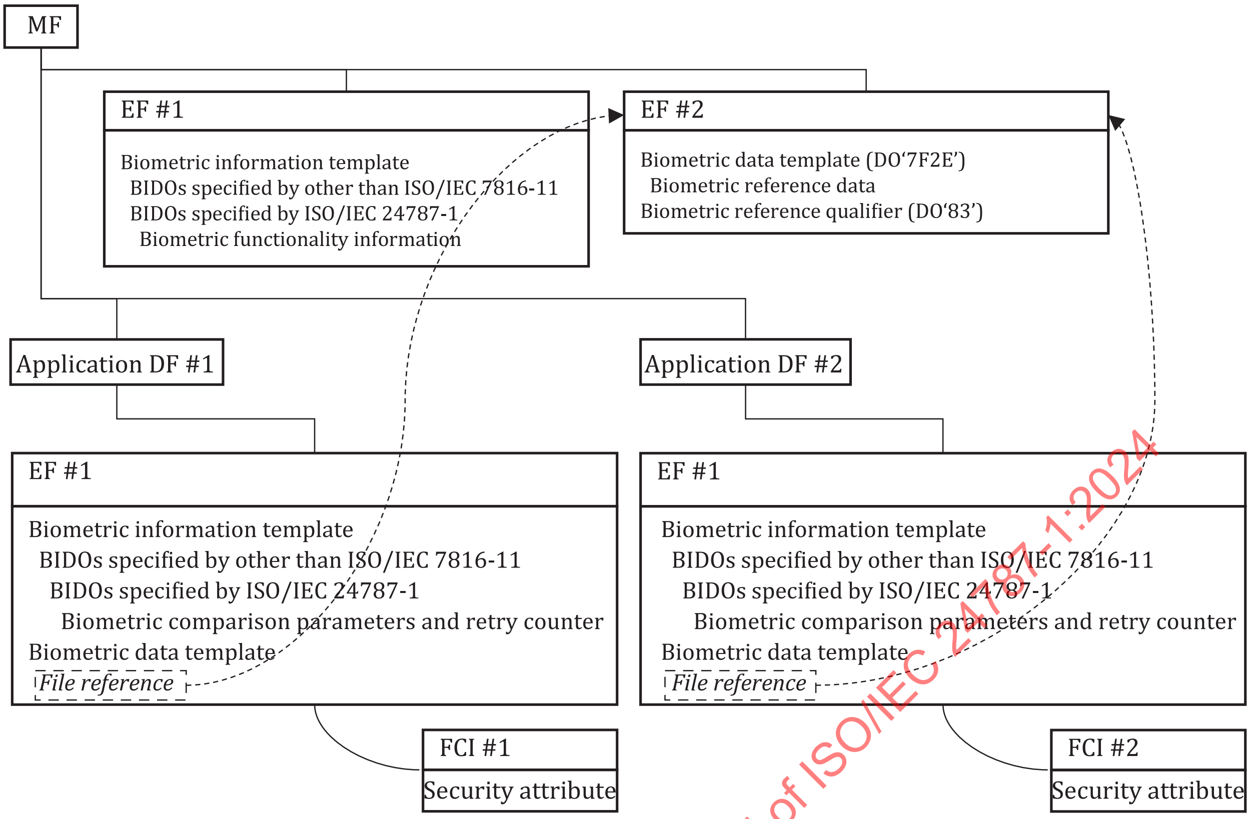

MF
EF #1
Biometric information template
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric functionality information
EF #2
Biometric data template (DO'7F2E')
Biometric reference data
Biometric reference qualifier (DO'83')
Application DF #1
Application DF #2
EF #1
Biometric information template
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric comparison parameters and retry counter
Biometric data template
File reference
EF #1
Biometric information template
BIDOs specified by other than ISO/IEC 7816-11
BIDOs specified by ISO/IEC 24787-1
Biometric comparison parameters and retry counter
Biometric data template
File reference
FCI #1
Security attribute
FCI #2
Security attribute

Figure B.2 — Example of structure for global reference-shared through file reference DO

Annex C
(informative)

Examples of security status transition model

C.1 General

This annex provides three examples of how to implement the on-card biometric comparison mechanisms related to the security status of the ICC. These examples are illustrated using state diagrams, where the circles refer to security statuses, and the arrows refer to operations and results from operations, both implying transitions among states.

The state is represented by "SX", where X=0 is the initial security status, and the larger the number, the more restrictive the security status is.

For simplicity in order to explain the examples, thresholds are used. A threshold is equivalent to a certain FMR grade. When a biometric comparison is done, the comparison score is compared to a certain threshold. If the following condition is fulfilled, a match is declared and the processing proceeds. Otherwise, the processing is not permitted.

$$C \geq T$$

where

C is comparison score;

T is threshold.

If the application in the ICC is using more than one threshold, T_1 and T_2 notation is used, where $T_2 > T_1$ and therefore, T_2 is more restrictive.

In all cases, no biometric verification is allowed if no secure channel between the ICC and the IFD is previously established and used in further operations.

C.2 Single application, homogeneous usage

The easiest example to start with is the use of a single application within the ICC, with a single verification level (single threshold). In Figure C.1 the overall workflow is represented. While basic operations that do not result in elevation of security status can be executed in the initial state S0, biometric verification is only performed when S1 is achieved by the establishing of a secure channel between the ICC and the IFD. Within S1, the cardholder can perform a `VERIFY` command. If a match is declared, S2 is achieved and allowed operations can be executed.

If the biometric verification is not successful, the retry counter for the biometric comparison is decremented in one unit, and if no further retries are allowed, no further biometric comparison can be executed.

In any case, if a security error is reported or an unauthorized operation is requested, the state is changed into the initial state S0 and a new secure channel between the ICC and the IFD should be established to proceed with restricted operations.