PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Contents

Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

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

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

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

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

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

— *Part 5: Registration of application providers*

— *Part 6: Interindustry data elements for interchange*

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

— *Part 8: Commands for security operations*

— *Part 9: Commands for card management*

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

— *Part 11: Personal verification through biometric methods*

— *Part 15: Cryptographic information application*

Introduction

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

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

Identification cards — Integrated circuit cards with contacts —

Part 11:
Personal verification through biometric methods

1 Scope

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

3 Terms and definitions

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

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

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

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

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

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

3.6
template
as defined in ISO/IEC 7816-4

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

4   Abbreviated terms

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

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

5   Commands for biometric verification processes

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

5.1   Commands to retrieve biometric information

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

5.2 Command for a static biometric verification process

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

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

— biometric verification data.

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

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

5.3 Commands for a dynamic biometric verification process

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

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

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

6 Data elements

6.1 Biometric information

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

Table 1 — Biometric information DOs

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

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

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

Table 2 — BIT group template

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

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

⎯ a GET DATA command

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

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

6.2   Biometric data

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

⎯   as a concatenation of data elements,

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

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

Table 3 — Biometric data DOs

Tag	L	Value				Presence
'5F2E'	Var.	Biometric data				
'7F2E'	Var.	Biometric data template				
		Tag	**L**	**Value**		
		'5F2E'	Var.	Biometric data		At least one of these DOs is present, if the template is used
		'81' / 'A1'	Var.	Biometric data with standardised format (primitive / constructed)		
		'82' / 'A2'	Var.	Biometric data with proprietary format (primitive / constructed)		

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

Structure and coding of biometric data are biometric type (e.g. facial features, fingerprint) dependent and out of scope of this standard.
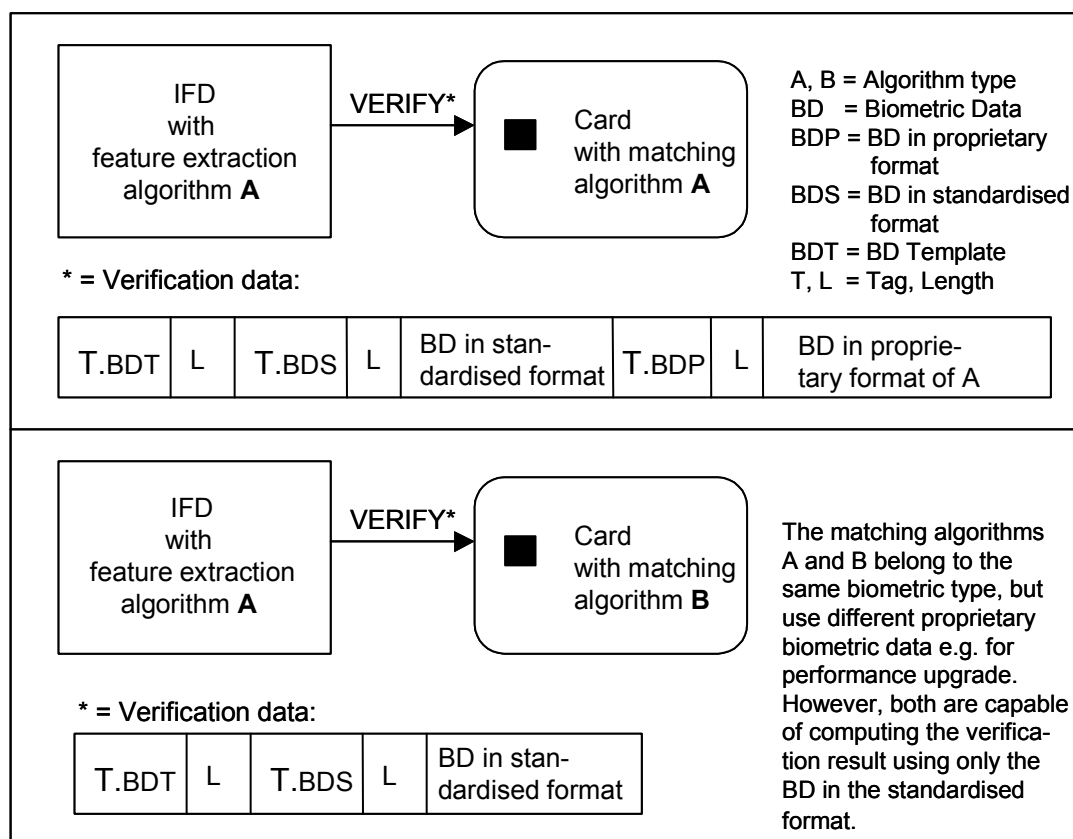
Figure 1 — Use of biometric data with standardized and proprietary structure

