INTERNATIONAL STANDARD

**ISO/IEC 7816-11**

First edition
2004-04-01

# Identification cards — Integrated circuit cards —

## Part 11: Personal verification through biometric methods



*Cartes d'identification — Cartes à circuit intégré —*
*Partie 11: Vérification personnelle par méthodes biométriques*



Reference number
ISO/IEC 7816-11:2004(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.

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.

ISO/IEC 7816-11 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification.*



ISO/IEC 7816 consists of the following parts, under the general title *Identification cards — Integrated circuit cards:*



— *Part 1: Cards with contacts — Physical characteristics*

— *Part 2: Cards with contacts — Dimensions and location of the contacts*

— *Part 3: Cards with contacts — Electrical interface and transmission protocols*

— *Part 4: Organization, security and commands for interchange*

— *Part 5: Registration of application providers*

— *Part 6: Interindustry data elements for interchange*

— *Part 7: Interindustry Commands for Structured Card Query Language (SCQL)*

— *Part 8: Commands for security operations*

— *Part 9: Commands for card management*

— *Part 10: Cards with contacts — Electronic signals and answer to reset for synchronous cards*

— *Part 11: Personal verification through biometric methods*

— *Part 15: Cryptographic information application*

## Introduction

This part of ISO/IEC 7816 is one of a series of standards describing the parameters for integrated circuit(s) cards with contacts and the use of such cards for international interchange.

This part of ISO/IEC 7816 may also apply to contactless cards.

# Identification cards — Integrated circuit cards with contacts —

# Part 11:
# Personal verification through biometric methods

## 1 Scope

This part of ISO/IEC 7816 specifies security related interindustry commands to be used for personal verification with biometric methods in integrated circuit(s) cards. It also defines the data structure and data access methods for use of the card as a carrier of the biometric reference data and/or as the device to perform the verification of a personal biometric (on-card matching). Identification of persons using biometric methods is outside the scope of this standard.

## 2 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 7816-4:2003, *Identification cards — Integrated circuit cards with contacts — Part 4: Organization, security and commands for interchange*



ISO/IEC CD 19785:2003, *Information technology — Common Biometric Exchange Framework Format (CBEFF)*

## 3 Terms and definitions

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

**3.1**
**biometric data**
data encoding a feature or features used in biometric verification

**3.2**
**biometric information**
information needed by the outside world to construct the verification data

**3.3**
**biometric reference data**
data stored on the card for the purpose of comparison with the biometric verification data

**3.4**
**biometric verification**
process of verifying by a one-to-one comparison of the biometric verification data against biometric reference data

**3.5**
**biometric verification data**
data acquired during a verification process for the comparison with the biometric reference data

**3.6**
**template**
as defined in ISO/IEC 7816-4

**WARNING — The term "template" means the value field of a constructed data object. It should not be confused with a processed biometric data sample.**

## 4 Abbreviated terms

For the purpose of this part of ISO/IEC 7816, the following abbreviations apply.

| | |
|---|---|
| AID | Application Identifier |
| AT | Authentication Template |
| BER | Basic Encoding Rules |
| BIT | Biometric Information Template |
| BD | Biometric Data |
| BDP | BD in proprietary format |
| BDS | BD in standardized format |
| BDT | Biometric Data Template |
| CCT | Cryptographic Checksum Template |
| CRT | Control Reference Template |
| CT | Confidentiality Template |
| DE | Data Element |
| DF | Dedicated File |
| DO | Data Object |
| DST | Digital Signature Template |
| EFID | Elementary File ID |
| FCI | File Control Information |
| ID | Identifier |
| L | Length |
| OID | Object Identifier |
| RD | Reference Data |
| SE | Security Environment |
| SM | Secure Messaging |
| TLV | Tag-Length-Value |
| UQ | Usage Qualifier |
| VIDO | Verification requirement Information Data Object |
| VIT | Verification requirement Information Template |



## 5 Commands for biometric verification processes

Commands for retrieval, verification and authentication defined in ISO/IEC 7816-4 are used for biometric verification. Biometric data (e.g. face features, ear shape, fingerprint, speech pattern, voice print, key stroke) may need protection against replay or presentation of verification data derived from original biometric data (e.g. a fingerprint, a face photo). A method to prevent this kind of attack is to send the verification data to the card with a cryptographic checksum or a digital signature applying secure messaging as defined in ISO/IEC 7816-4. Likewise, secure messaging may be used to guarantee the authenticity of the biometric data retrieved from the card.

