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: Vérification 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.

— STORE BIOMETRIC REFERENCE

— UPDATE BIOMETRIC REFERENCE

  — STORE BIOMETRIC REFERENCE and UPDATE BIOMETRIC REFERENCE operations of PBO command are provided for enrolment of externally-captured biometric data.

— CAPTURE AND STORE BIOMETRIC REFERENCE

— CAPTURE AND UPDATE BIOMETRIC REFERENCE

  — CAPTURE AND STORE BIOMETRIC REFERENCE and CAPTURE AND STORE BIOMETRIC operations of PBO command are provided for enrolment of internally-captured biometric data.

— COMPARE BIOMETRIC PROBE

  — COMPARE BIOMETRIC PROBE operation of PBO command is provided for comparison of externally-captured biometric probe with biometric reference.

— CAPTURE AND COMPARE BIOMETRIC PROBE

  — CAPTURE AND COMPARE BIOMETRIC PROBE operation of PBO command is provided for comparison of internally-captured biometric probe with biometric reference.

— RETRIEVE BIOMETRIC REFERENCE

  — RETRIEVE BIOMETRIC REFERENCE operation of PBO command is provided for retrieval of biometric reference from the ICC.

— GENERATE BIOMETRIC VALIDATION CERTIFICATE

  — GENERATE BIOMETRIC VALIDATION CERTIFICATE operation of PBO command is provided for generating biometric certificate validated.

— GENERATE CONTROL VALUE

  — GENERATE CONTROL VALUE operation of PBO command is provided for generating control value for biometrics.

— STORE BIOMETRIC INFORMATION

  — STORE BIOMETRIC INFORMATION operation of PBO command is provided for storing externally generated certificate for a biometric reference.

— GET BIOMETRIC CHALLENGE

  — GET BIOMETRIC CHALLENGE operation of PBO command is provided for getting biometric challenge before COMPARE BIOMETRIC PROBE or CAPTURE AND COMPARE BIOMETRIC PROBE operation in case of dynamic biometric verification process.

— SET BIOMETRIC PARAMETER

— CONTINUE CAPTURE

— ABORT CAPTURE

  — SET BIOMETRIC PARAMETER, CONTINUE CAPTURE and ABORT CAPTURE operations of PBO command are provided for the feedback mechanism.

Table 3 — 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	—	*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 (see 5.4.4 and 6.2.3)	—	*Absent*		Biometric reference as:
			DO'7F60'	biometric information template
			DO'7F61'	biometric information template group template

NOTE 1 Biometric data template DO'7F2E' is defined in Table 10.

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

NOTE 3 Biometric information template group template is defined in Table 9.

NOTE 4 DO'B1' encapsulated in a biometric information template DO'7F60' as data objects for configuration data elements is defined in ISO/IEC 24787.

Table 3 *(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 (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 template (primitive/constructed)
SET BIOMETRIC PARAMETER (see 5.4.6)	DO'B1'	Data objects for configuration data elements	—	*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 10.

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

NOTE 3 Biometric information template group template is defined in Table 9.

NOTE 4 DO'B1' encapsulated in a biometric information template DO'7F60' as data objects for configuration data elements is defined in ISO/IEC 24787.

Bit 8 of P1 set to 0 is meant for general use case operations. Bit 8 of P1 set to 1 is meant for specific use case operations (see Table 4). This edition covers ACBio defined in ISO/IEC 24761 as specific use case (see 6.2). P1 as '00' and 'FF' are RFU.

Table 4 — 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
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
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 3 and Table 4 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 3 and Table 4 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

RETRIEVE BIOMETRIC REFERENCE operation of PBO command defined in Table 3 and Table 4 is provided for retrieval of biometric reference 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 3 and Table 4 is provided for comparison of externally-captured biometric probe with biometric reference. In case of dynamic biometric verification process, GET BIOMETRIC CHALLENGE operation of PBO command defined in Table 3 and Table 4 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 3 and Table 4 is provided for comparison of internally-captured biometric probe with biometric reference. In case of dynamic biometric verification process, GET BIOMETRIC CHALLENGE operation of PBO command defined Table 3 and Table 4 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 3 and Table 4 are provided for the feedback mechanism.

Table 5 indicates details of SET BIOMETRIC PARAMETER operation of PBO command for application level timeout management defined in ISO/IEC 17839-3.

