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.

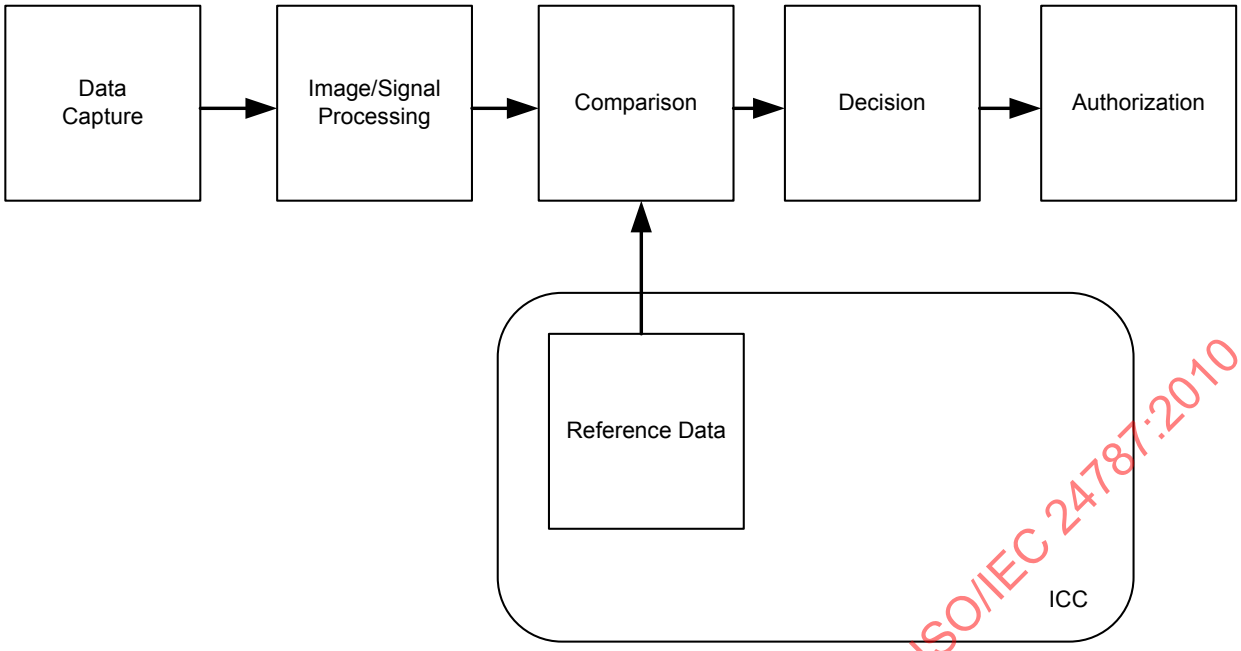


**Figure 1 — General architecture for biometric authentication using off-card matching**

## 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.

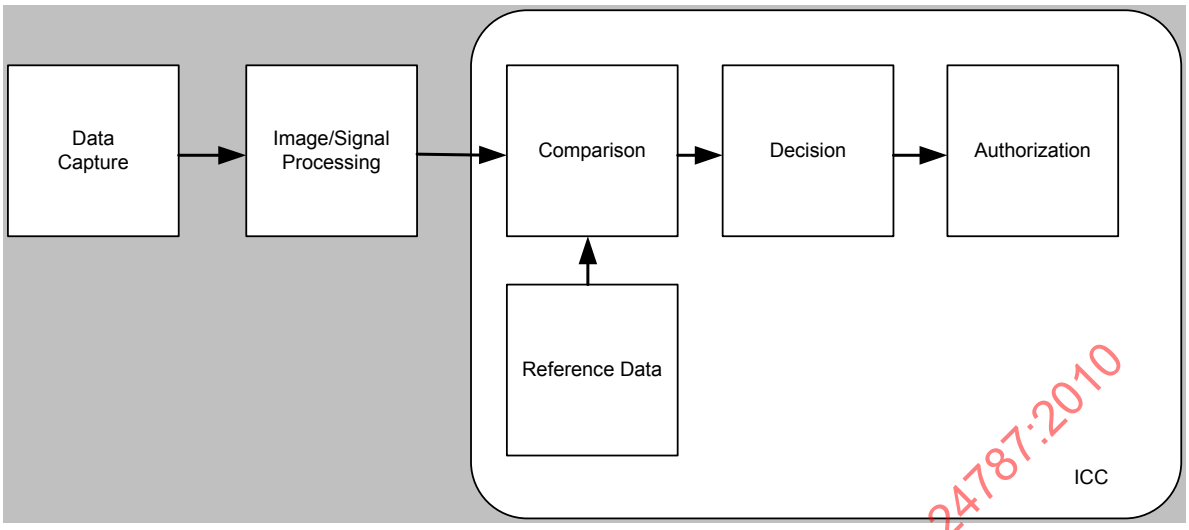


**Figure 2 — General architecture for biometric authentication using on-card matching**

## 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.

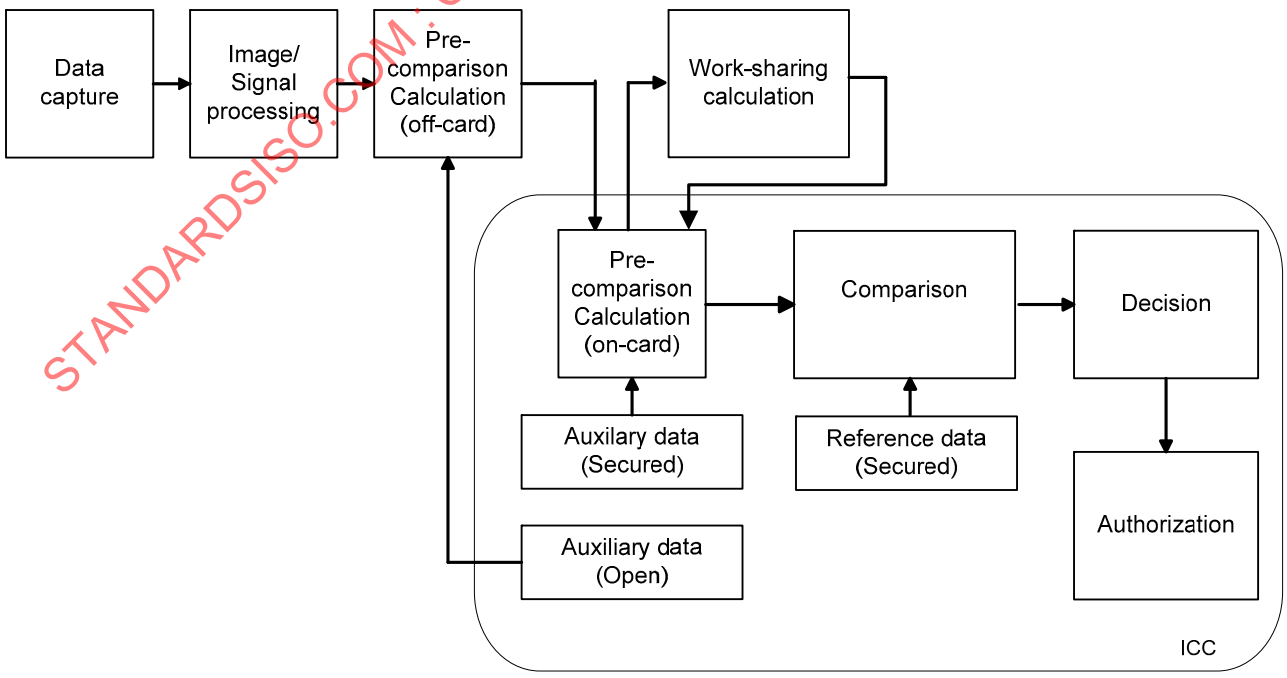


**Figure 3 — General architecture for biometric authentication using work-sharing**

NOTE Work-Sharing on-card comparison should only be considered when, with the biometric modality used, the performances of the on-card comparison process are not good enough with regards the required transaction time for a given application.

