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: Vérification 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.	

Table 4 — Command and response data field of PBO command

Operation	Command data field		Response data field	
SET INITIAL VALUES (see 6.2.2.1, 6.2.2.2, 6.2.3, 6.2.4.1 and 6.2.4.2)	DO'73'	Biometric initial value template (see Table 7)	—	Absent
STORE BIOMETRIC REFERENCE (see 5.4.3.1 and 6.2.2.1)		Biometric reference as:	—	Absent
	DO'7F2E'	Biometric data template		
	DO'7F60'	Biometric information template		
	DO'7F61'	Biometric information template group template		
UPDATE BIOMETRIC REFERENCE (see 5.4.3.1 and 6.2.2.1)		Biometric reference as:	—	Absent
	DO'7F2E'	Biometric data template		
	DO'7F60'	Biometric information template		
	DO'7F61'	Biometric information template group template		
CAPTURE AND STORE BIOMETRIC REFERENCE (see 5.4.3.2 and 6.2.2.2)	—	Absent	—	Absent
CAPTURE AND UPDATE BIOMETRIC REFERENCE (see 5.4.3.2 and 6.2.2.2)	—	Absent	—	Absent
COMPARE BIOMETRIC PROBE (see 5.4.5.1)		Biometric probe as:	—	Absent
	DO'7F2E'	Biometric data template		
	DO'7F60'	Biometric information template		
	DO'7F61'	Biometric information template group template		
CAPTURE AND COMPARE BIOMETRIC PROBE (see 5.4.5.2)	—	Absent	—	Absent
RETRIEVE BIOMETRIC REFERENCE (to be deprecated) or RETRIEVE BIOMETRIC REFERENCE INFORMATION (see 5.4.4 and 6.2.3)	—	Absent		Biometric reference information as:
			DO'7F60'	Biometric information template
			DO'7F61'	Biometric information template group template

NOTE 1 Biometric data template DO'7F2E' is defined in Table 11.

NOTE 2 Biometric information template DO'7F60' is defined in Table 8 and Table 9.

NOTE 3 Biometric information template group template is defined in Table 10.

NOTE 4 Biometric comparison parameters DO'B1' and biometric functionality information DO'B2' are defined in ISO/IEC 24787.

Table 4 *(continued)*

Operation	Command data field		Response data field	
GENERATE BIOMETRIC VALIDATION CERTIFICATE (see 6.2.2.1, 6.2.2.2, 6.2.3, 6.2.4.1 and 6.2.4.2)	DO'53'/ DO'73'/—	Reference data qualifier, reference data qualifier template or absent	DO'73'	Biometric certificate template
GENERATE CONTROL VALUE (see 6.2.2.1, 6.2.2.2, 6.2.2.3, 6.2.4.1 and 6.2.4.2)	—	Absent	DO'73'	Control value template
STORE BIOMETRIC INFORMATION (to be deprecated) or STORE BRT CERTIFICATE (see 6.2.2.3)	DO'A5'	Biometric information	—	Absent
GET BIOMETRIC CHALLENGE (see 5.4.5.1 and 5.4.5.2)	—	Absent	DO'53'/ DO'73'	Biometric challenge (primitive/constructed)
SET BIOMETRIC PARAMETER (see NOTE 4)	DO'B1'	Biometric comparison parameters	—	Absent
SET BIOMETRIC PARAMETER (see NOTE 4)	DO'B2'	Biometric functionality information	—	Absent
SET BIOMETRIC PARAMETER (see 5.4.6)	DO'89'	Application level timeout	—	Absent
CONTINUE CAPTURE (see 5.4.6)	—	Absent	—	Absent
ABORT CAPTURE (see 5.4.6)	—	Absent	—	Absent

NOTE 1 Biometric data template DO'7F2E' is defined in Table 11.

NOTE 2 Biometric information template DO'7F60' is defined in Table 8 and Table 9.

NOTE 3 Biometric information template group template is defined in Table 10.

NOTE 4 Biometric comparison parameters DO'B1' and biometric functionality information DO'B2' are defined in ISO/IEC 24787.