Table 5 — 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 3 and Table 4 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. The procedure of this enrolment with related processes may consist of four consecutive PBO commands with operations defined in Table 3 and Table 4 as below:

— to execute PBO command with 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,

— to execute PBO command with STORE BIOMETRIC REFERENCE operation to store a biometric reference,

— to execute PBO command with GENERATE CONTROL VALUE operation to calculate its hash value, and

— to execute PBO command with 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 6.

Table 6 — 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. The procedure of this enrolment with related processes may consist of four consecutive PBO commands with operations defined in Table 3 and Table 4 as below:

— to execute PBO command with SET INITIAL VALUES operation to set a control value, input index and/or output index of BPU I/O (see Table 6),

— to execute PBO command with CAPTURE AND STORE BIOMETRIC REFERENCE operation to capture and to store a biometric reference,

— to execute PBO command with GENERATE CONTROL VALUE operation to calculate its hash value, and

— to execute PBO command with 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 of PBO command defined in Table 3 and Table 4 is provided.

6.2.3 Retrieval of biometric reference

The main purpose of retrieval of a biometric reference for ACBio is to retrieve the biometric reference from an ICC. The procedure of this retrieval with its related processes may consist of three consecutive PBO commands with operations defined in Table 3 and Table 4 as below:

— to execute PBO command with SET INITIAL VALUES operation to set a control value, input index and/or output index of BPU I/O (see Table 6);

— to execute PBO command with RETRIEVE BIOMETRIC REFERENCE operation to retrieve a biometric reference;

— to execute PBO command with 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. The procedure of this comparison with its related processes may consist of four consecutive PBO commands with operations defined in Table 3 and Table 4 as below:

— to execute PBO command with SET INITIAL VALUES operation to set a control value, input index and/or output index of BPU I/O (see Table 6);

— to execute PBO command with COMPARE BIOMETRIC PROBE operation;

— to execute PBO command with GENERATE CONTROL VALUE operation to calculate the hash value of the result of biometric comparison;

— to execute PBO command with 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. The procedure of this comparison with its related processes may consist of four consecutive PBO commands with operations defined in Table 3 and Table 4 as below:

— to execute PBO command with SET INITIAL VALUES operation to set a control value, input index and/or output index of BPU I/O (see Table 6);

— to execute PBO command with CAPTURE AND COMPARE BIOMETRIC PROBE operation;

— to execute PBO command with GENERATE CONTROL VALUE operation to calculate the hash value of the result of biometric comparison;

— to execute PBO command with 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 7 and Table 8 define biometric information DOs.

A biometric information template may 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 7 — 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="9"></td><td rowspan="9"></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.
Var.
Var.
Var.</td><td colspan="2">Tag allocation authority (see ISO/IEC 7816-6):
— Object identifier (OID, encoding specified in ISO/IEC 8825-1)
— 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
The default tag allocation authority is ISO/IEC JTC 1/SC 37.</td><td>At most, one choice is mandatory if ‘A1’ is present</td></tr>
<tr><td>‘A1’</td><td>Var.</td><td colspan="2">Biometric information DOs specified by the tag allocation authority (mandatory indication, see above).
See TLV-encoded patron format specified in ISO/IEC 19785-3.</td><td>Mandatory, if ‘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’
‘9x’/‘Bx’</td><td>Var.
Var.</td><td>DOs defined by the tag allocation authority
... (primitive/constructed)
... (primitive/constructed)</td><td>DO dependent</td></tr>
<tr><td>‘5F2E’/‘7F2E’</td><td>Var.</td><td colspan="2">Biometric data (see 7.2)</td><td>Mandatory as biometric probe, or retrieved biometric reference in case of off-card biometric comparison</td></tr>
</table>