### 5.1 Commands to retrieve biometric information

The commands as specified in ISO/IEC 7816-4 in the clause related to data referencing shall be used for the retrieval of biometric information.

### 5.2 Command for a static biometric verification process

The command to be used for a static verification process (see Annex A) is the VERIFY command as specified in ISO/IEC 7816-4. The information to be conveyed is

— biometric reference data identifier (i.e. the qualifier of the reference data)

— biometric verification data.

The biometric verification data may be encoded as BER-TLV data objects (see Table 2). The CLA byte may indicate that the command data field is BER-TLV coded (see ISO/IEC 7816-4).

For combined biometric schemes, command chaining as defined in ISO/IEC 7816-8 may be used.

### 5.3 Commands for a dynamic biometric verification process

To get a challenge, to which a user response is required (see Annex A), the GET CHALLENGE command shall be used.

The type of challenge in a biometric verification process, e.g. a phrase for voiceprint or a phrase for keystroke, depends on the biometric algorithm, which can be specified in P1 of the GET CHALLENGE command (see ISO/IEC 7816-4). The respective algorithm may be selected alternatively by using the MANAGE SECURITY ENVIRONMENT command (e.g. SET option with CRT AT and DO usage qualifier and DO algorithm id in the data field).



After a successful GET CHALLENGE command, an EXTERNAL AUTHENTICATE command is sent to the card. The command data field conveys the relevant biometric verification data. For coding of the biometric verification data, the same principles apply as for the VERIFY command, see 5.1.



## 6 Data elements



### 6.1 Biometric information

The Biometric Information Template (BIT) provides descriptive information regarding the associated biometric data. It is provided by the card in response to a retrieval command prior to a verification process. Table 1 defines biometric information DOs.

**Table 1 — Biometric information DOs**

| Tag | L | Value | | | | Presence |
|---|---|---|---|---|---|---|
| '7F60' | Var. | Biometric Information Template (BIT) | | | | |
| | | **Tag** | **L** | **Value** | | |
| | | '80' | 1 | Algorithm reference for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SE command | | Optional |
| | | '83' | 1 | Reference data qualifier for use in the VERIFY / EXT. AUTH. / MANAGE SE command | | Optional |
| | | 'A0' | Var. | Biometric information DOs defined in this standard | | Optional |
| | | '06'<br>'41'<br>'42'<br>'4F' | Var.<br>Var.<br>Var.<br>Var. | Tag allocation authority (see ISO/IEC 7816-6):<br>- Object identifier (OID)<br>- Country authority (see ISO/IEC 7816-4)<br>- Issuer (see ISO/IEC 7816-4)<br>- Application Identifier (AID), identifies the application and its provider (see ISO/IEC 7816-4)<br>The default tag allocation authority is ISO/IEC JTC1/SC37. | | One of these DOs is mandatory, if 'A1' is present |
| | | 'A1' | Var. | Biometric information DOs specified by the tag allocation authority (mandatory indication, see above).<br>See also example in Annex C | | Mandatory, if 'A0' is not present |
| | | | | **Tag** | **L** | **Value** | | |
| | | | | '8x'/ 'Ax'<br>'9x'/ 'Bx' | Var.<br>Var. | DOs defined by the tag allocation authority<br>... (primitive / constructed)<br>... (primitive / constructed) | | DO dependent |



NOTE In case the card does not perform the verification process, the Biometric Information Template may also contain the biometric reference data (see Table 3) and possibly discretionary data (tag '53' or '73') e.g. for data to be delivered to a service system, if verification is positive (see Annex C).

