FINAL DRAFT
International Standard

ISO/IEC
FDIS
24787-1

Information technology — On-card biometric comparison —

Part 1: General principles and specifications

ISO/IEC JTC **1**/SC **17**

Secretariat: **BSI**

Voting begins on:
2024-02-23

Voting terminates on:
2024-04-19

Reference number
ISO/IEC FDIS 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

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.

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[1)]), 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*

1) Under preparation. Stage at the time of publication: ISO/IEC FDIS 24787-2.

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.

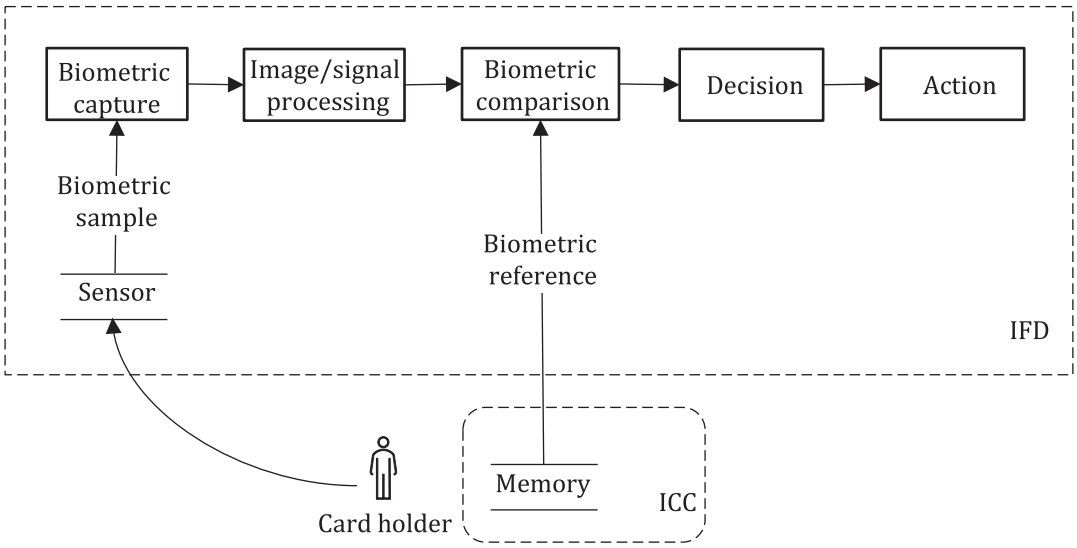

Figure 1 — General architecture of off-card biometric comparison

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.

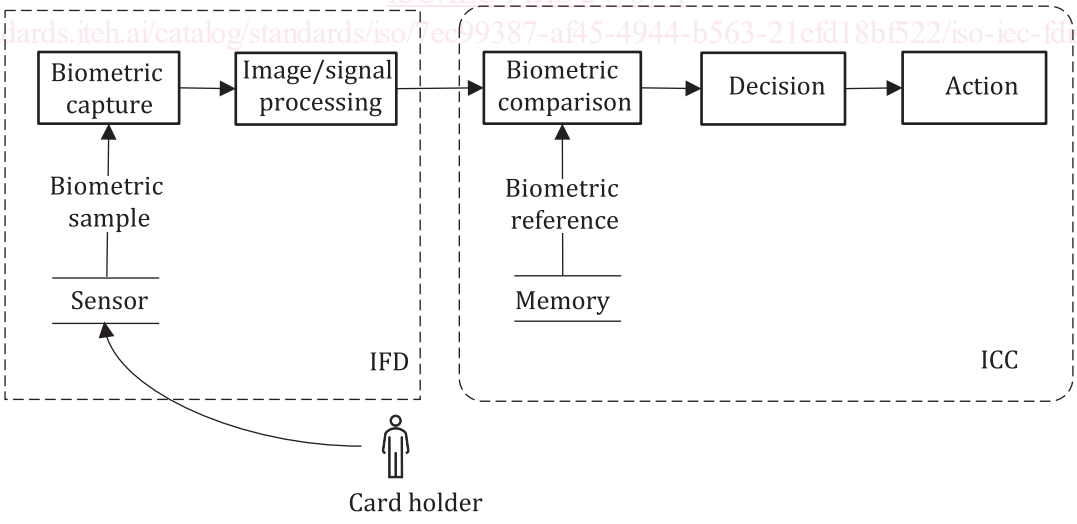

Figure 2 — General architecture of on-card biometric comparison (sensor-off-card)

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