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

<table>
<tr><th>Tag</th><th>L</th><th colspan="5">Value</th><th>Presence</th></tr>
<tr><td>‘7F60’</td><td>Var.</td><td colspan="5">Biometric information template</td><td></td></tr>
<tr><td rowspan="15"></td><td rowspan="15"></td><td>Tag</td><td>L</td><td colspan="3">Value</td><td></td></tr>
<tr><td>‘80’</td><td>1</td><td colspan="3">Algorithm reference of biometric verification</td><td>Optional</td></tr>
<tr><td>‘83’</td><td>1</td><td colspan="3">Reference data qualifier of biometric verification</td><td>Optional</td></tr>
<tr><td>‘A0’</td><td>Var.</td><td colspan="3">RFU for biometric information DOs defined in this document</td><td>Optional</td></tr>
<tr><td>‘A1’</td><td>Var.</td><td colspan="3">Biometric information DOs specified by other than this document</td><td>Mandatory, if ‘A0’ is not present</td></tr>
<tr><td rowspan="10"></td><td rowspan="10"></td><td>Tag</td><td>L</td><td colspan="2">Value</td><td></td></tr>
<tr><td>‘78’</td><td>Var.</td><td colspan="2">Compatible tag allocation authority</td><td>Mandatory, if ‘A1’ is present</td></tr>
<tr><td rowspan="5"></td><td rowspan="5"></td><td>Tag</td><td>L</td><td>Value</td><td></td></tr>
<tr><td>‘06’</td><td>Var.</td><td>Object identifier (OID, encoding specified in ISO/IEC 8825-1)</td><td rowspan="4">At most, one choice among these</td></tr>
<tr><td>‘41’</td><td>Var.</td><td>Country code (encoding specified in ISO 3166-1) and optional national data</td></tr>
<tr><td>‘42’</td><td>Var.</td><td>Issuer identification number (encoding and registration specified in ISO/IEC 7816-1) and optional issuer data</td></tr>
<tr><td>‘4F’</td><td>Var.</td><td>Application identifier (AID, encoding specified in ISO/IEC 7816-4)</td></tr>
<tr><td>‘70’</td><td>Var.</td><td colspan="2">Biometric information DOs specified by the tag allocation authority</td><td>Optional</td></tr>
<tr><td></td><td></td><td>‘B1’</td><td>Var.</td><td>Biometric information DOs specified in ISO/IEC 24787</td><td></td></tr>
<tr><td>‘5F2E’/ ‘7F2E’</td><td>Var.</td><td colspan="3">Biometric data (see 7.2)</td><td>Mandatory as biometric probe, or retrieved biometric reference in case of off-card biometric comparison</td></tr>
<tr><td colspan="8">NOTE If compatible tag allocation authority DO‘78’ under DO‘A1’ does not exist, the default tag allocation authority is ISO/IEC JTC 1/SC 17.</td></tr>
</table>

The tags shown in Annex C may exist in the biometric information template in the case of explicit tag allocation coding (see Table 8).

If several biometric information templates are present within the same application, then they shall be grouped as shown in Table 9.

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

Table 9 — 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
		'7F60'	Var.	biometric information template 1	Conditional
		...			
		'7F60'	Var.	biometric information template n	Conditional

7.2 Biometric data

Biometric data are encoded in DO'5F2E' or DO'7F2E' as defined in ISO/IEC 7816-6. Table 10 indicates biometric data DOs which may be included in a biometric information template. See 7.1.

Table 10 — Biometric data DOs

Tag	L	Value			Presence
'7F2E'	Var.	Biometric data template			
		Tag	**L**	**Value**	
		'80'/'A0'	Var.	Challenge for cardholder prompting See Table 11 for DO'A0'	Optional, for dynamic biometric verification
		'5F2E'	Var.	Biometric data	At least one of these DOs is present, if the template is used. The same tag number may 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	If a biometric data template is not in a biometric information template, this DO may exist.

As shown in Table 10, biometric data may be split up in one part in standardized format and in one part in proprietary format, whereby the part in the proprietary format may 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, respectively. Both algorithms belong to the same biometric type, e.g. fingerprint, but can compute verification results by using different proprietary biometric data as well as standardized biometric data. When an interface device supports only algorithm **A**, it can determine a biometric probe for the command data field of VERIFY command in accordance with an algorithm reference returned from an ICC.