Bit b8 of P1 set to 0 is meant for general use case operations. Bit b8 of P1 set to 1 is meant for specific use case operations (see Table 5). This edition covers ACBio defined in ISO/IEC 24761 as specific use case (see 6.2). P1 as '00' and 'FF' are RFU.

Table 5 — Coding of P1 for PBO command

P1								Operations
b8	b7	b6	b5	b4	b3	b2	b1	
0	x	x	x	x	x	x	x	General use case
1	x	x	x	x	x	x	x	Specific use case
x	0	0	0	0	0	0	1	SET INITIAL VALUES
x	0	0	0	0	0	1	0	STORE BIOMETRIC REFERENCE
x	0	0	0	0	0	1	1	UPDATE BIOMETRIC REFERENCE
x	0	0	0	0	1	0	0	CAPTURE AND STORE BIOMETRIC REFERENCE
x	0	0	0	0	1	0	1	CAPTURE AND UPDATE BIOMETRIC REFERENCE
x	0	0	0	0	1	1	0	COMPARE BIOMETRIC PROBE
x	0	0	0	0	1	1	1	CAPTURE AND COMPARE BIOMETRIC PROBE
x	0	0	0	1	0	0	0	RETRIEVE BIOMETRIC REFERENCE (to be deprecated) or RETRIEVE BIOMETRIC REFERENCE INFORMATION
x	0	0	0	1	0	0	1	GENERATE BIOMETRIC VALIDATION CERTIFICATE
x	0	0	0	1	0	1	0	GENERATE CONTROL VALUE
x	0	0	0	1	0	1	1	STORE BIOMETRIC INFORMATION (to be deprecated) or STORE BRT CERTIFICATE
x	0	0	0	1	1	0	0	GET BIOMETRIC CHALLENGE
x	0	0	0	1	1	0	1	SET BIOMETRIC PARAMETER
x	0	0	0	1	1	1	0	CONTINUE CAPTURE
x	0	0	0	1	1	1	1	ABORT CAPTURE
x	x	x	x	x	x	x	x	Other values are RFU.

5.4.3 Enrolment of biometric reference

5.4.3.1 Enrolment of externally-captured biometric data

STORE BIOMETRIC REFERENCE and UPDATE BIOMETRIC REFERENCE operations of PBO command defined in Table 4 and Table 5 are provided for enrolment of externally-captured biometric data and for storing the resulting biometric reference together with related biometric information in the ICC.

5.4.3.2 Enrolment of internally-captured biometric data

CAPTURE AND STORE BIOMETRIC REFERENCE and CAPTURE AND UPDATE BIOMETRIC REFERENCE operations of PBO command defined in Table 4 and Table 5 are provided for enrolment of internally-captured biometric data and for storing the resulting biometric reference together with related biometric information in the ICC.

5.4.4 Retrieval of biometric reference information

RETRIEVE BIOMETRIC REFERENCE operation (to be deprecated) and RETRIEVE BIOMETRIC REFERENCE INFORMATION operation of PBO command defined in Table 4 and Table 5 is provided for retrieval of biometric reference or its associated public data encoded either within biometric information template or biometric information template group template from the ICC.

5.4.5 Comparison of biometric probe

5.4.5.1 Comparison of externally-captured biometric probe

COMPARE BIOMETRIC PROBE operation of PBO command defined in Table 4 and Table 5 is provided for comparison of externally-captured biometric probe with biometric reference. In case of biometric dynamic verification process, GET BIOMETRIC CHALLENGE operation of PBO command defined in Table 4 and Table 5 is provided for getting biometric challenge before COMPARE BIOMETRIC PROBE operation.

5.4.5.2 Comparison of internally-captured biometric probe

CAPTURE AND COMPARE BIOMETRIC PROBE operation of PBO command defined in Table 4 and Table 5 is provided for comparison of internally-captured biometric probe with biometric reference. In case of biometric dynamic verification process, GET BIOMETRIC CHALLENGE operation of PBO command defined Table 4 and Table 5 is provided for getting biometric challenge before CAPTURE AND COMPARE BIOMETRIC PROBE operation.