6.3 Verification requirement information

6.3.1 Purpose

The current verification requirement is provided either by

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

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

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

— enabled or disabled and

— usable or unusable.

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

6.3.2 VIDO – the short format

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

Table 4 — VIDO structure

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

6.3.3   VIT – the long format

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

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

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

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

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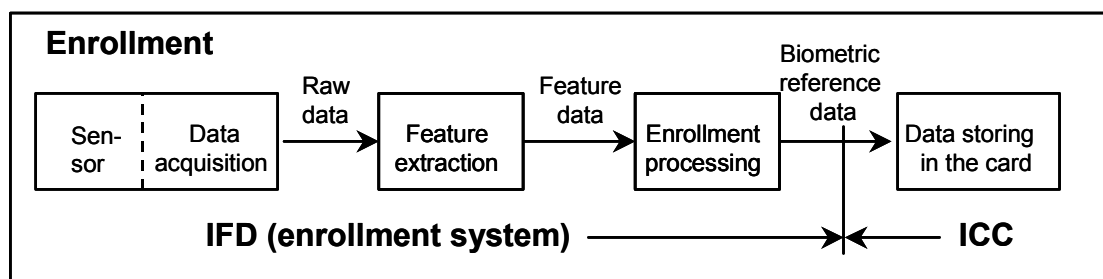
Annex A
(informative)

Biometric verification process

A.1 Abbreviations

ICC   Integrated Circuit(s) Card
IFD   Interface Device
OID   Object Identifier
SM   Secure Messaging

A.2 Enrollment process and verification process

The general (simplified) scheme for an enrollment process is shown in Figure A.1.

Figure A.1 — General scheme of an enrollment process

The sensor and data acquisition module are considered to be one logical unit although they may be separate modules. The raw data is usually processed outside the card due to the considerable size of the raw data. During this processing, the biometric features are extracted and formatted for later use. In the enrollment processing or at a later stage, the biometric reference data possibly together with additional information are sent in a secure way to the card for storage and subsequent use.

In case of on-card matching, these data cannot be retrieved after storing. In case of off-card matching, the biometric reference data can be retrieved as part of the BIT. The biometric reference data or possibly the whole BIT may be secured, e.g. by a digital signature. Also the access to the BIT may be restricted, e.g. access possible only after successful performance of an authentication procedure.

Biometric reference data may be stored in the card

⎯ during a card personalization phase, or

⎯ after issuing the card to the cardholder.

The storing of reference data after issuing of the card to the cardholder or when delivering the card to the cardholder is addressed in Annex B.

Figure A.2 shows a simplified scheme for a verification covering the following configurations:

⎯ with the biometric reference data and possibly parameters stored in the card

⎯ with matching and decision processing in the card

⎯ with feature extraction, formatting, matching and decision processing in the card

⎯ with a sensor on the card and performance of the whole verification process in the card.