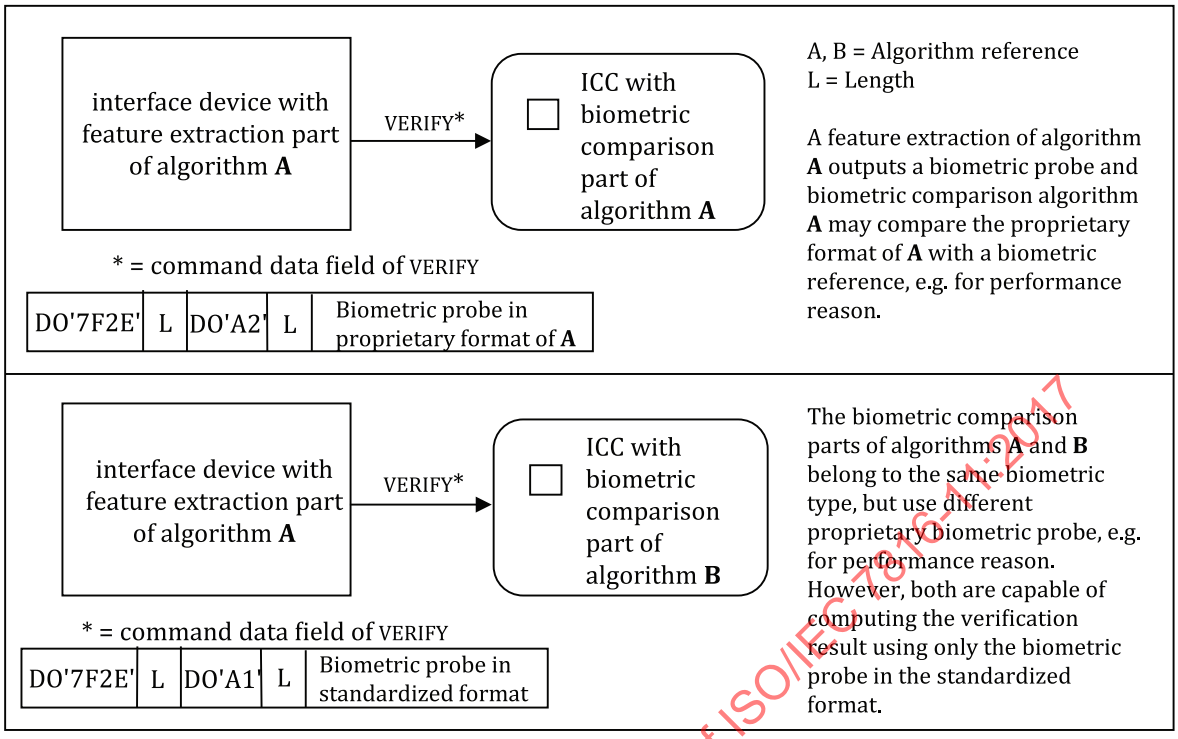

Figure 1 — Example use of biometric data in standardized and proprietary formats

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 dynamic biometric verification (see 5.3). A sample of biometric challenge template is shown in Table 11.

Table 11 — Biometric challenge template

Tag	L	Value		
'A0'	Var.	Challenge template		
		Tag	**L**	**Value**
		'90'	Var.	Challenge qualifier '00' = No information given (unspecified) '01' = UTF8 coding (default) Other values are RFU
		'80'	Var.	Challenge

7.3 Verification information

7.3.1 Purpose

The current verification information may 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 may be contained in the file control information of the respective DF as defined in ISO/IEC 7816-4 or may be stored in an EF containing an extension of the file control information. For this purpose, DO'87' as identifier of an EF containing an extension of the file control information 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 may 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 may 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 security environment (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 value field in a verification information data object (VIDO) indicates verification information of biometric references (see Table 12 and Table 13). Bit b8 of this byte indicates enabled/disabled verification information of biometric references (see Table 14) referred to by the third byte of value field in a VIDO, if it is present. Each bit followed by b8 indicates verification information of a biometric reference referred to by each byte followed by the third byte.

The second byte of value field in a VIDO indicates usable biometric references (see Table 14). Bit b8 of this byte indicates usable/unusable of a biometric reference referred to by the third byte of value field in a VIDO, if it is present. Each bit followed by b8 indicates usable of a biometric reference referred by each byte followed by 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 12 — 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 b8 in 1st and 2nd bytes	...

Table 13 — 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 14 — 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 verification information template is provided for supporting more than eight biometric reference qualifiers (see Table 15). 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 may exist in DO'A4'.