5.4.6 Feedback mechanism during biometric acquisition process

The acquisition of the biometric data during the enrolment or comparison requires a user interaction and the timing behaviour cannot be predicted. Therefore, the feedback mechanism specified in ISO/IEC 17839-3 should be used. SET BIOMETRIC PARAMETER, CONTINUE CAPTURE and ABORT CAPTURE operations of PBO command defined in Table 4 and Table 5 are provided for the feedback mechanism.

Table 6 indicates details of SET BIOMETRIC PARAMETER operation of PBO command for application level timeout management defined in ISO/IEC 17839-3.

Table 6 — Set application level timeout using SET BIOMETRIC PARAMETER operation of PBO command

Operation	P1	Command data field		Response data field	
SET BIOMETRIC PARAMETER (set application level timeout)	'0D'	DO'89'	An application level timeout specified in ISO/IEC 17839-3. If empty data object, the application level timeout is implicitly known.	—	Absent

6 Commands for specific use cases of biometric verification and its related processes

6.1 General

This clause provides commands of biometric verification and its related processes for specific use cases depending on other standards. The current edition provides only ACBio use case defined in ISO/IEC 24761 (see 6.2).

6.2 Use case for ISO/IEC 24761

6.2.1 Operations of PBO command

The operations of PBO command defined in Table 4 and Table 5 are employed for ACBio defined in ISO/IEC 24761 use case.

6.2.2 Enrolment of biometric reference

6.2.2.1 Enrolment of externally-captured biometric data

The main purpose of enrolment of externally-captured biometric data for ACBio is to store a biometric reference in an ICC. A typical sequence of PBO commands for this enrolment procedure is provided below:

— SET INITIAL VALUES operation to set a control value, input index and/or output index of BPU I/O, where BPU I/O is input/output communication lines of biometric processing unit defined in ISO/IEC 24761,

— STORE BIOMETRIC REFERENCE operation to store a biometric reference,

— GENERATE CONTROL VALUE operation to calculate the hash value of biometric reference, and

— GENERATE BIOMETRIC VALIDATION CERTIFICATE operation to generate ACBio instance.

The command data field of SET INITIAL VALUES operation of PBO command is specified in Table 7.

Table 7 — Data object of SET INITIAL VALUES operation of PBO command in case of ACBio use case

Tag	L	Value			Presence
'73'	Var.				—
		Tag	**L**	**Value**	
		'80'	Var.	Control value	Mandatory
		'81'	Var.	Input index of BPU I/O	Optional
		'82'	Var.	Output index of BPU I/O	Mandatory

6.2.2.2 Enrolment of internally-captured biometric data

The main purpose of enrolment of internally-captured biometric data for ACBio is to store the biometric data in an ICC. A typical sequence of PBO commands for this enrolment procedure is provided below:

— SET INITIAL VALUES operation to set a control value, input index and/or output index of BPU I/O (see Table 7),

— CAPTURE AND STORE BIOMETRIC REFERENCE operation to capture and to store a biometric reference,

— GENERATE CONTROL VALUE operation to calculate the hash value of biometric reference, and

— GENERATE BIOMETRIC VALIDATION CERTIFICATE operation to generate ACBio instance.

6.2.2.3 Enrolment of BRT certificate

After the procedure of enrolment of a biometric data (see 6.2.2.1 and 6.2.2.2) is executed, enrolment of BRT certificate is required. STORE BIOMETRIC INFORMATION operation (to be deprecated) or STORE BRT CERTIFICATE operation of PBO command defined in Table 4 and Table 5 is provided.

6.2.3 Retrieval of biometric reference information

The main purpose of retrieval of a biometric reference information for ACBio is to retrieve the biometric reference information from an ICC. A typical sequence of PBO commands for this retrieval procedure is provided below:

— SET INITIAL VALUES operation to set a control value, input index and/or output index of BPU I/O (see Table 7),

— RETRIEVE BIOMETRIC REFERENCE operation (to be deprecated) or RETRIEVE BIOMETRIC REFERENCE INFORMATION operation to retrieve a biometric reference information, and

— GENERATE BIOMETRIC VALIDATION CERTIFICATE operation to generate ACBio instance.