### 6.5 System-on-card comparison

System-on-card comparison means the whole biometric sample verification process is performed on the card. The process is schematically represented in Figure 4. To perform sensor-on-card comparison, a sensor that is built into the card captures the biometric sample and extracts biometric data. The created biometric data is then used for verification. The verification process is executed on-card. The card's security state is updated once the card finishes the verification. No biometric sample or reference data is transferred to or from the card.

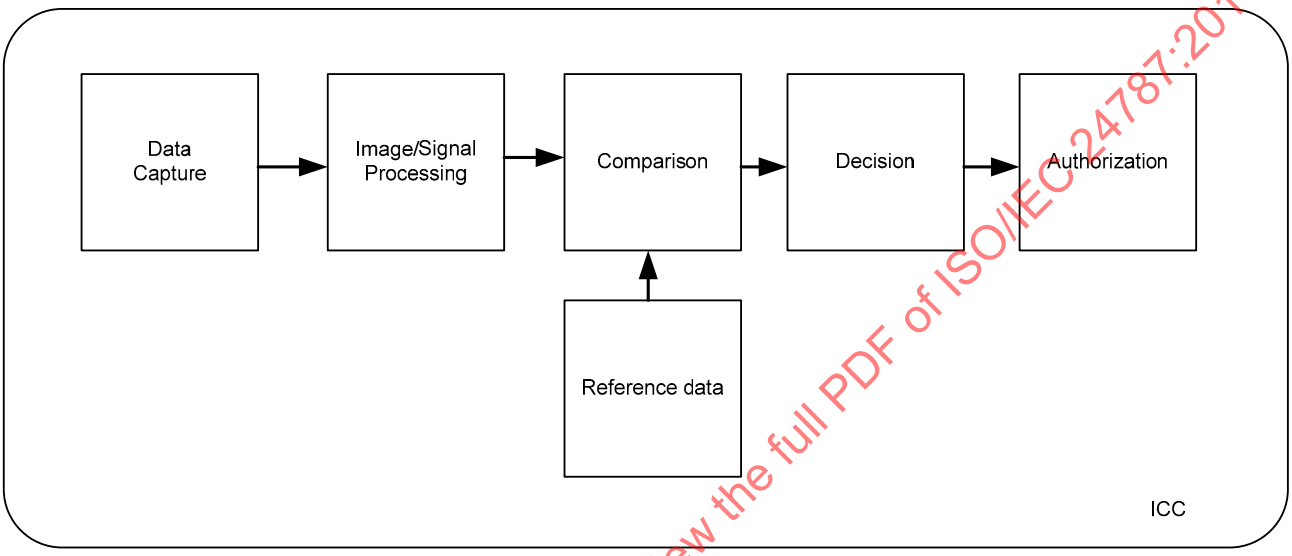


**Figure 4 — General architecture for biometric authentication using system-on-card matching**



## 7 General framework for on-card comparison applications

### 7.1 Data for on-card comparison

#### 7.1.1 General

Subclauses 7.1.2 to 7.1.5 specify the following features:

1) Biometric reference object handling
2) Configuration data for biometric verification
3) Shared interface for multiple applications
4) Retry counter management

#### 7.1.2 Biometric reference object handling

For reason of biometric reference interoperability, on-card comparison shall use the biometric data format as defined in the relevant part of ISO/IEC 19794 series. An example is provided in Annex C.

Unless the need for biometric reference interoperability is explicitly not required for a particular operational environment, then biometric data formats, as defined in the relevant part of the ISO/IEC 19794 series shall be used.

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

### 7.1.3 Configuration data for biometric verification

#### 7.1.3.1 Data objects for configuration data

The configuration data for biometric verification consists of a set of data objects described in Table 1. Retrieval of configuration data shall be subject to the access rules associated with the logical data structures that store this information. If configuration data is available, it shall be stored into the BIT (ISO/IEC 7816-11). This configuration data shall be coded when present, within the 'B1' tag of BIT (see ISO/IEC 7816-11:2004), as shown in Table 1.

**Table 1: Data objects for configuration data elements**

| Tag | Length | Valid values | Description |
|---|---|---|---|
| ‘80’ | ‘01’ to ‘03’ | | Maximum size of biometric verification data |
| '81’ | ‘01’ to ‘03’ | | Maximum size of the biometric reference data |
| ‘82’ | 1 | '00' – 'FF' | Supported number of biometric templates ('00' – no information given) |
| ‘83’ | 1 | '00': No re-enrolment possible<br>‘01’: Re-enrolment possible<br>Other values: RFU | Flag indicating the possibility of re-enrolment |
| ‘85’ | Var | As defined in ISO/IEC 29794-1 | Minimum verification data quality supported as defined in the relevant parts of the ISO/IEC 19794 and ISO/IEC 29794 series of standards. |
| ‘86’ | 1 | | Initial value of the retry counter, indicating the supported maximum number of permitted verification attempts |
| ‘87’ | Var | | Internal quality restrictions for performing the comparison |
| '8F' | Var | | Proprietary data |
| ‘90’ | Var | see Table 5 | Types of biometric authentication and, if applicable, performance of the card |
| ‘A4’ | 2 | As defined by the registration authority described in ISO/IEC 19785-2 | Reserve for future use, Algorithm ID as defined by SC 37 |



NOTE The encoding of other configuration parameters such as:

- required security status to perform biometric verification;
- required security status to perform biometric enrolment;
- the security status set after positive verification

is out of the scope of this standard.

#### 7.1.3.2 Biometric comparison algorithm parameters

Prior to biometric verification, a set of biometric comparison parameters should be read from the card. Tables 2 and 3 define biometric comparison algorithm parameters in the BIT for on-card comparison (tag '91'/'B1' in ISO/IEC 19785-3:2007, Table 11.1), where primitive parameters are headed by tag '91', and constructed parameters are headed by tag 'B1' and include total length.

**Table 2: Data objects for biometric comparison algorithm parameters**

| Tag | Length | Valid values | Description |
|---|---|---|---|
| '81' | * | * | Minimum and maximum length of biometric data as defined in the relevant part of the ISO/IEC 19794 series of standards. |
| '82' | * | * | Ordering, if applicable, of the features in the biometric data as defined in the relevant part of the ISO/IEC 19794 series of standards. |
| '83' | * | * | Biometric data handling information as defined in the relevant part of the ISO/IEC 19794 series of standards. |
| '84' | * | * | Alignment information as defined in the relevant part of the ISO/IEC 19794 series of standards. |
| '85' | ** | ** | Minimum verification data quality supported (See Table 1) |
| '90' | 1 | see Table 5 | Authentication type and algorithm strength |
| '91' | 2 | '0001' – 'FFFF' | Maximum response time in milli-seconds[1] |

NOTE 1 "*" denotes that this variable is defined in the relevant part of ISO/IEC 19794 series of standards.

NOTE 2 "**" denotes that this variable is defined in the relevant parts of the ISO/IEC 19794 and ISO/IEC 29794 series of standards.

On-card comparison may require access rules to be fulfilled, including any security channel to protect the transmission of APDU Commands and Responses, required for the completion of the process. The Data Field of these APDU convey biometric related data to/out of the card shall be encoded as specified in this standard. The access rules and the secure messaging used to protect APDUs shall comply with ISO/IEC 7816-4.



[1] A card performing a time-consuming operation has to support proper waiting time extensions according to ISO/IEC 7816-3.

**Table 3: Authentication type and discriminative power**

| b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 | Meaning |
|---|---|---|---|---|---|---|---|---|
| | | | | | | x | x | Authentication type |
| | | | | | | 0 | 0 | Comparison on-card |
| | | | | | | 0 | 1 | Work sharing comparison on-card |
| | | | | | | 1 | 0 | System-on-card |
| | | | | | | 1 | 1 | RFU |
| | | | x | x | x | | | FMR[2] 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 manufacturer shall declare the FMR value for their stated grading. Table 4 is an example of a FMR grading scale.