Other configurations are possible.
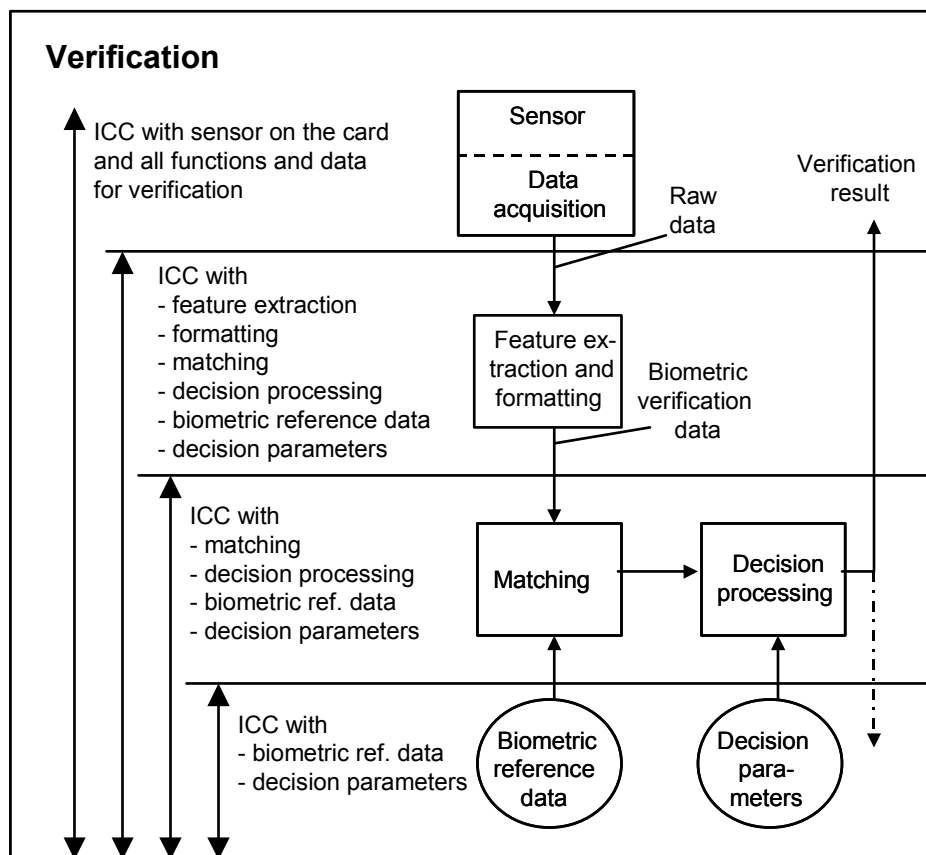
Figure A.2 — General scheme of a verification process

NOTE   Decision parameters are usually bound to the decision processing. When the card provides the biometric reference data (possibly cryptographically protected) for outside matching (lowest case in Figure A.2), decision parameters may only be present and retrievable (in a secure way), if they contain user specific components.

A.3 Classification of biometric verification methods

Taking into account the different message exchanges between the card and the IFD, the following classification is used:

— Static biometric verification method:
   a biometric verification method which requires the presentation of a physiological (i.e. static) feature of a person to be authenticated (see type A) or performance of an enrolled, pre-determined action (see type B).

— Dynamic biometric verification method:
   a biometric verification method which requires a dynamic action from the person to be authenticated (i.e. a user response to a biometric challenge, see type B).

Examples of biometric type A:

Ear shape
Facial features
Finger geometry
Fingerprint
Hand geometry
Iris
Palm geometry
Retina
Vein pattern

NOTE   These biometric types can only be used for static verification.

Examples of biometric type B:

Keystroke dynamics
Lip movements
Signature image
Speech pattern (voiceprint)
Write dynamics (signature dynamics)

NOTE   These biometric types may be used either for static verification or dynamic verification depending on the usage of the respective type.

The main characteristics of biometric type A features are

⎯ unique, not modifiable

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

⎯ public, if the respective feature (e.g. face, ear, fingerprint) can be captured or measured by everybody, i.e. the respective biometric verification data have to be presented to the card in an authentic way (see Annex B, Figure B.4).

The main characteristics of biometric type B features are

⎯ unique, but modifiable

⎯ challenge dependent, if dynamic verification is used.