6.2.4 Comparison of biometric probe

6.2.4.1 Comparison of externally-captured biometric probe

The main purpose of the comparison of externally-captured biometric probe for ACBio is to compare the biometric probe with a biometric reference in an ICC. A typical sequence of PBO commands for this comparison procedure is provided below:

— SET INITIAL VALUES operation to set a control value, input index and/or output index of BPU I/O (see Table 7),

— COMPARE BIOMETRIC PROBE operation,

— GENERATE CONTROL VALUE operation to calculate the hash value of the result of biometric comparison, and

— GENERATE BIOMETRIC VALIDATION CERTIFICATE operation to generate ACBio instance.

6.2.4.2 Comparison of internally-captured biometric probe

The main purpose of the comparison of internally-captured biometric probe for ACBio is to compare the biometric probe with a biometric reference in an ICC. A typical sequence of PBO commands for this comparison procedure is provided below:

— SET INITIAL VALUES operation to set a control value, input index and/or output index of BPU I/O (see Table 7),

— CAPTURE AND COMPARE BIOMETRIC PROBE operation,

— GENERATE CONTROL VALUE operation to calculate the hash value of the result of biometric comparison, and

— GENERATE BIOMETRIC VALIDATION CERTIFICATE operation to generate ACBio instance.

7 Data elements

7.1 Biometric information

The biometric information template 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 8 and Table 9 define biometric information DOs. This document specifies two different formats for specifying biometric information. The difference is stated on

— the entity specifying the coding is implicitly defined by a specific application profile (known as implicit tag allocation coding), or

— the entity defining the coding is explicitly contained into the biometric information template (known as explicit tag allocation coding).

Table 8 is called an implicit tag allocation coding which is dedicated to importing legacy data formats (e.g. according to ISO/IEC 19785-3, Clause 11) into the biometric information template DO'7F60'. Table 9 is called an explicit tag allocation coding which enables the import of data objects from other tag allocation authorities according to the compatible tag allocation scheme specified in ISO/IEC 7816-4:2020, 8.3.5.

A biometric information template can include biometric data (see 7.2).

In case of off-card comparison, a biometric reference as biometric data should be included in a biometric information template because off-card verification needs both biometric reference and its information.

In case of on-card comparison and if the off-card system needs information regarding a biometric reference, a biometric information template without biometric data and a biometric data as a biometric reference should be stored separately in an ICC because this biometric reference should be protected against retrieving.

Table 8 — Biometric information DOs in biometric information template (implicit tag allocation coding)

<table>
<tr><th>Tag</th><th>L</th><th colspan="4">Value</th><th>Presence</th></tr>
<tr><td>'7F60'</td><td>Var.</td><td colspan="4">Biometric information template</td><td>—</td></tr>
<tr><td rowspan="11"></td><td rowspan="11"></td><td>Tag</td><td>L</td><td colspan="2">Value</td><td></td></tr>
<tr><td>'80'</td><td>1</td><td colspan="2">Algorithm reference of biometric verification</td><td>Optional</td></tr>
<tr><td>'83'</td><td>1</td><td colspan="2">Reference data qualifier of biometric verification</td><td>Optional</td></tr>
<tr><td>'A0'</td><td>Var.</td><td colspan="2">RFU for biometric information DOs to be defined in this document</td><td>Optional</td></tr>
<tr><td>'06'
'41'
'42'
'4F'</td><td>Var.</td><td colspan="2">Tag allocation authority (see ISO/IEC 7816-6) of biometric information DOs located under DO'A1' (By default, the tag allocation authority is ISO/IEC 19785-3, Clause 11).
— Object identifier (OID, encoding specified in ISO/IEC 8825-1) [a]
— Country code (encoding specified in ISO 3166-1) and optional national data
— Issuer identification number (encoding and registration specified in ISO/IEC 7812-1) and optional issuer data
— Application identifier (AID, encoding specified in ISO/IEC 7816-4)</td><td>In case that DO'A1' is present,
If the tag allocation authority is ISO/IEC 19785-3, Clause 11, then these tags need not be present. [b]
Otherwise, at most one choice is mandatory</td></tr>
<tr><td>'A1'</td><td>Var.</td><td colspan="2">Biometric information DOs specified by the tag allocation authority (see above).
TLV-encoded patron format is applied if the default tag allocation authority is specified.</td><td>Mandatory, if DO'A0' is not present</td></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td><td>Tag</td><td>L</td><td>Value</td><td></td></tr>
<tr><td>'8x'/'Ax'</td><td>Var.</td><td rowspan="2">DOs defined by the tag allocation authority (primitive/constructed)</td><td rowspan="2">DO dependent</td></tr>
<tr><td>'9x'/'Bx'</td><td>Var.</td></tr>
<tr><td>'5F2E' / '7F2E'</td><td>Var.</td><td colspan="2">Biometric data</td><td>(see 7.2)</td></tr>
</table>

