INTERNATIONAL STANDARD

ISO/IEC 24787

First edition
2010-12-15

Information technology — Identification cards — On-card biometric comparison

Technologies de l'information — Cartes d'identification — Comparaison biométrique sur cartes

Reference number
ISO/IEC 24787:2010(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

ISO/IEC 24787 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

Introduction

On-card biometric comparison, also known as *on-card matching* in ISO/IEC 7816-11:2004, is one privacy-enhanced solution employing integrated circuit cards (ICCs) and biometric technologies, and provides a more secure biometric authentication in that the biometric comparison process is executed inside the ICC. In contrast with off-card comparison (*off-card matching*), on-card comparison does not need the biometric reference data in the ICC to be transferred to interface devices. Therefore, even if the ICC is lost or stolen, the biometric reference data stored on the ICC cannot be copied and remains private.

ISO/IEC 7816-11 and ISO/IEC 19785-3 cover technologies concerning off-card comparison and simple on-card comparison. Most robust biometric comparison processes using biometric samples acquired in the "real" world require high computational intensity. In contrast, CPU performance and other resources available on the ICC progress more slowly because requirements for low power consumption, small geometry of the chip, demand of low-cost cards and so on are obstacles to their more rapid advancement. Biometric sensors embedded onto the ICCs are still presenting technical challenges.

As a result of these circumstances, industry requires a new International Standard for on-card comparison excluding off-card and system-on-card comparison. This International Standard specifies the requirements of and provides recommendations for the following:

— architectural description of on-card comparison processes;

— architectural description of work-sharing on-card comparison process that can reduce the work-load on the ICCs by pre-processing computation;

— management of threshold values and other security issues for on-card comparison.

The International Organization for Standardization (ISO) and 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 8.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the 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 International Standard establishes

— requirements for performing comparisons of biometric samples and returning decisions on an integrated circuit card, and

— security policies for on-card biometric comparison

It also establishes commands and rules to permit pre-comparison computations to be done off-card.

This International Standard does not establish

— requirements for off-card comparison implementations,

— requirements for system-on-card implementations, or

— modality-specific requirements for storage and comparison.

2 Conformance

An on-card comparison system claiming conformance to this International Standard shall conform to the requirements of 7.1.2 to 7.1.5, 7.2.1 to 7.2.8, 8.1, and 8.2.2 to 8.2.3, as applicable.

A card conforming to this International Standard shall

1. Be personalized with two sets of data:

   Biometric reference object handling data, as described in 7.1.2

   Configuration data for biometric verification, as described in 7.1.3

2. Support a shared interface for ICCs with multiple applications, as described in 7.1.4

3. Support retry counter management, as described in 7.1.5

4. Comply with the requirements set forth in 7.2.1 and 7.2.8 for on-card comparison implementations

5. Comply with the requirements set forth in 8.1, 8.2.2. and 8.2.3 for work-sharing implementations.

Biometric authentication might coexist with other authentication mechanisms, such as PIN. The rules for such coexistence shall comply with ISO/IEC 7816-4:2005.

The biometric data shall be organized and managed using either a file structure or data objects as per ISO/IEC 7816-4.

a) If the biometric data is organized as a file structure then the system shall also be fully compliant with the provisions in ISO/IEC 7816-11.

b) If the biometric data are organized and managed as data objects then the card shall comply with the provisions in ISO/IEC 7816-4 for data object handling.

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

3 Normative references

The following referenced documents are indispensable for the application 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 7816-4:2005, *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 19785-1, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

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

4 Terms and definitions

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

4.1
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.

4.2
biometric, adj.
of or having to do with biometrics

[SC37 SD2 *Harmonised biometric vocabulary*]

NOTE "biometric" is never used as a noun.