If several BITs are present within the same application, then they shall be grouped as shown in Table 2.

**Table 2 — BIT group template**

| Tag | L | Value | | | Presence |
|---|---|---|---|---|---|
| '7F61' | Var. | BIT group template | | | |
| | | **Tag** | **L** | **Value** | |
| | | '02' | Var. | Number of BITs in the group | Mandatory |
| | | '7F60' | Var. | BIT 1 | Conditional |
| | | | | ... | |
| | | '7F60' | Var. | BIT n | Conditional |

A BIT group template can be recovered e.g. by

— a GET DATA command

— reading out of a file in the corresponding DF, EFID found in the FCI, or

— reading an SE template (see ISO/IEC 7816-4), in which the BIT group template is stored.

## 6.2 Biometric data

Biometric data (biometric verification data, biometric reference data) may be presented

— as a concatenation of data elements,

— within a biometric data DO as defined in ISO/IEC 7816-6, or

— as concatenation of DOs within a biometric data template, see Table 3.

**Table 3 — Biometric data DOs**

<table>
<tr><th>Tag</th><th>L</th><th colspan="3">Value</th><th>Presence</th></tr>
<tr><td>‘5F2E’</td><td>Var.</td><td colspan="3">Biometric data</td><td></td></tr>
<tr><td>‘7F2E’</td><td>Var.</td><td colspan="3">Biometric data template</td><td></td></tr>
<tr><td></td><td></td><td>Tag</td><td>L</td><td>Value</td><td></td></tr>
<tr><td></td><td></td><td>‘5F2E’</td><td>Var.</td><td>Biometric data</td><td rowspan="3">At least one of these DOs is present, if the template is used</td></tr>
<tr><td></td><td></td><td>‘81’ / ‘A1’</td><td>Var.</td><td>Biometric data with standardised format (primitive / constructed)</td></tr>
<tr><td></td><td></td><td>‘82’ / ‘A2’</td><td>Var.</td><td>Biometric data with proprietary format (primitive / constructed)</td></tr>
</table>



As shown in Table 3, biometric data may be split up in a part with standard format and in a part with proprietary format, whereby the part with the proprietary format may be used, e.g. for achieving a better performance. The usage of biometric data with standardized and proprietary formats is shown in Figure 1.



Structure and coding of biometric data are biometric type (e.g. facial features, fingerprint) dependent and out of scope of this standard.