[a] If the OID refers to NISTIR 6529, then the OID of the Computer Security Objects Register (CSOR) at NIST {joint-iso-itu-t (2) country (16) us (840) organization (1) gov (101) csor (3)} is used (hexadecimal coding of the OID is '608648016503').

[b] If ISO/IEC 19785-3, Clause 11 is specified by an OID DO'06' as the tag allocation authority, the OID is 1.1.19785.0.257.1.5, i.e. {iso(1) registration-authority(1) cbeff(19785) biometric-organization(0) jtc1-sc37(257) patron-format(1) tlv-encoded(5)} (hexadecimal coding of the OID is '29819A490082010105').

Table 9 — Biometric information DOs in biometric information template (explicit tag allocation coding)

Tag	L	Value							Presence
'7F60'	Var.	Biometric information template							—
		Tag	**L**	**Value**					
		'80'	1	Algorithm reference of biometric verification					Optional
		'83'	1	Reference data qualifier of biometric verification					Optional
		'A0'	Var.	RFU for biometric information DOs defined in this document					Optional
		'AX' [a] (X=1 to 4)	Var.	Biometric information DOs specified by other than this document					At least one DO'AX' (X=1 to 4) is mandatory, if DO'A0'is not present
				Tag	**L**	**Value**			
				'78'	Var.	Compatible tag allocation authority [b]			Mandatory, if explicit tag allocation coding is applied
						Tag	**L**	**Value**	
						'06'	Var.	Object identifier (OID, encoding specified in ISO/IEC 8825-1)	At most, one choice among these
						'41'	Var.	Country code (encoding specified in ISO 3166-1) and optional national data	
						'42'	Var.	Issuer identification number (encoding and registration specified in ISO/IEC 7812-1) and optional issuer data	
						'4F'	Var.	Application identifier (AID, encoding specified in ISO/IEC 7816-4)	
				'70'	Var.	Template for non-interindustry data objects, which is defined by the authority specified by DO'78' responsible for compatible tag allocation scheme. [c]			Mandatory, if DO'78' is present
		'5F2E' / '7F2E'	Var.	Biometric data					(see 7.2)

NOTE The default tag allocation authority is ISO/IEC 7816-6 managed by ISO/IEC JTC 1/SC 17.

[a] Application specific profiles can require multiple occurrences of the same DO'AX' within DO'7F60'.

[b] When an individual standard becomes a compatible tag allocation authority, the object identifier DO'06' within the DO'78' is chosen for indication of the standard number. For example, in case ISO/IEC 24787:2018 becomes a compatible tag allocation authority, the value field of DO'06' under Biometric information DO'A2' indicates its OID as {iso(1) standard(0) 24787 2018}, i.e. '28 81 C1 53 8F 62'.

[c] For example, in case ISO/IEC 24787:2018 is specified as the compatible tag allocation authority in DO'78', the biometric information DOs defined by ISO/IEC 24787:2018 are stored under DO'70'

EXAMPLE In the context of an ISO/IEC 19785-3, Clause 19 based product, DO'A1' is used for the CBEFF related information and DO'A2' is used for ISO/IEC 24787 related information. ISO/IEC 19785-3, Clause 19 allows only single occurrence of DO'A1' and DO'A2'.

