INTERNATIONAL STANDARD

ISO/IEC 7816-11

Second edition
2017-12

Identification cards — Integrated circuit cards —

Part 11: Personal verification through biometric methods

Cartes d'identification — Cartes à circuit intégré —
Partie 11: Verification personelle par méthodes biométriques

Reference number
ISO/IEC 7816-11:2017(E)

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

Contents

Page

Foreword

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

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

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

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

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO/IEC 7816-11:2004), which has been technically revised. The main change is the addition of specification of PERFORM BIOMETRIC OPERATION command that enables ICCs to treat with various biometric operation flexibly.

A list of all parts in the ISO/IEC 7816 series can be found on the ISO website.

Introduction

The ISO/IEC 7816 series of standards specifies integrated circuit cards and the use of such cards for interchange. These cards are identification cards intended for information exchange negotiated between the outside world and the integrated circuit in the card. As a result of an information exchange, the card delivers information (computation result, stored data) and/or modifies its content (data storage, event memorization).

Five parts in the ISO/IEC 7816 series are specific to cards with galvanic contacts and three of them specify electrical interfaces.

— ISO/IEC 7816-1 specifies physical characteristics for cards with contacts.

— ISO/IEC 7816-2 specifies dimensions and location of the contacts.

— ISO/IEC 7816-3 specifies electrical interface and transmission protocols for asynchronous cards.

— ISO/IEC 7816-10 specifies electrical interface and answer to reset for synchronous cards.

— ISO/IEC 7816-12 specifies electrical interface and operation procedures for USB cards.

All of the other parts in the ISO/IEC 7816 series are independent from the physical interface technology. They apply to cards accessed by contacts and/or by radio frequency.

— ISO/IEC 7816-4 specifies organization, security and commands for interchange.

— ISO/IEC 7816-5 specifies registration of application providers.

— ISO/IEC 7816-6 specifies interindustry data elements for interchange.

— ISO/IEC 7816-7 specifies commands for structured card query language.

— ISO/IEC 7816-8 specifies commands for security operations.

— ISO/IEC 7816-9 specifies commands for card management.

— ISO/IEC 7816-11 specifies personal verification through biometric methods.

— ISO/IEC 7816-13 specifies commands for handling the life cycle of applications.

— ISO/IEC 7816-15 specifies cryptographic information application.

ISO/IEC 10536 (all parts) specifies access by close coupling. ISO/IEC 14443 (all parts) and ISO/IEC 15693 (all parts) specify access by radio frequency. Such cards are also known as contactless cards.

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 Authentication Context for Biometrics (ACBio) instance specified in ISO/IEC 24761, given in 6.2.

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:

Toshiba Corporation, Toshiba Solutions Corporation, 1-1, Shibaura 1-chome, Minato-ku, Tokyo 105-8001, Japan.

Identification cards — Integrated circuit cards —

Part 11: Personal verification through biometric methods

1 Scope

This document specifies security-related interindustry commands to be used for personal verification through biometric methods in integrated circuit cards. It also defines the data structure and data access methods for use of the card as a carrier of the biometric reference and/or as the device to perform the verification of the cardholder's biometric probe (on-card biometric comparison). Identification of persons using biometric methods is outside the scope of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37:2017, *Information technology — Vocabulary — Part 37: Biometrics*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and ISO/IEC 7816-4 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
biometric characteristic
biological and behavioural characteristic of an individual from which distinguishing, repeatable *biometric features* (3.5) can be extracted for the purpose of *biometric verification* (3.11)

3.2
biometric comparison
estimation, calculation or measurement of similarity or dissimilarity between *biometric probe* (3.8) and *biometric reference* (3.9)

3.3
biometric data
biometric sample (3.10) or aggregation of biometric samples at any stage of processing

EXAMPLE *Biometric reference* (3.9), *biometric probe* (3.8), *biometric feature* (3.5).

3.4
biometric data subject
individual whose individualized *biometric data* (3.3) is within the biometric system

[SOURCE: ISO/IEC 2382-37:2017, 3.7.5, modified — Note 1 to entry has not been included.]

3.5
biometric feature
numbers or labels extracted from *biometric samples* (3.10) and used for *biometric comparison* (3.2)

3.6
biometric feature extraction
process applied to a *biometric sample* (3.10) with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other biometric samples

[SOURCE: ISO/IEC 2382-37:2017, 3.5.4, modified — Notes to entry have not been included.]

