INTERNATIONAL STANDARD

**ISO/IEC 18584**

First edition
2015-11-15

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

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



Reference number
ISO/IEC 18584:2015(E)

## COPYRIGHT PROTECTED DOCUMENT



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

# Contents

Page

# Foreword

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

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

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

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

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

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



 

# Introduction

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

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

## 1 Scope

This International Standard establishes

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

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

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

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

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



## 2 Normative references

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

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

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

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

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

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

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

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

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

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

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

## 3 Terms and definitions

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

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

EXAMPLE Data such as orientation, scaling, etc.

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

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

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

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

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

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

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

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

**3.6**
**biometric data format**
structure for representing biometric data

**3.7**
**biometric Information Template**
descriptive information regarding the associated biometric data

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

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

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

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

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

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



 

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 4 Abbreviated terms

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