If several biometric information templates are present within the same application, then they shall be grouped as shown in Table 10.

Further examples of biometric information template are shown in Annex B.

Table 10 — Biometric information template group template

Tag	L	Value			Presence
'7F61'	Var.	Biometric information template group template			—
		Tag	**L**	**Value**	
		'02'	Var.	Number of biometric information templates in the group	Mandatory if all of the biometric information template 1..n are formatted by implicit tag allocation coding (see Table 8)
		'7F60'	Var.	Biometric information template 1[a]	Conditional
		...	...	...	...
		'7F60'	Var.	Biometric information template n [a]	Conditional

[a] A biometric information template is formatted by either implicit tag allocation coding (see Table 8) or explicit tag allocation coding (see Table 9). These two different tag allocation codings shall not be present together in a single biometric information template group template.

7.2 Biometric data

Biometric data are not always present, but it is mandatory in the following cases:

— When sending a biometric probe to ICC (in case of on-card biometric comparison),

— When retrieving a biometric reference (in case of off-card biometric comparison), or

— When storing a biometric reference.

Biometric data are encoded in DO'5F2E' or DO'7F2E'. Table 11 indicates biometric data DOs which are included in a biometric data template. See 7.1.

Table 11 — Biometric data template

Tag	L	Value			Presence
'7F2E'	Var.	Biometric data template			—
		Tag	**L**	**Value**	
		'80'/'A0'	Var.	Challenge for cardholder prompting See Table 12 for DO'A0'	Optional, for biometric dynamic verification
		'91'-'95'	Var.	Biometric modality specific additional data	Optional, to be defined elsewhere (e.g. ISO/IEC 19794-2)
		'5F2E'	Var.	Biometric data	At least one of these DOs is present, if the template is used. The same tag number can exist multiple times under the template.
		'81'/'A1'	Var.	Biometric data in standardized format (primitive/constructed)	
		'82'/'A2'	Var.	Biometric data in proprietary format (primitive/constructed)	
		'83'	1	Biometric reference qualifier	Optional [a]

[a] This DO is used to reference biometric data within the biometric data template when the biometric data template is not stored in a biometric information template.

If DO'7F2E' is used for coding of biometric data, it is recommended to use DO'A1', and including the explicit tag allocation authority by adding DO'78' inside DO'A1'.

As shown in Table 11, biometric data can be split up in one part in standardized format and in one part in proprietary format, whereby the part in the proprietary format can be used, e.g. for achieving a better performance and/or employing intrinsic knowledge. The usage of biometric data in standardized and proprietary formats is shown in Figure 1. This example describes two kinds of algorithm references embedded on cards, indicated as X and Y, respectively. Both algorithms X and Y belong to the same biometric type, e.g. fingerprint, but can compute verification results by using different proprietary

format of biometric data as well as standardized format of biometric data. When an interface device supports only algorithm X, it can determine a format of biometric probe for the command data field of VERIFY command in accordance with an algorithm reference returned from an ICC.