4.3
biometrics
automated recognition of individuals based on their behavioral and biological characteristics

[SC37 SD2 *Harmonised biometric vocabulary*]

4.4
biometric claim
claim that a biometric capture subject is or is not the bodily source of a specified or unspecified biometric reference

[SC37 SD2 *Harmonised biometric vocabulary*]

4.5
biometric data
biometric sample or aggregations of biometric samples at any stage of processing, biometric reference, biometric feature or biometric property

[SC37 SD2 *Harmonised biometric vocabulary*]

4.6
biometric data format
structure for representing biometric data

4.7
biometric Information template
descriptive information regarding the associated biometric data

[ISO/IEC 7816-11:2004]

4.8
biometric product identifier
unique identifier registered with the registration authority in accordance with ISO/IEC 19785-1

4.9
biometric property
descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means

[SC37 SD2 *Harmonised biometric vocabulary*]

4.10
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison

[SC37 SD2 *Harmonised biometric vocabulary*]

4.11
biometric verification system
system that aims to perform the process of confirming a biometric claim

[SC37 SD2 *Harmonised biometric vocabulary*]

4.12
installation
writing of the required parameters into the non-volatile memory inside an integrated circuit card (ICC) by the card OS executing the installation procedure after the application has been uploaded to the ICC

4.13
on-card comparison
performing comparison and decision making on an integrated circuit card where the biometric reference data is retained on-card in order to enhance security and privacy

4.14
off-card comparison
biometric comparison performed outside the card by the biometric verification system against the biometric reference data stored on the card

4.15
pre-comparison computation
computation procedure executed outside the ICC that requires the (open) on-card auxiliary data to compute metadata that can be used to speed up the subsequent on-card biometric data comparison process

4.16
work-sharing
splitting the computational work load of the comparison process between the card and the biometric interfacing device

NOTE Work-sharing on-card comparison is one type of on-card comparison.

4.17
system-on-card
complete biometric verification system on a card, including data acquisition, processing and comparison

NOTE System-on-card comparison is one type of on-card comparison.

4.18
zeroize data
electronically stored data that have been degaussed, erased, or over-written

[ANSI X9.17]

5 Abbreviated terms

AID	application identifier
ADF	application dedicated file
APDU	application protocol data unit
AUT	authenticate
BER	basic encoding rules
BIT	biometric information template
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

ICC	integrated circuit card
MAC	message authentication code
MSE	manage security environment
RFU	reserved for future use
SW1-SW2	status bytes
TLV	tag length value
WSCP	work-sharing computation protocol
WSR	work-sharing request

6 Architecture of biometric matching using an ICC

6.1 General

The following subclauses details, for the purposes of illustration, four methods for allocating the biometric matching functionality between an ISO/IEC 7816 conformant card and the biometric verification system. Only 6.3 and 6.4 are within the scope of this standard.

To perform enrolment, the biometric sample from the user is captured for biometric reference creation, then the user's information are uploaded to the card. This does not apply to system-on-card comparison as specified in 6.5.

6.2 Off-card comparison

Off-card comparison means the biometric verification is performed on the biometric verification system side. The card acts as a storage device to store the biometric reference(s) of the user. Figure 1 provides a schematic of the various process steps.

To perform verification, the biometric verification system will obtain access to the ICC and read the user's biometric reference. The role of the biometric verification system is to capture the biometric sample and to perform biometric verification. If the biometric verification is successful, the biometric verification system will change its security status. This may include downloading further information from the card for a subsequent transaction. If unsuccessful, further access will be denied.

Cryptography is usually used to mutually authenticate the card and the biometric verification system. To protect the communication between the biometric verification system and the card, a secure channel should be established prior to the transfer of any template or data.

EXAMPLE Consider a physical access system where the biometric reference and access code is stored on the ICC. The biometric verification system reads the biometric reference from the card, and performs biometric verification. In case of successful verification, it reads the access code from the card and sends it to the back end system that opens the door.