3.7
biometric information
information needed by the outside world to construct the *biometric probe* (3.8)

3.8
biometric probe
data acquired during a *biometric verification* (3.11) in the course of the *biometric comparison* (3.2) with the *biometric reference* (3.9)

Note 1 to entry: The term "biometric verification data" was used in ISO/IEC 7816-11:2004.

3.9
biometric reference
one or more data objects, stored on ICC during enrolment, representing *biometric data* (3.3) of the person to be authenticated, of any *biometric characteristic* (3.1)

Note 1 to entry: The term "biometric reference data" was used in ISO/IEC 7816-11:2004.

3.10
biometric sample
analogue or digital representation of *biometric characteristics* (3.1) prior to *biometric feature extraction* (3.6)

3.11
biometric verification
process of verifying by a one-to-one *biometric comparison* (3.2) of the *biometric probe* (3.8) with *biometric reference* (3.9)

3.12
data acquisition
collection or attempt for collection of a *signal(s)* (3.20) from a *biometric characteristics(s)* (3.1), or a representation of a biometric characteristic(s), and conversion of the signal(s) to an acquired *biometric sample* (3.10) set

3.13
dynamic biometric verification
biometric verification (3.11) that requires a dynamic action from the person to be authenticated

Note 1 to entry: Examples of dynamic actions are speech, sign time series data, etc. with dynamically changed patterns. These actions may be used for *static biometric verification* (3.21) with fixed patterns.

3.14
enrolment processing
act of creating and storing a *biometric reference* (3.9) in accordance with an enrolment policy

3.15
externally-captured, adj.
which is captured outside ICC through *data acquisition* (3.12)

3.16
feedback mechanism
mechanism of informing devices outside of a biometric system on card of detailed error, warning or progress message complementing the status bytes by using card-originated byte strings

[SOURCE: ISO/IEC 17839-3:2016, 3.2, modified — The definition has been revised.]

3.17
internally-captured, adj.
which is captured in ICC through *data acquisition* (3.12)

3.18
raw data
sample acquired by *data acquisition* (3.12)

3.19
sensor
device to acquire a *biometric characteristic(s)* (3.1) and to convert it (them) to the *signal(s)* (3.20)

3.20
signal
sequence of analogue or digital output whose variations represent coded information

3.21
static biometric verification
biometric verification (3.11) that requires the presentation of a physiological (i.e. static) feature of the person to be authenticated or performance of an enrolled, pre-determined action

Note 1 to entry: Examples of physiological features are face, fingerprint, iris, vein, etc.

Note 2 to entry: Examples of performances of enrolled, pre-determined actions are gait, speech, sign time series data, etc. with fixed patterns.

3.22
template
concatenation of BER-TLV data objects, forming the value field of a constructed BER-TLV data object

Note 1 to entry: The term "template" means the value field of a constructed data object. It should not be confused with a processed *biometric data* (3.3) sample.

[SOURCE: ISO/IEC 7816-4:2013, 3.58, modified — Note 1 to entry has been added.]

4 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 7816-4 and the following apply.

ACBio	Authentication Context for Biometrics (see ISO/IEC 24761)
AID	Application Identifier
ASN.1	Abstract Syntax Notation One (see ISO/IEC 8825-1)
AT	Control Reference Template for Authentication
BDB	Biometric Data Block

BER	Basic Encoding Rules of ASN.1 (see ISO/IEC 8825-1)
BHT	Biometric Header Template
BPU	Biometric Processing Unit (see ISO/IEC 24761)
BRT certificate	Biometric Reference Template certificate (see ISO/IEC 24761)
CBEFF	Common Biometric Exchange Formats Framework
CCT	Control Reference Template for Cryptographic Checksum
CT	Control Reference Template for Confidentiality
DF	Dedicated File
DO	BER-TLV data object
DST	Control Reference Template for Digital Signature
FCI	File Control Information
ICC	Integrated Circuit Card
ID	Identifier
I/O	Input/Output
L	Length field of TLV DO
MAC	Message Authentication Code
MSE	MANAGE SECURITY ENVIRONMENT
OID	Object identifier
PBO	PERFORM BIOMETRIC OPERATION
RFU	Reserved for Future Use by ISO/IEC JTC 1/SC 17
SM	Secure Messaging
SMT	Secure Messaging Template
TLV	Tag, Length, Value
VIDO	Verification requirement Information Data Object
VIT	Verification requirement Information Template

5 Commands for biometric verification and its related processes

5.1 General

PERFORM BIOMETRIC OPERATION (PBO) command defined in 5.4 describes biometric operations for enrolment (storage of biometric data in an ICC) and verification (comparison of biometric data with reference data stored in the ICC). Both storage and comparison of biometric data may also be achieved by use of commands defined in ISO/IEC 7816-4 (e.g. PUT DATA, UPDATE BINARY for storage, VERIFY for comparison).