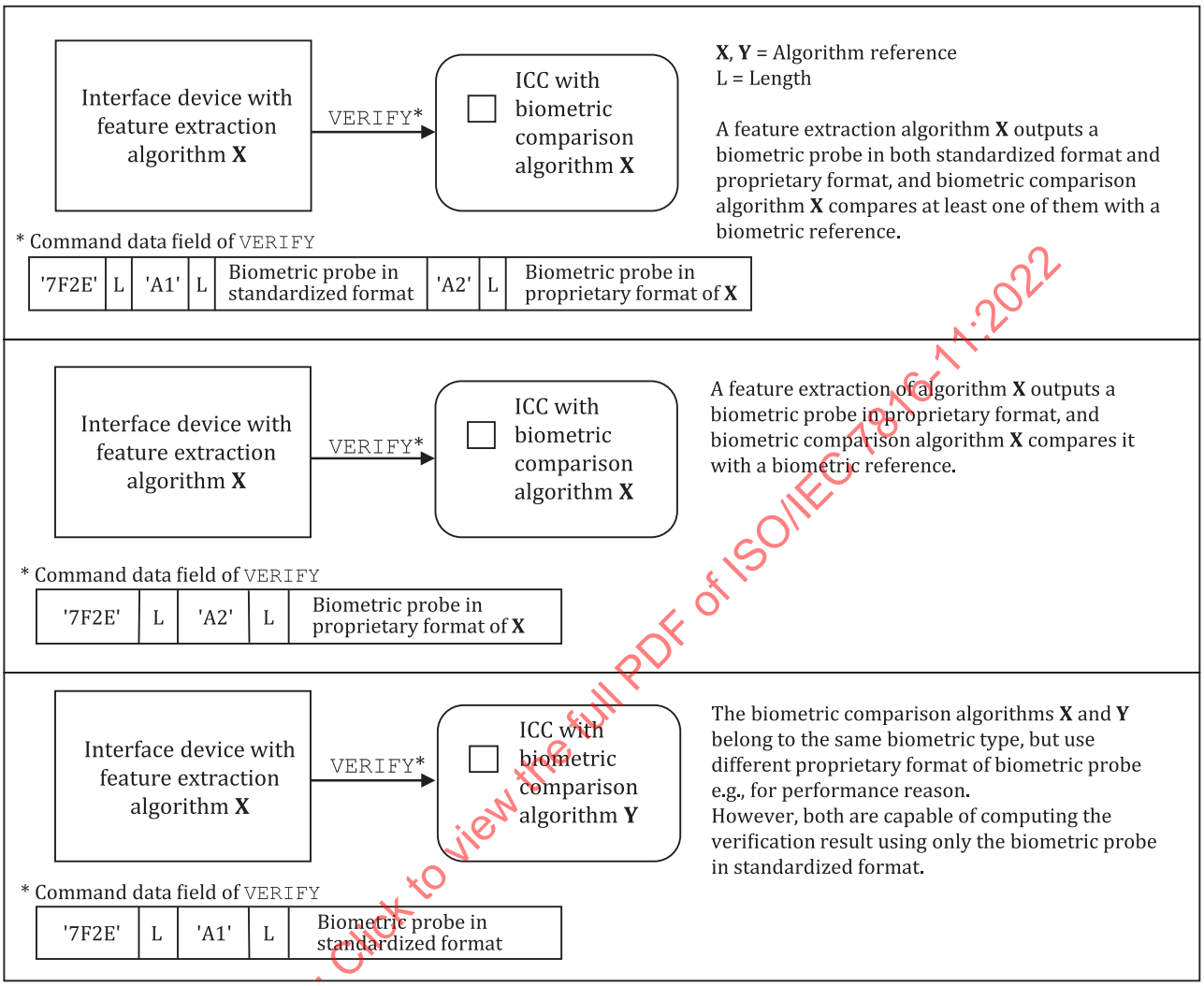

Figure 1 — Example use of biometric data in standardized and proprietary formats

Structure and coding of cardholder biometric reference and biometric probe in standardized format are biometric type (e.g. facial features, fingerprint) dependent, and it is out of the scope of this document.

Biometric challenge for cardholder prompting should be encoded under DO'A0' or DO'80' for biometric dynamic verification (see 5.3). A sample of biometric challenge template is shown in Table 12.

Table 12 — Biometric challenge prompting template

Tag	L	Value		
'A0'	Var.	Challenge template		
		Tag	**L**	**Value**
		'90'	Var.	Challenge qualifier '00': No information given (unspecified) '01': UTF8 coding (default) Any other value is RFU
		'80'	Var.	Challenge

7.3 Verification information

7.3.1 Purpose

The current verification information can be provided either by

— the verification information data object (VIDO) (tag '96', primitive), or

— the verification information template (VIT) (tag 'A6', constructed).