**Table 4: Example for FMR grading**

| | |
|---|---|
| FMR grade 1 | FMR < 0.1 |
| FMR grade 2 | FMR < 0.01 |
| FMR grade 3 | FMR < 0.001 |
| FMR grade 4 | FMR < 0.0001 |
| FMR grade 5 | FMR < 0.00001 |
| FMR grade 6 | FMR < 0.000001 |



#### 7.1.3.3 Biometric product identifier

Biometric product identifier shall be an integer within the range 1 to 65535 and shall be registered with the registration authority in accordance with ISO/IEC 19785-1.

### 7.1.4 Shared interface for multiple applications

#### 7.1.4.1 General

A possible requirement in an interoperable on-card comparison system is to use one single biometric reference, for example, a minutiae template, in different applications using different configuration data. This requirement is implemented with the use of access rules references and data elements as defined in ISO/IEC 7816 and other biometrics-related standards for sharing information among independent applications.

---

[2] This value is provided to enable the system designer to set different comparison levels for different applications with the specific on-card comparison product.

#### 7.1.4.1.1 Comparison information

A biometric on-card comparison system might require additional parameters, for example:

- Pointer to the biometric reference
- Comparison parameters, for example:
  - Template format
  - Algorithm to be used
  - Threshold parameters

The maximal score of the comparison can be determined or the comparison return can return positive result as soon as the threshold has been passed

There is a 1-to-1 relation between these parameters and the key numbers which are defined in Annex A. Therefore it is possible to attach the parameters to the key number.

### 7.1.4.2 File control parameter

The file control parameter (FCP) as contained in Tables A.1 to A.3, according to ISO/IEC 7816-4, shall be required for every application dedicated file (ADF), dedicated file (DF) or elementary file (EF) in the card. Depending on the command parameters, the FCP shall be returned after a successful SELECT APDU. The FCP shall include access rule references according to 7.1.4.3. The tables in annex A summarize the common TLV-structure of the FCI for a DF or EF.

### 7.1.4.3 Access rules

An access rule shall determine which security conditions (SC) have to be met in order to enable the access to protected resources of the card for a specific access mode. The “NEVER” access rule shall be associated with reading operations dealing with the biometric reference. For cards compliant with this standard, access rules shall be encoded according to ISO/IEC 7816-4 by associating security conditions to access modes for the card logical data structures to be protected. Once these security conditions are met, the external application will obtain the security status required for the card to consider access to the protected data structure for the associated access mode.

NOTE The “NEVER” access rule is defined in ISO/IEC 7816-4:2005, Table 20 and 23.

When encoding access rules in a card compliant with this standard the following applies:

Access rules may be associated with any ADF, DF, and EF as well as with protected Data Objects.

For the on-card biometric comparison application, the FCP associated with the ADF storing the application may encode the access rules to perform the on-card biometric comparison.

For any other application resident in the card, access rules may contain a reference to an authentication control reference template (CRT AUT) storing the data object biometric information template “7F60” as per ISO/IEC 7816-11.

If required, the retrieval of the biometric information template (BIT) shall be protected using secure messaging templates according to ISO/IEC 7816-11.

NOTE “Access rules” are defined in ISO/IEC 7816-4.

#### 7.1.4.4 Double indirection

Double indirection is an optional functionality that a card compliant with this standard may offer only when it does not support any high security application according to 7.2.8 and Annex B requirements. Double indirection refers to the ability to proceed to an on-card biometric comparison using different configurations, as set down by the corresponding different access rules.

ISO/IEC 7816-4 offers different possibilities for the specification of the access rules that may apply for the interoperable implementation of the double indirection functionality. Thus, access rule encodes (in either compact or expanded format as per ISO/IEC 7816-4) the relationships between the access modes for those commands referring to a biometric reference and the required security conditions to be fulfilled. According to ISO/IEC 7816-4 these security conditions may refer to an application security environment with an authentication control reference template. This mechanism enables different applications to specify different access rules for biometrics verification operations with the same biometrics reference.

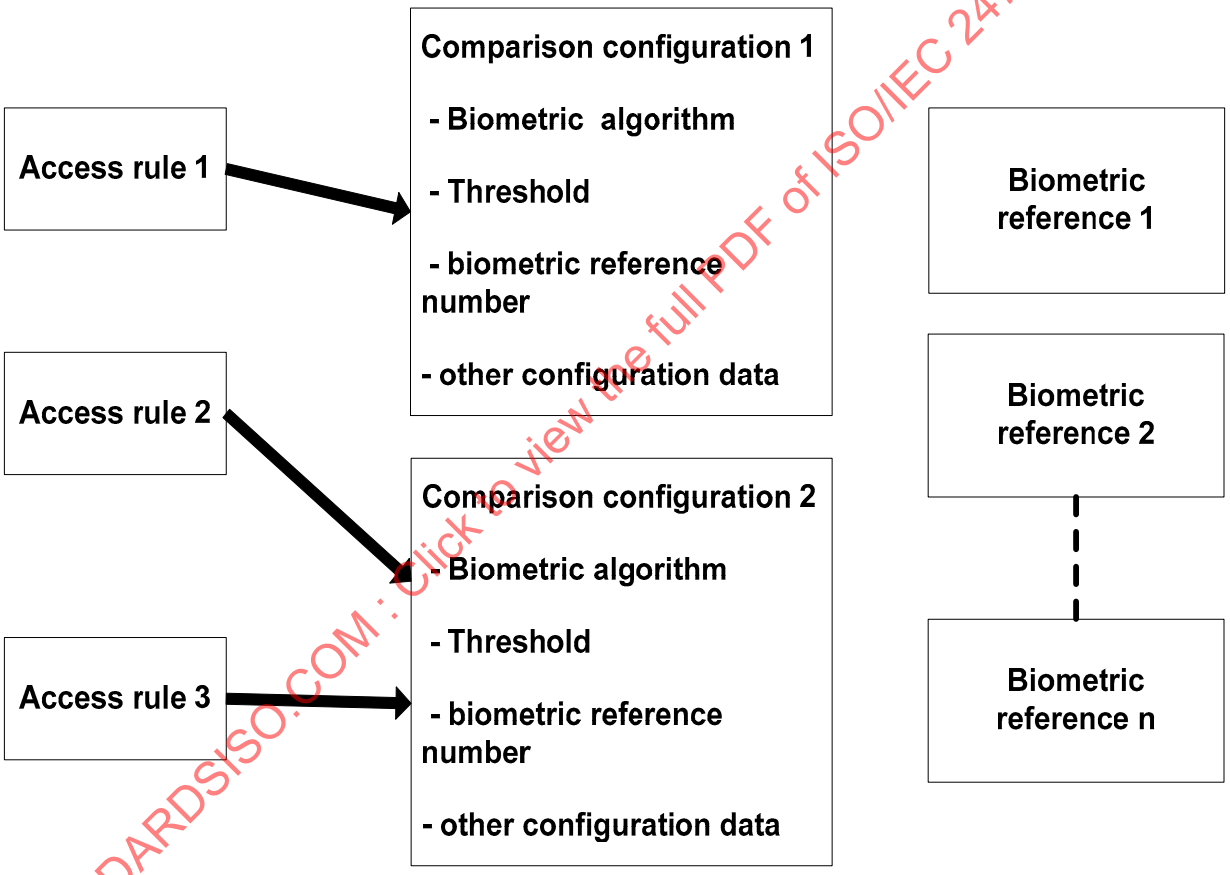


**Figure 5 — Example of sharing references and biometric references**



#### 7.1.4.5 Usage of security environment

The key number used in MSE SET determines

— Reference template

— Security level

In ISO/IEC 7816-4:2005 a usage qualifier for biometric authentication is defined (‘04’, see Table 35 of that standard).

