INTERNATIONAL STANDARD

ISO/IEC 7816-11

Third edition
2022-04

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 7816-11:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

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

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

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

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

This third edition cancels and replaces the second edition (ISO/IEC 7816-11:2017), which has been technically revised.

The main changes are as follows:

— In Subclause 5.4, functionality of `RETRIEVE BIOMETRIC REFERENCE` operation has been expanded to retrieve the following two different cases of biometric reference information:

  — including biometric reference;

  — not including biometric reference.

— In Subclause 5.4, new alternative names have been assigned to the following two operations of `PERFORM BIOMETRIC OPERATION` command:

  — `RETRIEVE BIOMETRIC REFERENCE` operation (to be deprecated)
  `RETRIEVE BIOMETRIC REFERENCE INFORMATION` operation (assigned)

  — `STORE BIOMETRIC INFORMATION` operation (to be deprecated)
  `STORE BRT CERTIFICATE` operation (assigned).

— In Table 4, according to ISO/IEC 24787:2018, the parameters to be used by `SET BIOMETRIC PARAMETER` operation has been added.

— In Table 8, the presence condition of tag allocation authority DOs has been clarified for the case of the default tag allocation authority.

— In Table 9, the format of a biometric information template has been modified and clarified for the following use cases:

  — The template conveys multiple sets of DOs defined by more than one compatible tag allocation authority.

  — An individual standard becomes a tag allocation authority within the template.

— In Table 10, the format of a biometric information template group template has been modified for explicit tag allocation coding, keeping backward compatibility to implicit tag allocation coding.

— In Table 11, biometric modality specific additional data DOs have been added as optional into a biometric data template to support existing biometric data format standards.

— In Figure 1, a use case has been copied from the first edition of ISO/IEC 7816-11, which sends two different formats of biometric probes at the same time.

— Annex C has been deleted.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

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 (this document) 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.

The ISO/IEC 10536 series specifies access by close coupling. The ISO/IEC 14443 series and the ISO/IEC 15693 series specify access by radio frequency. Such cards are also known as "contactless cards".

Identification cards — Integrated circuit cards —

Part 11:
Personal verification through biometric methods

1 Scope

This document specifies security-related interindustry commands that are intended 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, *Information technology — Vocabulary — Part 37: Biometrics*

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

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37, ISO/IEC 7816-4, ISO/IEC 24761, and the following apply.

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

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

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

3.1
biometric information
information needed by the outside world to construct the biometric probe

3.2
data acquisition
collection or attempt for collection of a signal(s) from a biometric characteristics(s), or a representation of a biometric characteristic(s), and conversion of the signal(s) to an acquired biometric sample set

3.3
biometric dynamic verification
verification process where the challenge from the integrated circuit card (ICC) is random and might not correspond to a biometric reference

Note 1 to entry: Actions taken by biometric dynamic verification are, e.g. speech, sign time series data, with dynamically changed patterns. These actions can be used for *biometric static verification* (3.9) with fixed patterns.

3.4
enrolment processing
act of creating and storing a biometric reference in accordance with an enrolment policy

3.5
externally-captured, adj.
captured outside the integrated circuit card (ICC) through *data acquisition* (3.2)

3.6
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 — Removed "defined in ISO/IEC 7816-4" at the end of the definition. Replaced "BSoC" with "Biometric System-on-Card".]

3.7
internally-captured, adj.
captured inside the integrated circuit card (ICC) through *data acquisition* (3.2)

3.8
sensor
device to acquire a biometric characteristic(s) and to convert it (them) to the signal(s)

3.9
biometric static verification
verification process that requires the presentation of a biometric sample without the need of a random challenge from the integrated circuit card (ICC)

Note 1 to entry: Examples of biometric type used in the process are, e.g. face, fingerprint, iris, vein.

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

3.10
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 sample.