Table 15 — Coding of verification information template (VIT)

Tag	L	Value				
'A6'	Var.	Verification information template (VIT)				
		Tag	**L**	**Value**		
		'A4'	Var.	Biometric based authentication template		
				Tag	**L**	**Value**
				'81'	1	Verification requirement data object — '00': disabled verification requirement — '01': enabled verification requirement — any other value is RFU
				'82'	1	Usable biometric reference qualifier data object — '00': unusable biometric reference qualifier — '01': usable biometric reference qualifier — any other value is RFU
				'83'	1	Biometric reference qualifier data object
		'A4'	Var.	Biometric based authentication template		

Annex A
(informative)

Biometric verification process

A.1 Enrolment process and verification process

The general (simplified) schemes for enrolment processes are shown in Figure A.1 and Figure A.2.

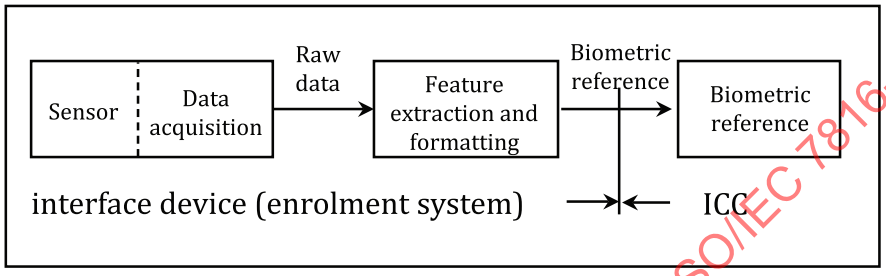

Figure A.1 — General scheme of an enrolment process of externally-captured biometric data

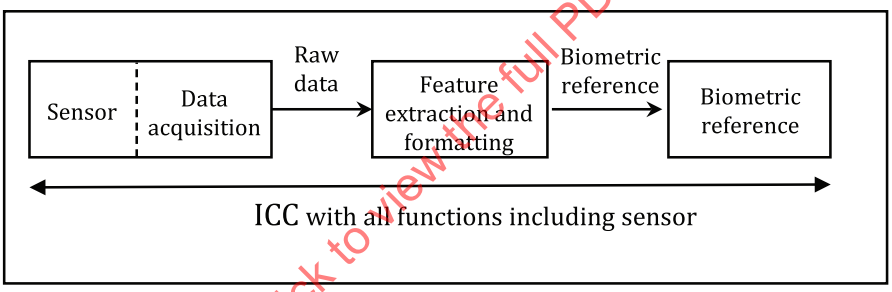

Figure A.2 — General scheme of an enrolment process of internally-captured biometric data

In case of enrolment of externally-captured biometric data (Figure A.1), a biometric sample is usually processed outside the card due to the considerable size of the biometric sample. During this processing, the biometric features are extracted and formatted for later use. In the enrolment processing or at a later stage, the biometric reference is sent in a secure way to the card for storage and subsequent use.

There are ICCs containing the sensor and data acquisition module that can enrol internally-captured biometric data (Figure A.2). In this case, they capture the biometric sample, process it and store the biometric reference data internally.

For both schemes, parameters related to biometric verification may be stored during enrolment processing.

Biometric reference may be stored in the card

— during a card personalization phase, or

— after issuing the card to the cardholder.

ISO/IEC 24787 shows simplified schemes for verification.

A.2 Classification of biometric verification methods

Biometric modalities can be categorized into two types.

The main characteristics of the first biometric type (type A) features are

— unique, not modifiable,

— selectable, if several instances of the same kind exist (e.g. thumb, pointer finger), and

— public, if the respective feature (e.g. face, ear, fingerprint) should be captured or measured by everybody, i.e. the respective biometric probe should be presented to the card in an authentic way.

The main characteristics of the second biometric type (type B) features are

— unique, but modifiable, and

— challenge dependent, if dynamic verification is used.

Examples of biometric type A:

— ear shape;

— facial features;

— finger geometry;

— fingerprint;

— hand geometry;

— iris;

— palm geometry;

— retina;

— vein pattern.

Examples of biometric type B:

— keystroke dynamics;

— lip movements;

— signature image;

— speech pattern (voiceprint);

— write dynamics (signature dynamics).

Taking into account the different message exchanges between the card and the interface device, the following classification is used.

— Static biometric verification: biometric types A and B are used.

— Dynamic biometric verification: biometric type B is used.

Figures A.3 and A.4 illustrate the differences between static and dynamic biometric verification at the card interface in case of biometric comparison and decision processing on the card.