The sequence for performing a biometric comparison is given in ISO/IEC 7816-11:2004, Annex B (see Figure 6, reproduced from Figure B.6 of that standard).

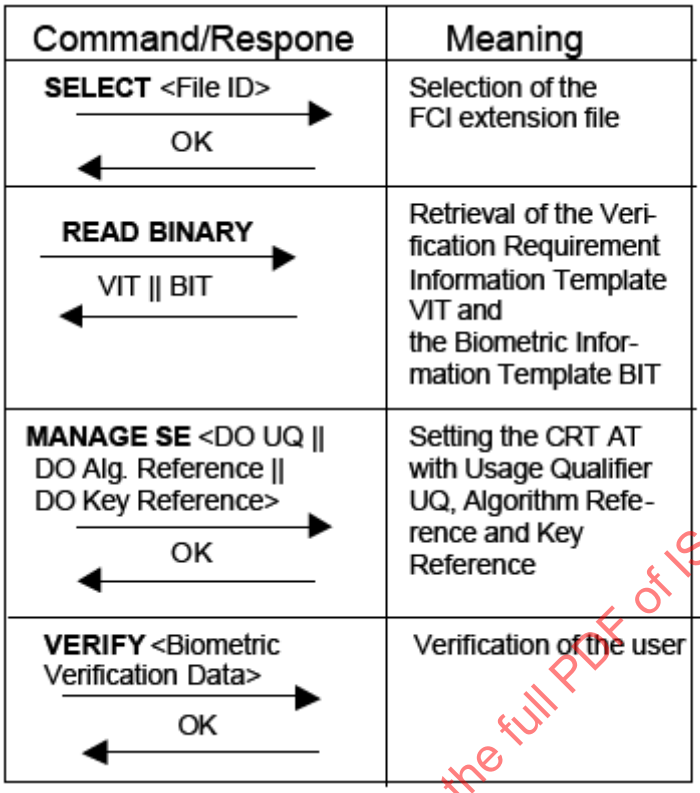


**Figure 6 — Commands for verification without secure messaging (example)**

However, ISO/IEC 7816-11 does not specify how the biometric reference and comparison parameters are stored internally because the complete enrolment process is not specified in that document.

In ISO/IEC 7816-4:2005 the following data objects are defined in Table 33:

- '80' Cryptographic mechanism reference
- File and key references
  - '81' — File reference (same encoding as ISO/IEC 7816-4:2005, 5.3.1.2)
  - '82' — DF name (see ISO/IEC 7816-4:2005, 5.3.1.1)
  - '83' — Reference of a secret key (for direct use)
    - Reference of a public key
    - Qualifier of reference data
  - '84' — Reference for computing a session key
    - Reference of a private key
  - 'A3' Key usage template (see ISO/IEC 7816-4:2005)
- Initial data reference: not applicable

#### 7.1.5 Retry counter management

Retry counter management defines the policies for managing the retry counter mechanisms. The policies are:

a) The cardholder of biometric comparison process shall be under the control of a retry counter which determines if the verification process may continue to be used with a given biometric reference.

b) An initial value of the retry counter shall be associated to the on-card biometric reference.

c) This association may be encoded using ISO/IEC 7816-15 sub-class attributes assigned to a Biometric Data Info Object as defined in ISO/IEC 7816-15.

d) If the verification fails, the retry counter shall be decremented by one and an error status that contains the remaining attempts shall be returned by the application.

e) The number of allowed retries may be encoded in the status bytes SW1-SW2= “63CX” (where X is the remaining number) of a response to a VERIFY command where the data field is absent according to ISO/IEC 7816-4.

f) A successful verification of the biometrics reference shall reset the associated retry counter to its initial value.

### 7.2 Standard processes for on-card comparison

#### 7.2.1 Application identifier (AID) for on-card biometric comparison

The card shall support an AID. When the on-card biometric comparison is implemented as an independent application, it shall be identified by an AID according to ISO/IEC 7816-4. The on-card comparison application may be selected by this AID ‘E8 28 81 C1 53 00’.

NOTE The AID is derived from the standard's object identifier according to ISO/IEC 7816-4, 8.2.1.2 and Annex A.

#### 7.2.2 Read biometric reference data

In an on-card comparison application, read access to the biometric reference to be used for comparison shall not be granted. Auxiliary data (open) related to the biometric reference may be read according to the needs of the application.

#### 7.2.3 Enrolment

Enrolment is the process through which a biometric reference is created and stored. In on-card comparison systems, this process shall involve:

1) transmitting one or more biometric templates to the ICC and storing them there,

2) transmitting and storing any other parameters needed for performing biometric comparisons (for example, comparison threshold, quality assurance parameters, etc.).

Depending on the capabilities of the ICC, signal processing may be split between the biometric interfacing device and the ICC. In all cases, all biometric data shall be transferred to the card through a secure and trusted channel or in a trusted environment, guaranteeing user's privacy. It is recommended to perform a verification test directly after enrolment to test the quality of the process.

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

In order to update the biometric data of the user, re-enrolment might occur. The enrolment rules shall apply in such a case.

### 7.2.4 Verification

Verification is the comparison of biometric data with biometric reference. In an on-card system the comparison shall be performed within the ICC. The biometric reference may include a plurality of enrolments, e.g. multiple fingerprints of the same person or a variety of modalities such as iris and face.

Biometric comparison requires access conditions as defined in the application file structure. Such conditions should preferably be met through mutual authentication or external authentication, as defined in the application file structure. Secure messaging according to ISO/IEC 7816-4 should be used for the transmission to the card of the biometric data for verification.

A VERIFY command (in accordance with ISO/IEC 7816-4:2005) shall be used to initiate the on-card comparison process. If the comparison is successful, the card security state may be set according to the access condition. In order to avoid hill-climb attacks, a retry counter shall be used, unless the need for such counter-measure is explicitly not required for a particular operational environment. If the comparison fails, the retry counter shall be decremented and may be returned in the status word of the response. If the retry counter reaches zero, further verification attempts shall be blocked. The retry counter may be reset with the use of unblocking methods as described in ISO/IEC 7816-4:2005.

### 7.2.5 Termination of on-card comparison application

When terminating an on-card comparison application, the on-card logical data structure containing biometric reference data pertaining only to such application shall be made inaccessible. A possible way is to “zeroize” the data.

### 7.2.6 Comparison process and result output

#### 7.2.6.1 Comparison process

The comparison process shall take place fully within the card.

#### 7.2.6.2 Comparison result

The comparison result is the result of the comparison between the comparison score of given biometric data and a predefined threshold to achieve the desired security level. If a similarity score is higher than the predefined threshold, SW1-SW2 in the VERIFY response APDU shall be ’90 00’. Otherwise, SW1-SW2 shall comply with ISO/IEC 7816 error codes.

### 7.2.7 Security requirements and biometric reference management

Security requirements and biometric reference management policies are:

a) the security access conditions for the biometric reference shall not allow the data to be read through any commands;

b) in order to update the biometric reference data, the rules applicable for enrolment shall apply;

c) biometric verification shall only be performed in the predefined security state;

d) there may be an independent retry counter for each reference to a stored biometric reference; and

e) the retry counters for different applications may be independent. This means that if one retry counter is expired, the retry counters for other applications referring to the same biometric data remain unchanged.

### 7.2.8 Threshold management

Threshold management defines the policies for managing the threshold parameters and related mechanisms. The following policies shall be followed:

(a) If cards have multiple applications with on-card biometric comparisons that use the same biometric reference, then a unique threshold and a single retry counter shall be used by these applications.

NOTE This standard acknowledges that for commercial or implementation reason, the need of having different thresholds for the same biometric reference may exist. If such is the case, the policy given in Annex B in particular SP2 applies.

(b) The configuration data shall define a parameter for internal quality restrictions for performing comparisons during the first time installation of the on-card biometric authentication application.