[SOURCE: ISO/IEC 7816-4:2020, 3.59, 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

AT	Control Reference Template for Authentication
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
DF	Dedicated File
DO	BER-TLV data object
FCI	File Control Information
ICC	Integrated Circuit Card
I/O	Input/Output
L	Length field of TLV DO
MSE	MANAGE SECURITY ENVIRONMENT
OID	Object identifier
PBO	PERFORM BIOMETRIC OPERATION
RFU	Reserved for Future Use by ISO/IEC JTC 1/SC 17
SE	Security Environment
TLV	Tag, Length, Value
VIDO	Verification Information Data Object
VIT	Verification 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 can also be achieved by use of commands defined in ISO/IEC 7816-4 (e.g. PUT DATA, UPDATE BINARY for storage, VERIFY for comparison).

PBO command also supports ACBio defined in ISO/IEC 24761 (see 6.2).

5.2 Commands for a biometric static verification process

The commands to be used for a static verification process (see an example shown in 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 can be either

— defined in a 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 can be encoded as BER-TLV data object (see Table 11). It can be recorded in a biometric information template (see Table 8 and Table 9) or a biometric information template group template (see Table 10).

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 biometric dynamic verification process

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

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

If the challenge is requested using PBO command, the biometric algorithm shall be either

— implicitly known, or

— defined in a SE within control reference template for authentication.

Alternatively, the respective algorithm can be selected 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) can 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
INS	'2E'
P1	Function number and use case variant (see Table 5)
P2	See Table 2
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Command data field	Absent or present in accordance with P1 (see Table 4)
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$

Response data field	Absent or present in accordance with P1 (see Table 4)
SW1-SW2	As defined in ISO/IEC 7816-4:2020, Table 6 and Table 7 when relevant, e.g. '6281', '6282', '6700', '6981', '6982', '6A81', '6A82', '6A83'.
NOTE ISO/IEC 7816-4 defines INS = '2E' and '2F' for PBO command but this document defines '2E' only, and '2F' is reserved for future extension.	

In Table 1, P1 indicates single operation related to biometrics. In Table 2, P2 qualifies the 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 can 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 SE. When PBO command executes, this SE can convey an indication of biometric user authentication with qualifier of its biometric reference.

5.4.2 Operations of PBO command

Table 3 explains the functionalities of PBO operations outlined in Table 4 and Table 5.

Table 3 — PBO operation and functionality

Operation	Functionality
SET INITIAL VALUES	Setting initial values for biometrics
STORE BIOMETRIC REFERENCE	Enrolment of externally-captured biometric data
UPDATE BIOMETRIC REFERENCE	
CAPTURE AND STORE BIOMETRIC REFERENCE	Enrolment of internally-captured biometric data
CAPTURE AND UPDATE BIOMETRIC REFERENCE	
COMPARE BIOMETRIC PROBE	Comparison of externally-captured biometric probe with biometric reference
CAPTURE AND COMPARE BIOMETRIC PROBE	Comparison of internally-captured biometric probe with biometric reference

Table 3 *(continued)*

Operation	Functionality
RETRIEVE BIOMETRIC REFERENCE (to be deprecated)	Retrieval of biometric reference information from the ICC
RETRIEVE BIOMETRIC REFERENCE INFORMATION	
GENERATE BIOMETRIC VALIDATION CERTIFICATE	Generating ACBio instance
GENERATE CONTROL VALUE	Generating control value for biometrics
STORE BIOMETRIC INFORMATION (to be deprecated)	Storing externally generated certificate for a biometric reference
STORE BRT CERTIFICATE	
GET BIOMETRIC CHALLENGE	Getting biometric challenge before COMPARE BIOMETRIC PROBE or CAPTURE AND COMPARE BIOMETRIC PROBE operation in case of biometric dynamic verification process.
SET BIOMETRIC PARAMETER	Setting parameters such as card-specific biometric functionality information or application-specific biometric comparison parameters, and also application level timeout for the feedback mechanism of Biometric System-on-Card (see ISO/IEC 17839-3).
CONTINUE CAPTURE	Indicating to the ICC that the ongoing biometric sample acquisition process, which has reached its application level timeout, is to be continued.
ABORT CAPTURE	Indicating to the ICC that the ongoing biometric sample acquisition process, which has reached its application level timeout, is to be aborted.
NOTE SET BIOMETRIC PARAMETER, CONTINUE CAPTURE and ABORT CAPTURE operations of PBO command are provided for the feedback mechanism.	