VIDO or VIT can be contained in the file control information (FCI) of the respective DF as defined in ISO/IEC 7816-4 or can be stored in an EF containing an extension of the FCI. For this purpose, DO'87' as identifier of an EF containing an extension of the FCI under file control parameter (FCP) template DO'62' for DF is defined in ISO/IEC 7816-4. VIDO and VIT contain information which indicates enable/disable verification requirement using a biometric reference. For switching this verification information state, `ENABLE VERIFICATION REQUIREMENT`/`DISABLE VERIFICATION REQUIREMENT` command defined in ISO/IEC 7816-4 can be used. VIDO and VIT also contain information which indicates whether further attempts of verification are allowed (usable) or not (unusable). When maximum tries of biometric verification are set and the number of consecutive biometric verification failure is reached to this maximum, the biometric reference is unusable. For switching unusable state into usable state, `RESET RETRY COUNTER` can be used if the security attribute allows this.

NOTE P2 field of `ENABLE VERIFICATION REQUIREMENT` or `DISABLE VERIFICATION REQUIREMENT` command indicates a qualifier, i.e. number of the reference data or number of the secret. A usage qualifier in a control reference template valid for authentication (AT) in the current SE can indicate whether user authentication is password-based (secret) or biometric-based (biometric reference). This usage qualifier in the current SE can be handled by using `MANAGE SECURITY ENVIRONMENT` (`MSE`) command.

7.3.2 Verification information data object (VIDO)

The first byte of the value field in a VIDO indicates enabled/disabled verification information of biometric references (see Table 13 and Table 14). Bit b8 of this byte indicates enabled/disabled verification information of the biometric reference referred to by the third byte of the value field in the VIDO. Each bit following b8 indicates enabled/disabled verification information of the biometric reference referred to by each byte following the third byte.

The second byte of the value field in a VIDO indicates the usability of biometric references (see Table 15). Bit b8 of this byte indicates the usability of the biometric reference referred to by the third byte of the value field in a VIDO. Each bit following b8 indicates the usability of the biometric reference referred to by each byte following the third byte.

Biometric reference qualifiers are at most eight in value field of a VIDO. When the number of biometric reference qualifiers is less than eight, the number of bits from b8 in first and second byte is valid.

Table 13 — Coding of verification information DO

Tag	L	Value			
		1st byte	2nd byte	3rd byte	...
'96'	3 to 10	Verification information byte	Usable biometric reference byte	Biometric reference qualifier corresponding to bit b8 in 1st and 2nd bytes	...

Table 14 — Coding of verification information byte

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	—	—	—	—	—	—	—	Enabled verification information using biometric reference referred to by the 3rd byte if present
—	1	—	—	—	—	—	—	The same as above for the 4th byte
—	—	1	—	—	—	—	—	The same as above for the 5th byte
—	—	—	1	—	—	—	—	The same as above for the 6th byte
—	—	—	—	1	—	—	—	The same as above for the 7th byte
—	—	—	—	—	1	—	—	The same as above for the 8th byte
—	—	—	—	—	—	1	—	The same as above for the 9th byte
—	—	—	—	—	—	—	1	The same as above for the 10th byte

Table 15 — Coding of usable biometric reference byte

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	—	—	—	—	—	—	—	Usable biometric reference referred to by the 3rd byte if present
—	1	—	—	—	—	—	—	The same as above for the 4th byte
—	—	1	—	—	—	—	—	The same as above for the 5th byte
—	—	—	1	—	—	—	—	The same as above for the 6th byte
—	—	—	—	1	—	—	—	The same as above for the 7th byte
—	—	—	—	—	1	—	—	The same as above for the 8th byte
—	—	—	—	—	—	1	—	The same as above for the 9th byte
—	—	—	—	—	—	—	1	The same as above for the 10th byte

7.3.3 Verification information template (VIT)

A VIT is provided for supporting more than eight biometric reference qualifiers (see Table 16). It consists of one or more biometric-based authentication templates DO'A4'. A biometric-based authentication template DO'A4' consists of verification requirement data object DO'81', usable biometric reference qualifier data object DO'82' and biometric reference qualifier data object DO'83'. Each of DO'81', DO'82' and DO'83' exists in DO'A4' at most once. Other DOs can exist in DO'A4'.