(c) The access rule for the double indirection, especially for the context of different configuration in particular comparison threshold, shall be defined during the installation phase of the applications.

(d) The following parameters as described in 7.1.3.2 shall be considered in order to determine the authenticity during verification:

i) biometric comparison algorithm parameters; and

ii) authentication type and discriminative power.

(e) The security levels that can be achieved as a result of positive biometric verification should be obtained from the configuration data. The host shall select the security level that is required by its application before initiating verification.

(f) The threshold parameters described in 7.2.8 shall not be changed during on-card verification.

## 8 Work-sharing

### 8.1 Runtime work-sharing mechanism using WSR protocol

In work-sharing on-card comparison architecture, the comparison shall be performed within the ICC. The pre-comparison computation may be performed totally or partially in the biometric verification system, depending on the design of specific biometric verification system for ICC. An ENVELOPE command as described in 8.2.2 to 8.2.3 may be used to discover whether the supported WSR protocol is available. As described in 6.4, two portions of biometric data are stored inside the ICC. The secured portion, which is the biometric reference, shall not be sent out to the biometric verification system. The auxiliary data (open) portion, which contains the biometric property, can be sent out using WSR protocol for processing by biometric interfacing device to speed up the processing time. Both pre-comparison calculation and work-sharing at runtime shall use this mechanism to implement. An example of work-sharing architecture is described in Annex F. Figure F.2 shows the mechanism for work-sharing, according to Figure 3. Figure F.2 is not applicable for other variations of work-sharing architectures. Those APDU commands and responses, which are specified in ISO/IEC 7816-4:2005, 8.6 “Card-originated byte strings”, shall be used to support the WSR protocol. The card may send multiple WSRs request to the local biometric verification system in single APDU secession. Before starting the WSR function call, the corresponding data for computation shall be transferred into the APDU buffer. In Figure 7, the number inside the bracket of each arrow indicates the sequence. When a WSR protocol is ascertained (see 8.2.2) or selected (see 8.2.3), the following sequence summarizes the WSR protocol:

(1) The card receives a biometric comparison command needing WSR, and starts internally its WSR function.

(2) The card OS shall return response bytes “62 XX” to the biometric verification system to notify that the card is confirming the initiation of WSR request as step 1). The card has a query of 'XX' bytes that the biometric verification system should retrieve and for which the card expects a response.

(3) & (4) Once the biometric verification system receives the 62 XX, the biometric verification system shall send GET DATA command (00 CB 00 00 XX) to the card to fetch the intermediate data from the card. For retrieving a query of 'XX' bytes available in the card, the interface device shall send a GET DATA command with P1-P2 set to '0000' and a Le field set to 'XX'.If the card still needs to transmit data before receiving data from the outside world, it shall send SW1-SW2 = 62 XY and resume phase 3&4.

(5) Once the biometric verification system completes the processing of the intermediate data, the device shall reply the processed data to the card. The biometric verification system shall use PUT DATA command (00 DB 00 00 YY …) to send back the processed data to the card to continue on-card comparison process. The interface device shall send a PUT DATA command with P1-P2 set to '0000' and Lc field set to 'YY'.If the outside world has not yet transmitted all the data, the PUT DATA shall be chained and phase5 shall be resumed.

(6) If the card still needs WSR, the card OS resumes the execution of the biometric comparison function at step 2). If not, see below.

(7) If the card does not need WSR any more, it shall answer with SW1-SW2, which is the response to the biometric comparison command received at step 1)

See informative Annex H for a state diagram of the WSR protocol.

Where XX is the number of bytes of intermediate data to the biometric verification system and YY is the number of returning bytes of processed data to the card.

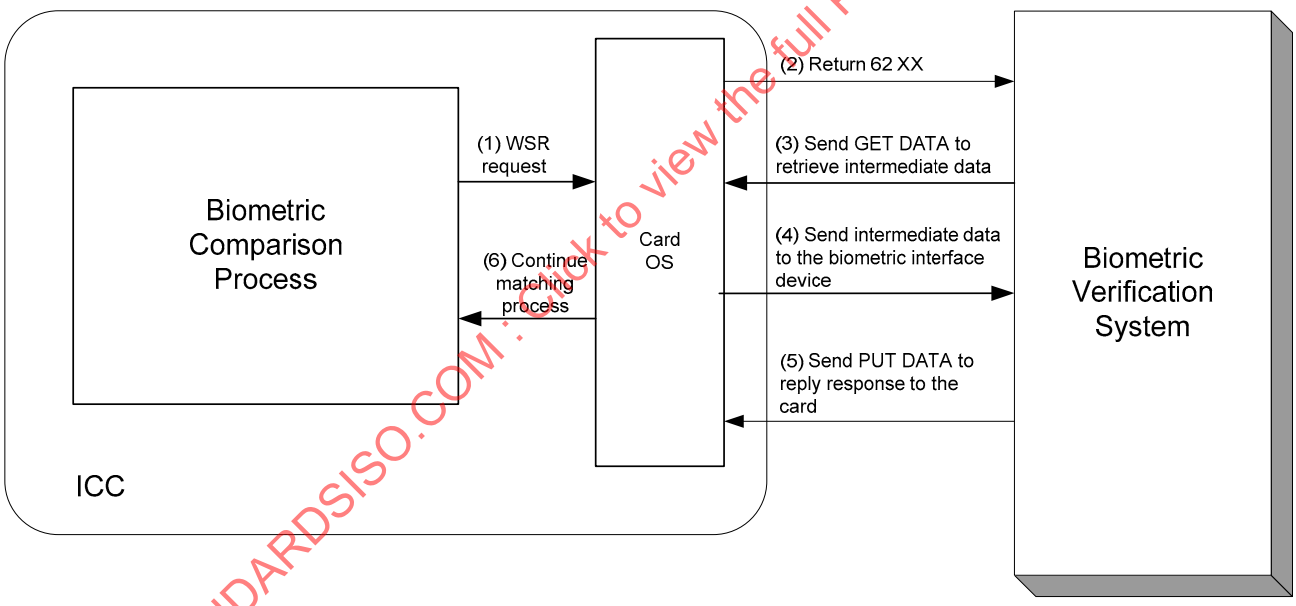




**Figure 7 — WSR mechanism**

## 8.2 Work-sharing management

### 8.2.1 General

The on-card comparison application may need management procedures to make the biometric verification system aware of the availability of a WSR protocol and to invoke unambiguously a given WSR protocol. In this case, a unique object identifier shall be used to let the biometric verification system accept the WSR request during biometric comparison process. Hence, a specification precise enough to allow an implementation of a WSR protocol shall be available belonging to the object identifier tree, which means that the specification has a unique object identifier.

### 8.2.2 Work-sharing procedure discovery

The support of a particular WSR protocol in conjunction with an application which needs on-card biometric authentication can be indicated by encapsulating the object identifier in the constructed version of the proprietary data (tag '73') within the application template (tag '61') to be read in a DIR file or recovered by a standard GET DATA; On channel 0, it shall be:

'00' 'CB' '2F' '00' '02' '5C' '00' '00'

NOTE ISO/IEC 7816-15 uses this kind of coding in the proprietary data for different purposes.

### 8.2.3 Work-sharing procedure operation

An application which needs on-card comparison shall be currently selected. The interface device should know (according to 8.1) that a WSR protocol is available. In order to select a WSR protocol compliant with 8.1, the interface device may send to the card an odd ENVELOPE command encapsulating the object identifier of the WSR protocol. On channel 0, it shall be:

'00' 'C3' '00' '00' <Lc> '06' <Lc-2> < object identifier of the WSR protocol>

The success of the command (response = '90 00') states that:

— the card has understood the object identifier, hence supports the referenced WSR protocol,

— is ready to execute this protocol, for example, that it is launched at the right place in the workflow of the application and that an adequate security environment is set.