ACBio may be used by a validator to validate the authenticity of the biometric verification process (see ISO/IEC 24761). This is an alternative use case to validate the authenticity of the verification process (see 6.2).

5.2 Commands for a static biometric verification process

The commands to be used for a static verification process (see Annex A) shall be VERIFY command as specified in ISO/IEC 7816-4 or PERFORM BIOMETRIC OPERATION (PBO) command with relevant operations, e.g. comparison of biometric probe as specified in 5.4. When VERIFY command is used and the biometric data is externally captured, the command shall contain the biometric data as biometric probe to be compared in its data field, encoded as defined in 7.1 and 7.2. The biometric algorithm identifier shall be either

— implicitly known,

— defined in a security environment (SE) within a control reference template for authentication (AT),

— defined in a command data within a biometric information template (see ISO/IEC 24787), or

— defined in a command data within a control reference template for authentication.

The biometric reference qualifier may be either

— defined in a security environment (SE) within control reference template for authentication,

— defined in parameter P2 of VERIFY or PBO command,

— defined in a command data within a biometric information template (see 7.1),

— defined in a command data within a biometric data template (see 7.2), or

— defined in a command data within a control reference template for authentication.

The biometric probe may be encoded as BER-TLV data object (see Table 10). It may be recorded in a biometric information template (see Table 7 and Table 8) or a biometric information template group template (Table 9).

Biometric data captured either in ICC or out of ICC can be compared. In the case of comparing internally-captured biometric probe, feedback mechanism specified in ISO/IEC 17839-3 with the PBO operations in 5.4.6 should be implemented.

5.3 Commands for a dynamic biometric verification process

To get a challenge to which a user response is required (see Annex A), GET CHALLENGE command defined in ISO/IEC 7816-4 or PBO command defined in 5.4 shall be used.

As specified in ISO/IEC 7816-4, the P1 set to '00' means that no information is given, i.e. the biometric algorithm is known before issuing the command. Any other values of the P1 are RFU.

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. If the challenge is requested using GET CHALLENGE command, parameter P1 of GET CHALLENGE command shall identify the biometric algorithm. If the challenge is requested using PBO command, the biometric algorithm shall be either

— implicitly known, or

— defined in a security environment (SE) within control reference template for authentication.

The respective algorithm may be selected alternatively by using MSE command (e.g. SET option with AT, usage qualifier DO and algorithm reference DO in the command data field).

After receiving a biometric challenge, EXTERNAL AUTHENTICATE command or PBO command shall be sent to the ICC. The command data field conveys the relevant biometric probe.

5.4 Perform biometric operation command

5.4.1 General definition of PBO command

One or more PBO command(s) may be used for biometric verification and its related processes. It initiates various kinds of biometric operations and other relevant operations, in accordance with the value indicated in P1.

Table 1 — PERFORM BIOMETRIC OPERATION command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'2E'
P1	Function number and use case variant (see Table 4)
P2	See Table 2
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Data field	Absent or present in accordance with P1
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$

Data field	Absent or present in accordance with P1
SW1-SW2	As defined in ISO/IEC 7816-4:2013, Table 5 and Table 6 when relevant, e.g. '6281', '6282', '6700', '6981', '6982', '6A81', '6A82', '6A83'

In Table 1, P1 indicates single operation related to biometrics. In Table 2, P2 qualifies biometric reference in the same manner as for basic security handling command specified in ISO/IEC 7816-4.

Table 2 — P2 of PBO command

P2								Meaning
b8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0	0	0	0	0	No information given
0	—	—	—	—	—	—	—	Global biometric reference (e.g. MF specific)
1	—	—	—	—	—	—	—	Specific biometric reference (e.g. application DF specific)
—	x	x	—	—	—	—	—	00 (any other value is RFU)
—	—	—	x	x	x	x	x	Qualifier, i.e. number of the biometric reference

PBO command may be preceded by MSE command in order to set appropriate parameters. For example, MSE command set a control reference template valid for authentication (AT) to a security environment (SE). When PBO command executes, this SE may convey indication of biometric user authentication with qualifier of its biometric reference.

5.4.2 Operations of PBO command

The following list explains functionalities of PBO operations outlined in Table 3 and Table 4.

— SET INITIAL VALUES

  — SET INITIAL VALUES operation of PBO command is provided for setting initial values for biometrics.