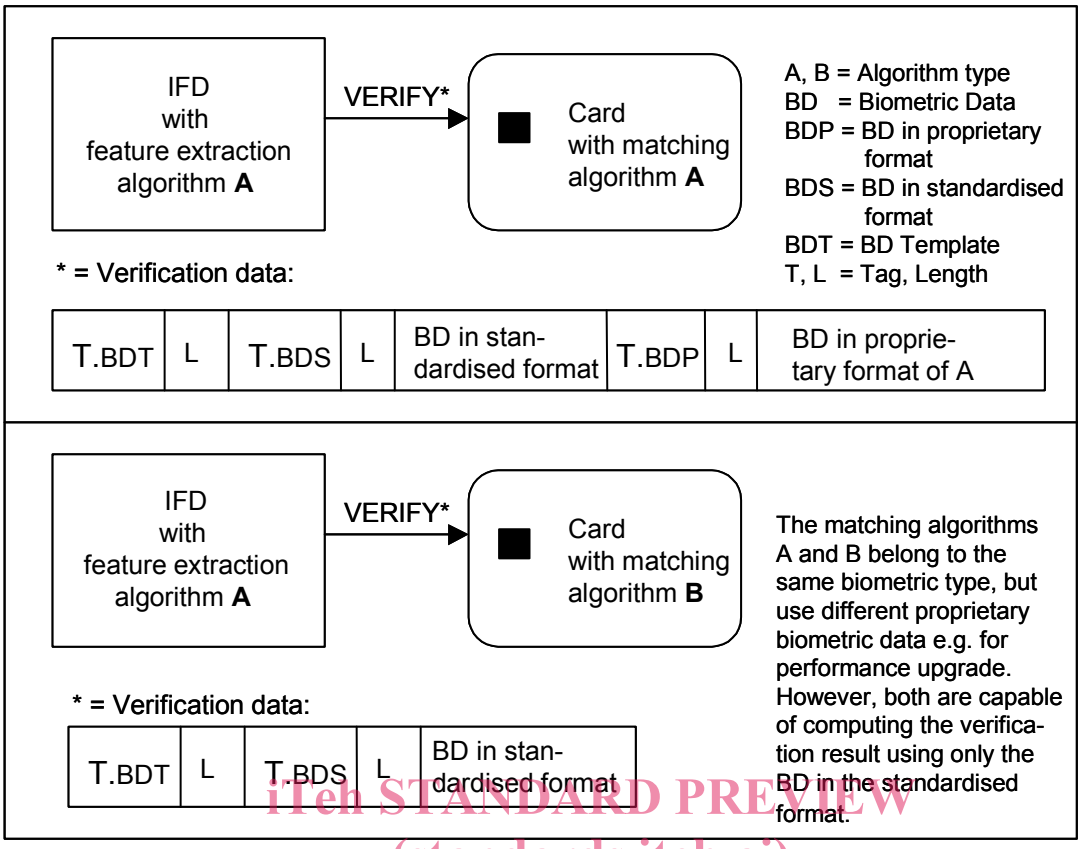




**Figure 1 — Use of biometric data with standardized and proprietary structure**



## 6.3 Verification requirement information

### 6.3.1 Purpose

The current verification requirement is provided either by

— the verification requirement information data object VIDO (tag '96', short format), or

— the verification requirement information template VIT (tag 'A6', long format).

VIDO or VIT, if present, is part of the file control parameter information of the respective DF or stored in a FCI extension file as defined in ISO/IEC 7816-4. VIDO and VIT contain information, which indicate whether the reference data for user verification (i.e. passwords and/or biometric data) are

— enabled or disabled and

— usable or unusable.

NOTE Usually the enabled/disabled flag is under control of the cardholder, the usable/unusable flag under control of the application provider.

### 6.3.2 VIDO – the short format

The first byte of the VIDO (see Table 4) indicates by bit map which keys (i.e. reference data for user verification) are enabled (bit set to 1) or disabled (bit set to 0). The second byte indicates by bit map which keys are usable (bit set to 1) or unusable (bit set to 0). Each of the following bytes are key references. The first key reference corresponds to bit b8 of the bit maps, the second key reference to bit b7, and so on. The number of key references is given implicitly by the length of the VIDO, e.g. when L is less than or equal to 10, the number of key references is L-2.

**Table 4 — VIDO structure**

| VIDO Tag | L | Enabled / disabled Flags | Usable / unusable Flags | Key Ref. | Key Ref. | ... |
|---|---|---|---|---|---|---|
| '96' | Var. | 'xx' | 'xx' | 'xx' | 'xx' | ... |

### 6.3.3 VIT – the long format

The VIT presents the information in long format, whereby additional information can be provided in the usage qualifier DO. The DOs, which may occur in a VIT, are shown in Table 5.

**Table 5 — Verification requirement information template (VIT) and embedded DOs**

| **Tag** | **L** | **Value** | | |
|---|---|---|---|---|
| 'A6' | Var. | Verification requirement information template | | |
| | | **Tag** | **L** | **Value** |
| | | '90' | 1 | Enabled/disabled flags (Flag DO) |
| | | '95' | 1 | Usage qualifier as defined in ISO/IEC 7816-4 |
| | | '83' | 1 | Key reference |



The enabled/disabled flags DO is mandatory. At least one key reference DO shall be present. Each key reference DO may be preceded by an associated usage qualifier DO. If no usage qualifier is associated to a key, then the usage is implicitly known. In this context, a usage qualifier set to zero means, the associated key shall not be used.



NOTE It is not necessary to introduce a VIT with an application tag to be retrieved by GET DATA, because the FCI or the FCI extension file can be read always.