All other SW1 SW2 values deny either the support of the referenced WSR protocol, or the timely use of it. SW1 SW2 = '6A' '81' is recommended. If the ENVELOPE command is successfully executed by the card, the object identifier of the data field of the ENVELOPE APDU command shall identify the specification where the WSR protocol is defined.

# Annex A
(normative)

# Common TLV-structure of the file control parameter

The following Tables (A.1 to A.3) are defined in ISO/IEC 7816-4 for encoding of an access rule consists of an access mode data object followed by one or more security condition data objects.

**Table A.1 — Common TLV structure of the FCI for a DF**

| Tag | Length | Value | | |
|---|---|---|---|---|
| 62 | x | Tag | Length | Value |
| | | 82 | 1 | '38' File Descriptor |
| | | 83 | 2 | File ID |
| | | 84 | '01' to '10' | DF name (AID) |
| | | 8A | 1 | 5 |

**Table A.2 — Common TLV structure of the FCI for a formatted EF**

| Tag | Length | Value | | |
|---|---|---|---|---|
| 62 | X | Tag | Length | Value |
| | | 82 | 5 | File Descriptor (1 Byte)<br>41<br>00<br>maximum record length (1 Byte)<br>maximum record count ( 1 Byte) |
| | | 83 | 2 | File ID |
| | | 85 | 2 | Maximum size |
| | | 88 | 1 | Short EFID |
| | | 8A | 1 | 5 (activated state) |
| | | A1 | var. | Data objects with access rule references |

**Table A.3 — Common TLV structure of the FCI for a transparent EF**

| Tag | Length | Value | | |
|---|---|---|---|---|
| 62 | X | Tag | Length | Value |
| | | 80 | 02 | Memory space of transparent EF |
| | | 82 | 01 | File descriptor for transparent EF |
| | | 83 | 2 | File ID |
| | | 88 | 1 | SFI |
| | | 8A | 1 | 5 |
| | | A1 | x | Data object with access rule reference(s) |

# Annex B
(normative)

# Security policies for on-card biometric comparison

## B.1 Introduction

This annex defines the minimum set of security policies for those ICC applications using on-card biometric comparison. As it will be explained, different architectures can be considered, and although some of the policies can be common to all, there are other policies that are specific for certain architecture.

Within this introduction, an overview to the different architectures will be provided, as well as a table to map those architectures to the security policies detailed in the following clauses. Those different architectures can be classified as:

a) Using the biometric reference as a global element. This includes the following situations:

   1) Card with a single application that uses on-card biometric comparison

   2) Card with multiple applications that use on-card biometric comparison with a single comparison configuration (i.e. same threshold, same retry counter, etc.). In this case, if one application blocks the on-card biometric comparison mechanism, then all applications using the same verification mechanism will be affected. On the other hand, if one application has a successful verification, then for all applications the retry counter will be reset.

b) Using the biometric reference as a local element. This case includes the following situations:

   1) Each application has its own biometric reference structure, including the biometric reference data, configuration data such as thresholds and maximum value for the retry counter, retry counter, etc.

   2) All applications only share the same biometric reference data, but each application has its own configuration data (comparison configuration data), which includes the different thresholds, retry counter, etc.

The following table states the relationship between the above mentioned architectures and the security policies defined in this annex.

**Table B.1 — Mapping about on-card biometric comparison architectures and security policies**

| | SP1: Global Comparison Configuration Data | SP2: Local Comparison Configuration Data |
|---|---|---|
| **a.1** | X | |
| **a.2** | X | |
| **b.1** | X | |
| **b.2** | | X |

The following clauses define the common security policies, the SP1 policies, and the SP2 policies.

## B.2 Common security policies (CSP) for on-card biometric comparison

In all cases the following minimum security policies apply:

- No application shall be allowed to send the biometric reference outside the ICC. (see 7.2.2).
- The policies specified in 7.1.5 shall be used to implement the retry counter mechanism.
- All applications shall use the security mechanisms available either for creating the biometric reference (enrolment), updating the biometric references (re-enrolment), or compare with the biometric reference (verify). In particular:
  - A secure messaging shall be established prior to any of the above mentioned operations (see ISO/IEC 7816-4).
  - All data exchanged regarding the on-card biometric comparison shall be authenticated for its integrity.
  - All biometric data shall be enciphered for transmission to the ICC, to assure confidentiality (see ISO/IEC 24761:2009).
- The card operating system might have a mechanism to unblock the on-card biometric comparison. If such is the case, the unblocking process shall "zeroise" the biometric reference in the ICC, and request for a new enrolment.

## B.3 Security policies (SP1) for global comparison configuration data

For those applications where the biometric reference is to be used as a global verification mechanism, there is no need to establish a double indirection for determining a comparison configuration. Furthermore, the following policies shall apply:

- For cards with multiple applications with on-card biometric comparisons using the same biometric reference, if any application using the biometric reference is a high security application, a unique threshold should be used by all applications and a single retry counter associated to the biometric reference shall be used (see 7.2.8 a).
- All configuration data is linked to the biometric reference. In particular:
  - The verification threshold
  - The maximum amount of verification retries
  - The retry counter
  - All parameters for the comparison algorithm
- None of the applications using the on-card biometric comparison mechanism with such biometric reference can change the configuration data independently.
- When the retry counter reaches zero, the on-card biometric comparison mechanism is blocked, and therefore all applications using such biometric reference for verification will not be able to execute those operations protected by the on-card biometric comparison.
- A successful verification of the biometrics reference resets the associated retry counter to its initial value, no matter which of the applications have carried out the successful verification.

## B.4 Security policies (SP2) for local comparison configuration data

In the case of a card whose applications request an independent control of the on-card biometric comparison, but shares the same biometric reference, the following policies apply:

- All applications that use the double indirection mechanism will have their own comparison configuration data, including, at least:
  - Threshold
  - Retry counter
- It is not allowed to configure applications sharing the same biometric data, that will have different thresholds, but sharing the same retry counter.
- The use of the biometric reference by one application, shall not affect the security and integrity of the rest of the applications. More specifically:
  - Any time an application successfully verifies the biometric reference, only the retry counter for such application will be reset to its initial state.
  - Any time an application fails in the verification of the biometric reference data, only the retry counter for such application will be decremented in one unit.
  - If the retry counter of one of the applications reaches zero, then only such application denies subsequent execution of the VERIFY command for the on-card biometric comparison.
- Any application can change its comparison configuration data as desired, without modifying any of the comparison configuration data of the other applications which share the same biometric reference.

# Annex C
(informative)

# Sample APDU for on-card comparison

Table C.1 is a construction of a sample APDU according to current standards.

The VERIFY command APDU is used to send a fingerprint minutiae template to the ICC. It has the following structure:

**Table C.1 — Command APDU structure**

| CLA | INS | P1 | P2 | Lc | Data |
|---|---|---|---|---|---|
| 0x00 | 0x20<br>0x21[1] | 0x00 | 0x00 | length | Lc Bytes |
| NOTE 1 The Le field is empty, because no response data is returned for VERIFY in ISO/IEC 7816-4. Only the status word is returned to the interface device.<br><br>NOTE 2 The biometric in-use is indicated inside the BIT.<br><br>[1] Tag 0x20 is used if the data field contains transparent plain data while tag 0x21 indicates that the data field is BER TLV-encoded. | | | | | |

The data field contains the verification data. The ICC's capabilities may be implicitly known. The recommended way is to hold a BIT (biometric information template) that can publicly be read off the card with a GET DATA command using tag 0x7F60 and gives the outside world information on the card capabilities, for example, support of on-card comparison, what data format and format type is expected and whether the ICC wants the minutiae ordered or not. Details on the BIT are found in ISO/IEC 7816-11.

The template in the data field should be BER-TLV-coded. The following tags are relevant for encoding:

0x7F2E biometric reference

0x5F2E biometric data

0x81/0xA1 biometric data with standardized format (primitive/constructed)

0x82/0xA2 biometric data with proprietary format (primitive/constructed)

If sending a standard minutiae data set to the card, this encodes to the data field in Table C.2.