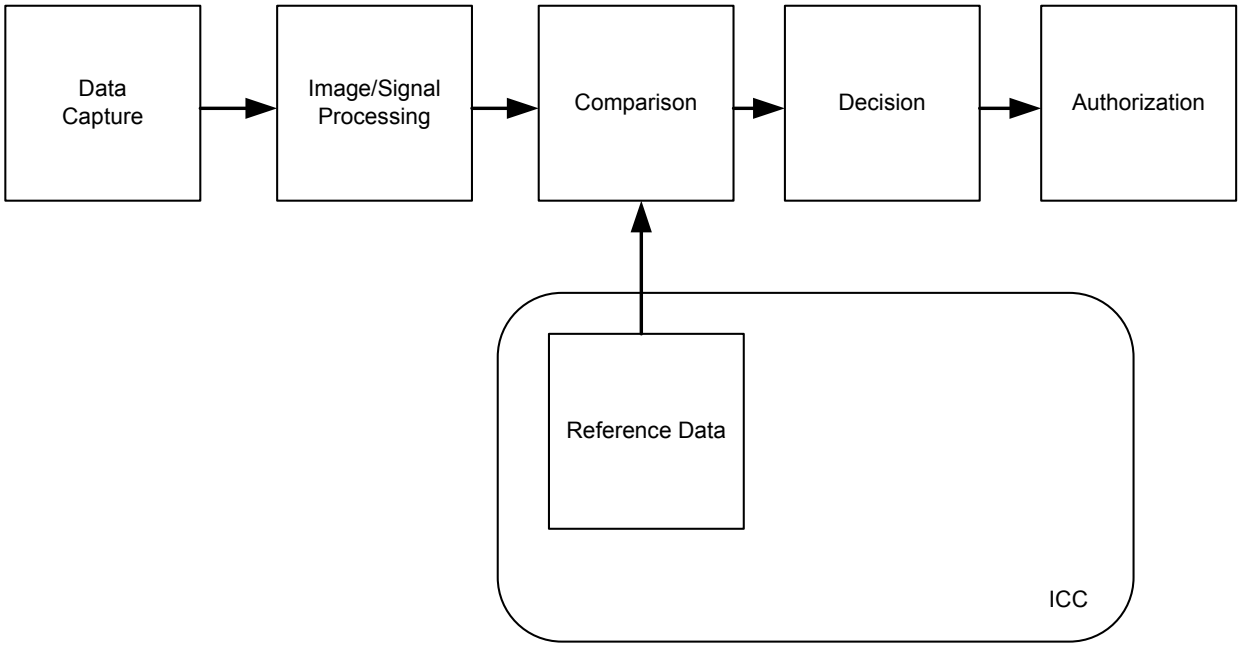

Figure 1 — General architecture for biometric authentication using off-card matching

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

On-card comparison means the biometric sample verification is performed in the card. The process is schematically represented in Figure 2. The ICC CPU should have sufficient processing power to perform the matching. The enrolment process is the same as or similar to that for off-card matching.

To perform on-card comparison, the biometric verification system captures the biometric sample and extracts biometric data. The created biometric data is then uploaded to the card for verification. The verification process is executed on-card. If the biometric verification is successful the card's security state is updated and an appropriate signal sent to the back-end system.

In order to protect the communication between the biometric verification system and the card, a secure and trusted channel is recommended (using Secure Messaging according to ISO/IEC 7816 and mechanisms defined by ISO/IEC 24761 for distributed comparison verification).

EXAMPLE Consider a card with the ability to create digital signatures using a key that never leaves the card. A request sent to the card to initiate the creation of a digital signature receives a response message of security status error. This indicates to the user that verification is required. The user presents the required biometric sample to the biometric verification system for creation of biometric data, which is transmitted to the ICC. The ICC then compares the newly captured biometric data with the stored biometric reference, and in case of successful comparison, ICC updates the security status that subsequently allows the ICC to create digital signature upon receiving the corresponding APDU commands.

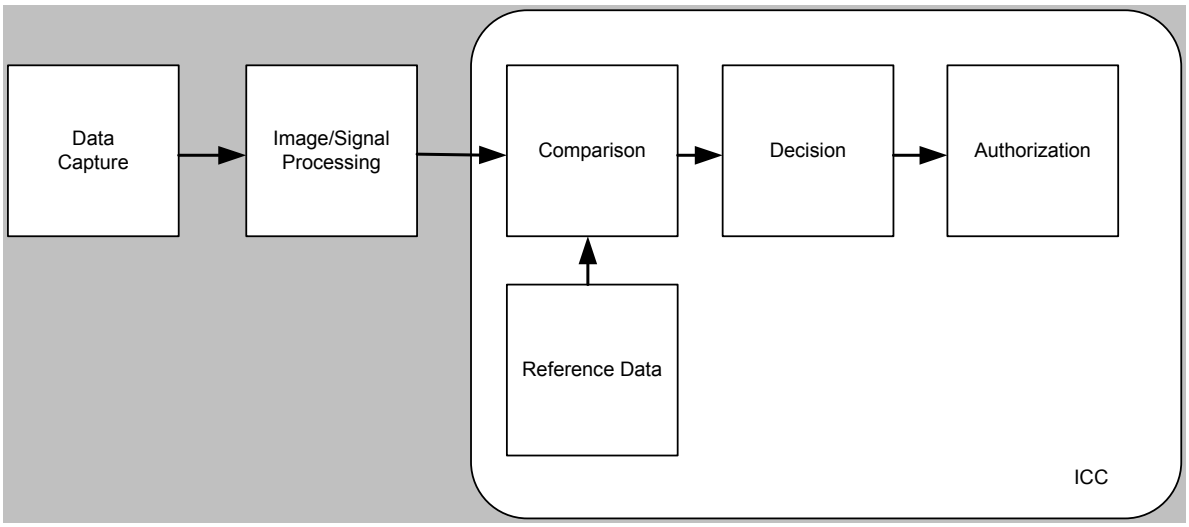

Figure 2 — General architecture for biometric authentication using on-card matching

