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.

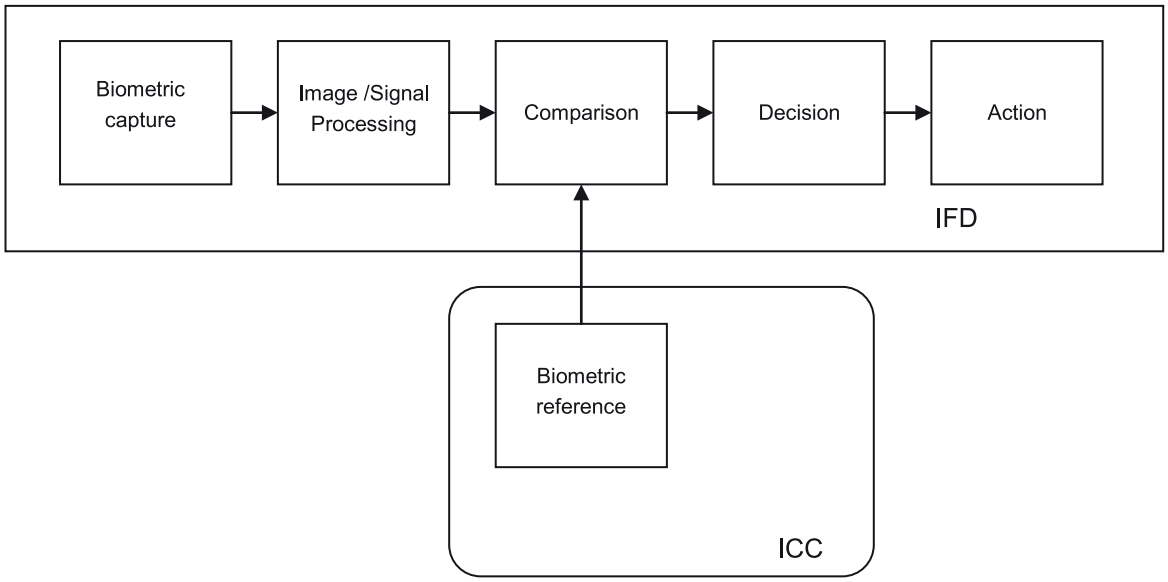

Figure 1 — General architecture for biometric verification using off-card biometric comparison

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.

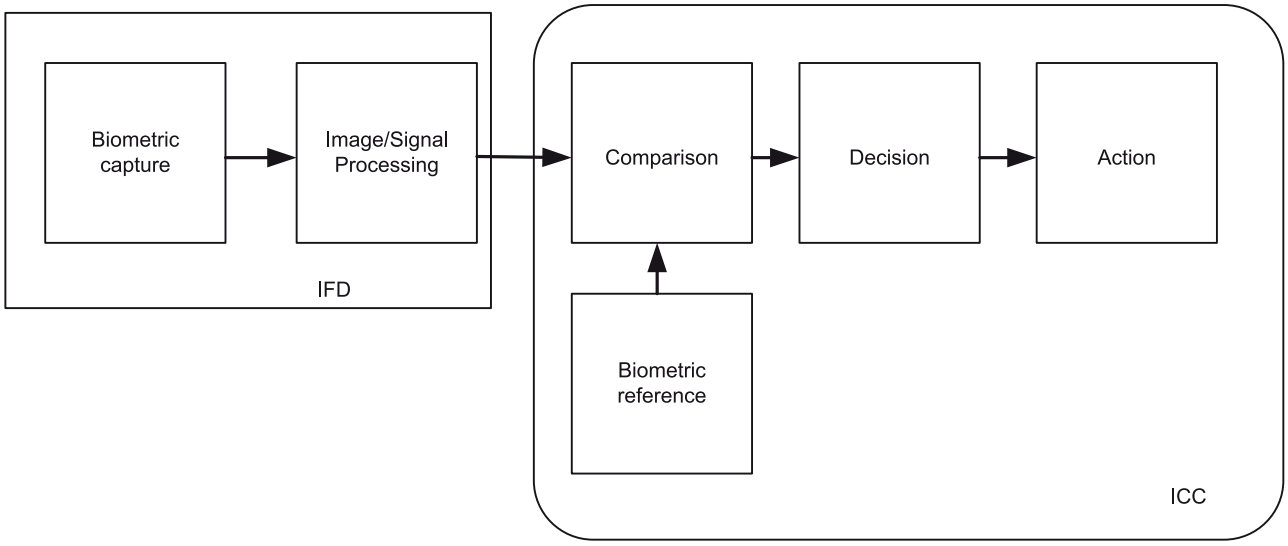

Figure 2 — General architecture for biometric verification using on-card biometric comparison

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.

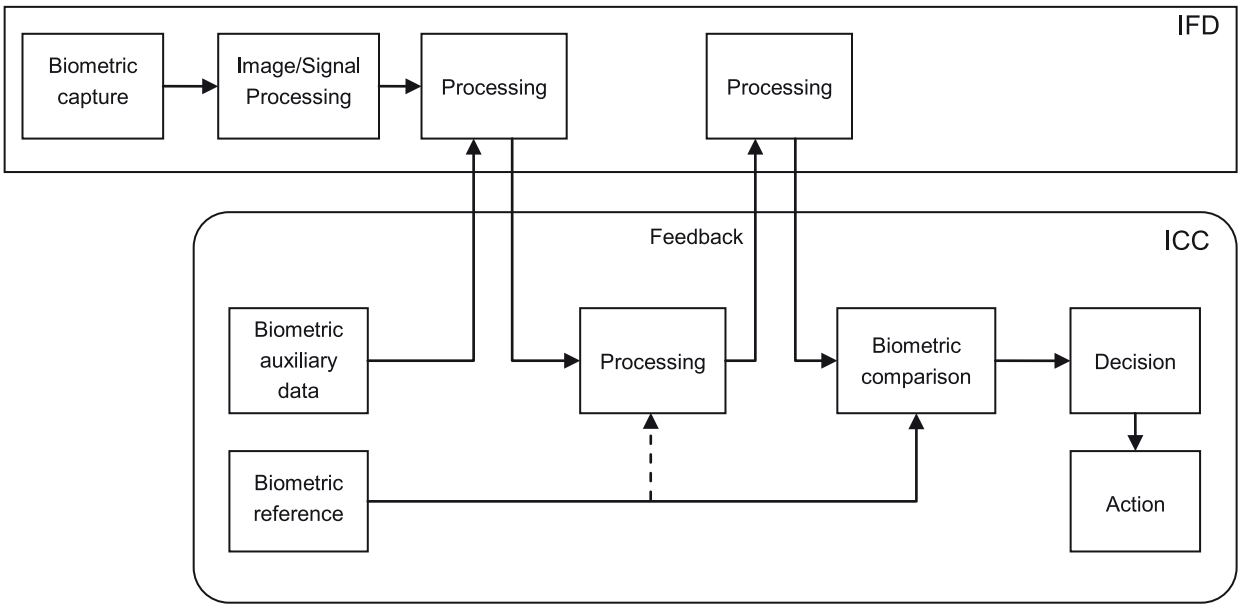

Figure 3 — Example of architecture for work-sharing on-card biometric comparison