**Table C.2 — Data fields for standard minutiae**

| Tag Biometric reference | Length of Data Object | Tag Biometric Data Standardized | Length of minutiae data | Minutiae data |
|---|---|---|---|---|
| 0x7F2E | L+2 | 0x81 | L | |

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

**Figure C.1 — Fingerprint image with minutiae positions**



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

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 from ISO/IEC 19794-2 was used to encode the minutiae. 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 0x5D, vertical position 0x69, type bifurcation and orientation are stored in 0x2D.

A total of 35 minutiae were detected, which results in a total minutiae size of 3x35 = 105 bytes, hexadecimal 0x69.

The data added to the above structure results in the following command:

| CLA | INS | P1 | P2 | Lc | Data |
|---|---|---|---|---|---|
| 0x00 | 0x21 | 0x00 | 0x00 | 0x6D | |

| Tag<br>Biometric reference | Length of Data Object | Tag Biometric Data Standardized | Length of minutiae data | Minutiae data |
|---|---|---|---|---|
| 0x7F2E | 0x6B | 0x81 | 0x69 | |

0x5D 0x69 0x2D 0xA1 0x43 0x2F 0xAA 0x82 0x2F 0x6F 0x48 0x2F 0x43 0x49 0x35 0x96 0x45 0x37 0xAF 0x81 0x48 0xB0 0xBF 0x48 0x96 0x48 0x48 0x5D 0x89 0x4A 0x9C 0x43 0x4D 0x7C 0x6A 0x4D 0x63 0x6A 0x4D 0x19 0x45 0x4F 0x73 0x8B 0x50 0x91 0x42 0x54 0x85 0x6B 0x57 0x6B 0xAA 0x58 0x86 0xB2 0x58 0x7D 0x70 0x59 0x36 0x82 0x5B 0x8C 0x57 0x5E 0x94 0x9C 0x5F 0x73 0x71 0x61 0x61 0x66 0x64 0x4C 0x9C 0x69 0x97 0x9B 0x6F 0xA5 0x9D 0x70 0x33 0xB9 0x72 0x50 0x96 0x74 0x92 0x58 0x7D 0x27 0x59 0x7E 0x9D 0x59 0x80 0x66 0x93 0x83 0x4A 0x56 0x86 0x8E 0x56 0x90 0x3D 0x74 0x9A 0x3A 0x76

**Figure C.2 — Structure of APDU for on-card comparison**

Total command:

0x00 0x21 0x00 0x00 0x6D 0x7F 0x2E 0x6B 0x81 0x69 0x5D 0x69 0x2D 0xA1 0x43 0x2F 0xAA 0x82 0x2F 0x6F 0x48 0x2F 0x43 0x49 0x35 0x96 0x45 0x37 0xAF 0x81 0x48 0xB0 0xBF 0x48 0x96 0x48 0x48 0x5D 0x89 0x4A 0x9C 0x43 0x4D 0x7C 0x6A 0x4D 0x63 0x6A 0x4D 0x19 0x45 0x4F 0x73 0x8B 0x50 0x91 0x42 0x54 0x85 0x6B 0x57 0x6B 0xAA 0x58 0x86 0xB2 0x58 0x7D 0x70 0x59 0x36 0x82 0x5B 0x8C 0x57 0x5E 0x94 0x9C 0x5F 0x73 0x71 0x61 0x61 0x66 0x64 0x4C 0x9C 0x69 0x97 0x9B 0x6F 0xA5 0x9D 0x70 0x33 0xB9 0x72 0x50 0x96 0x74 0x92 0x58 0x7D 0x27 0x59 0x7E 0x9D 0x59 0x80 0x66 0x93 0x83 0x4A 0x56 0x86 0x8E 0x56 0x90 0x3D 0x74 0x9A 0x3A 0x76

There are other possibilities to encode the minutiae and to construct the command. Optional features or proprietary data may 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.

# Annex D
(informative)

# Software shareable interface for biometrics comparison

## D.1 General

Cards have built in firewall mechanism to protect sensitive data of each application in multi-application ICC. This mechanism is good in the sense that it denies access of a rogue application from accessing data of another application. However, this mechanism also poses the problem of a trusted application wanting to share a method/data from another trusted application. Having a secured shareable interface or software firewall will allow applications to share only selected method/data while protecting sensitive data from being accessed. This is important for biometrics application to share the results or biometric data with other applications in the card.

## D.2 Shareable Interface Mechanism

The method to share functions/data through the shareable interface is described below. Figure D.1 shows a card with two applications. The sharing biometric application creates two sets of functions/data: Non shareable functions for full access itself and Shareable functions/data for other application limited access. The shareable functions are derived from the shareable interface. Another generic application wants to use the shared functions/data from the Biometric Application. It will also create two sets of functions/data: Non Shareable functions for its own methods and Shareable functions for using other application method.

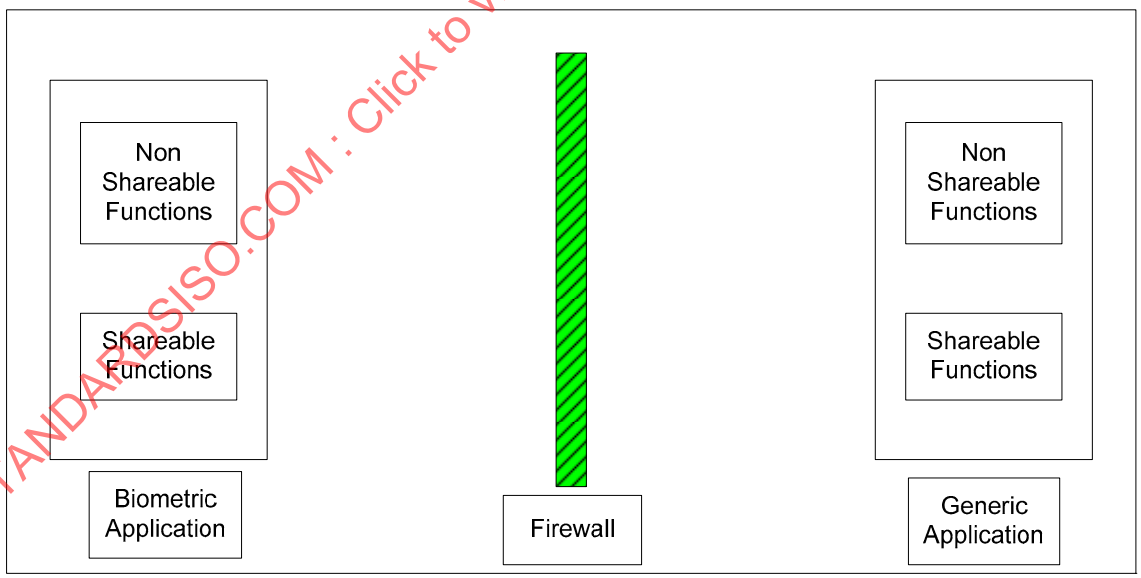


**Figure D.1 — Applications in card**

The generic application calls a shareable function of the Biometric Application. The OS checks and forwards the request to the biometric application. The biometric application receives the request and determines whether or not it will share its shareable function with the requester. If the biometric application finds the request agreeable, then a reference to its shareable function is provided; otherwise, an error is returned. The OS forwards this reference to the requester (generic application). Figure D.2 illustrates the process.