6.4 Work-sharing on-card comparison

Work-sharing on-card comparison is similar to on-card comparison except for the comparison procedure. The process is schematically represented in Figure 3. This type of comparison is designed for an ICC that does not have sufficient processing capability to execute the biometric data comparison. In this case, certain activities that are computationally intensive, for example, a mathematical transformation, are sent to the biometric verification system to perform the calculation. The result of the computation is sent back to the ICC so that the final determination of the matching score is calculated on the card. During the pre-comparison calculation, communication takes place between the card and the biometric verification system. A secure and trusted channel is used to protect the communication between the terminal and the card unless the need for such protection is explicitly not required for a particular operational environment. The final comparison shall be performed in the card. A detailed description of the work-sharing architecture is given in Annex D.

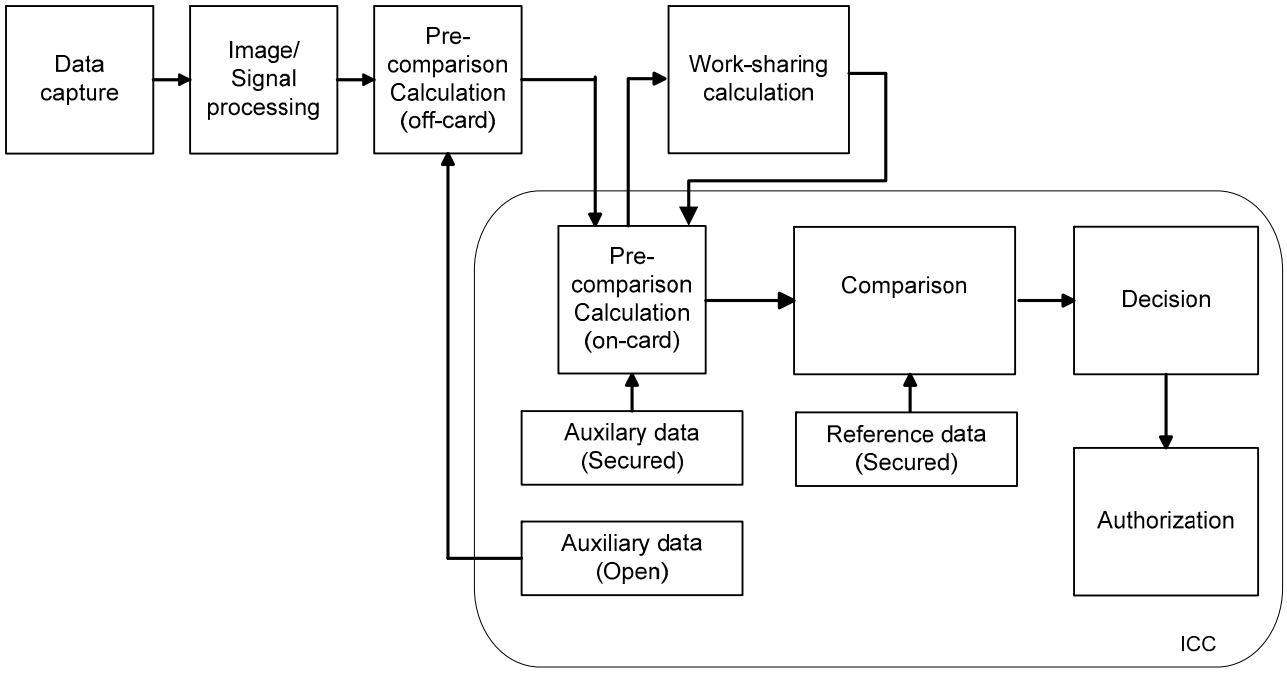

Figure 3 — General architecture for biometric authentication using work-sharing