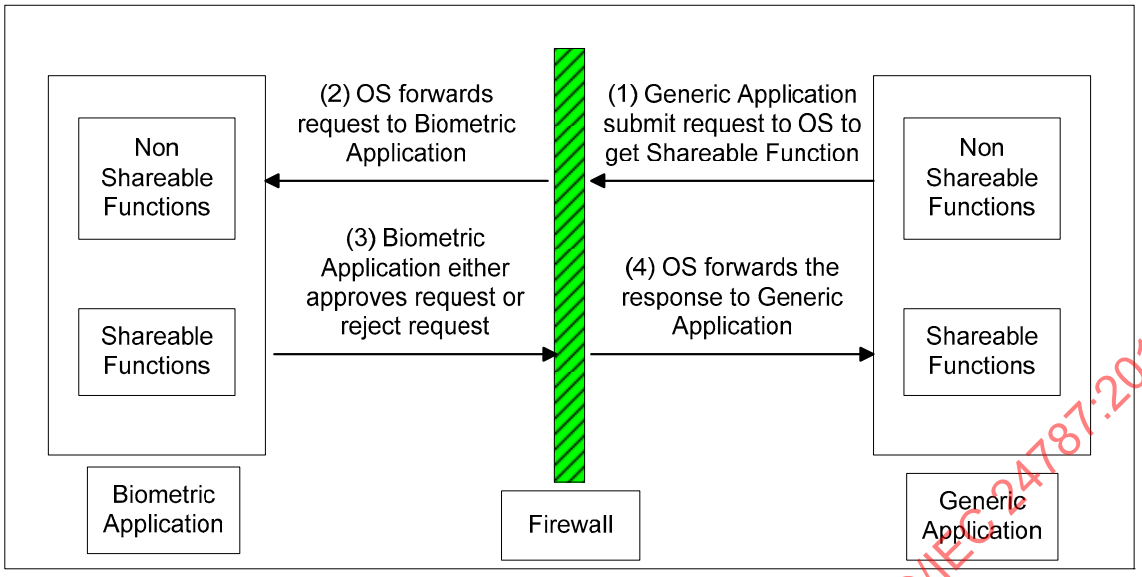


**Figure D.2 — Accessing shared object**

Once the generic application has this reference, it can use the shareable functions/data provided by the biometric application. The generic application can get the biometric comparison score through the shared function to approve a transaction or obtain needed information of the authorised user for transmission. The shared function can be shared for a period of time determined by either the OS or the biometric application for added security, as illustrated in Figure D.3.

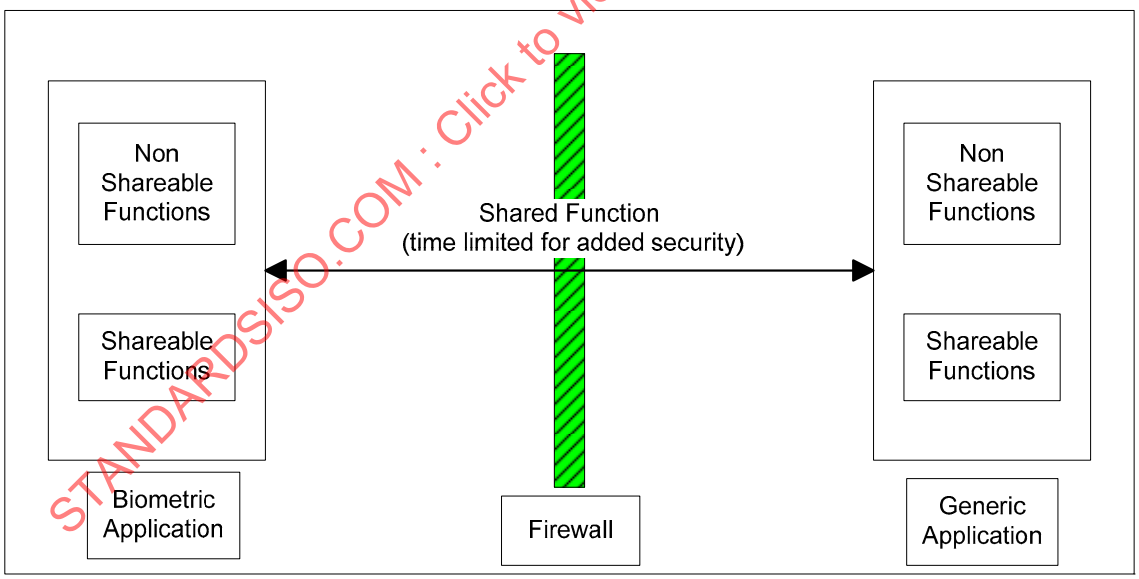


**Figure D.3 — Successful sharing of object**

For example, once the biometric application completes the biometric verification, a comparison score will be computed and stored inside the program. The generic application can access to biometric application to get the comparison score by accessing the shareable functions through the Firewall. The firewall verifies the accessibilities of the requester (generic application), and then allows it to fetch the comparison score from biometric application (upon successful verification). The firewall is controlled by the operating system in the card.

# Annex E
(informative)

# Recommendation for security mechanisms in on-card comparison

## E.1 General

This annex is intended to introduce the security mechanism to be considered when working with on-card comparison identification cards. As mentioned in this standard, due to privacy constraints of biometric information, security mechanisms are strongly recommended.

Readers should refer to other security related standards, for all technical details needed for implementing these security mechanisms. Readers should refer to the ISO/IEC 7816 series of standards for information of commands and mechanisms related to integrated circuit identification cards (e.g. parts 4, 8, 11 and 15), and to those related standards developed by ISO/IEC JTC1/SC 27.

## E.2 Mutual authentication

The first point to be considered when trying to guarantee security when two entities are exchanging data is for each of those entities to trust the other. Therefore, when starting communication, a mechanism for the terminal to trust the card, and another for the card to trust the terminal, are to be used. Those mechanisms are known as internal and external authentication. When both mechanisms are used, then it is called mutual authentication.

Mutual authentication usually ends up generating a session key in order to generate a secure channel. In order to avoid replay attacks, such session key should be completely different among sessions. Some of the algorithms used for mutual authentication will request the generation of random or pseudo-random numbers by both, the card and the terminal.

Once a secure channel is established between the card and the terminal, the following mechanisms can be achieved with higher levels of success.

## E.3 Message integrity

During APDU exchange, hackers may try to intercept the messages and change them in their own benefit by, for example, re-sending a previous biometric sample to gain access to the card information and/or services. To avoid this kind of attacks, it is recommended that both terminal and card will check the integrity of the APDUs received.

One way of doing this is by signing the APDU, both header and data, with a symmetric key cryptographic algorithm, and appending the signature obtained to the data exchanged. Using the session key generated during mutual authentication, avoids the use of the attacks mentioned above.

## E.4 Confidentiality

Integrity is recommended for use with all APDUs exchanged, but sometimes a higher level of security might be used. Especially critical are those APDUs where the biometric template or the biometric sample is transmitted from reader to the card (or from the card to the reader in off-card comparison). In these kinds of messages, data should not be transmitted in raw format, but enciphered with the highest level of security available, thereby improving confidentiality in the system.

For example, if using a symmetric key cryptographic algorithm, data can be enciphered with the session key obtained by mutual authentication (when establishing the secure channel). Integrity checking is also recommended, so integrity can be applied before or after enciphering data transmitted.

## E.5 Prevention of replay attack using MAC with secret key

It is recommended to implement protection mechanism in the ICC to prevent replay attack. One possible method to avoid replay attack is to use the Message Authentication Code (MAC) of the biometric data in conjunction with a random number and a secret key. The terminal can get the random number from the card, and calculate a MAC of the biometric data that concatenates with the random number (from the card) and the secret key. The secret key is stored in both the application and the card. During the communication, only the random number and the MAC are necessary to be transmitted. When the card receives the biometric data and the MAC, the MAC should be verified on-card before biometric comparison.

If an attacker is able to get the biometrics data, even the random number from the card and the MAC from a previous matching process, the attacker cannot produce a correct MAC for the next time of verification without knowing the secret key.

However, in this approach, assuming that the terminal is trusted and is able to keep a secret key within it, this method can be regarded as a kind of “secure channel”.

NOTE This approach is optional with respect to the working environment.