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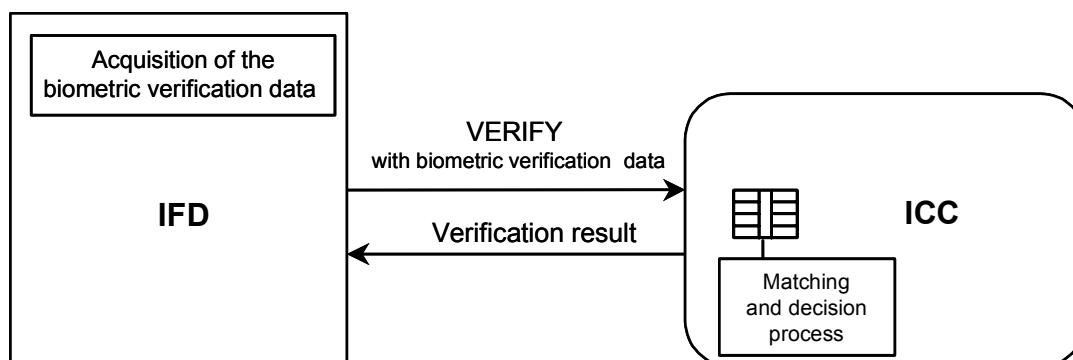

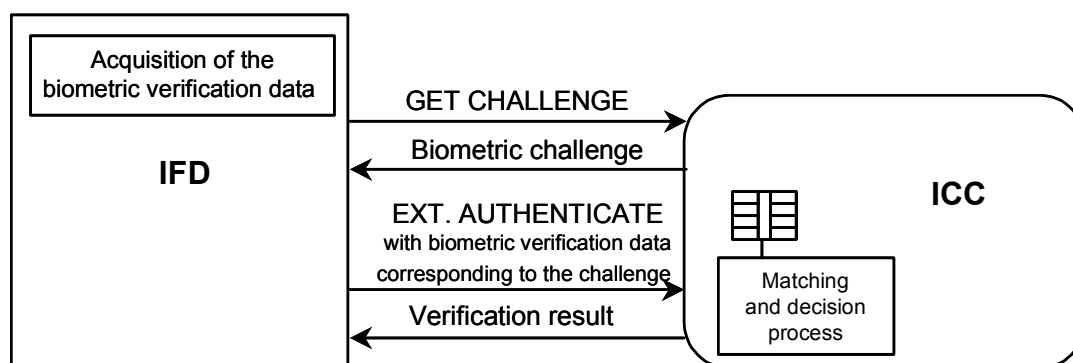**Figure A.3 — Commands for static biometric verification**

Figure A.4 — Commands for dynamic biometric verification

A.4 Scenarios

The Figures A.5 and A.6 illustrate some scenarios relevant to biometric user verification.
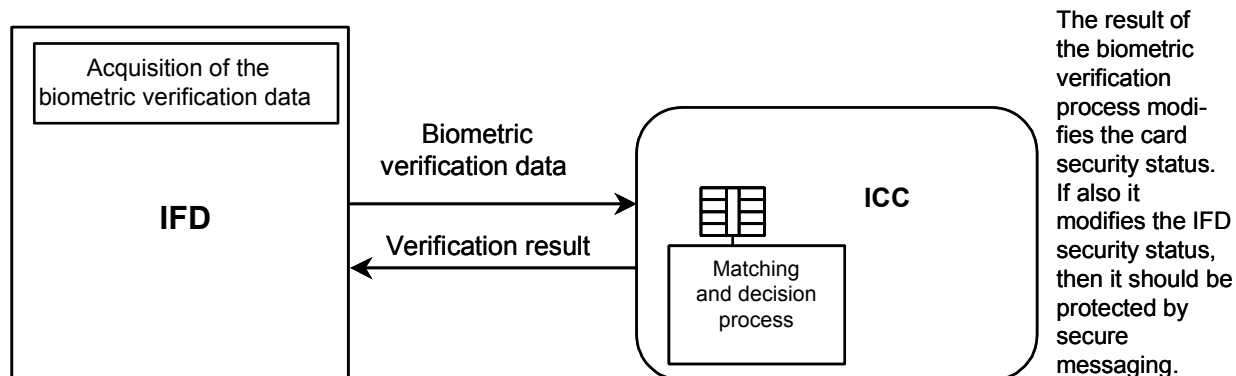
Figure A.5 — Scenario with matching and decision process inside the card
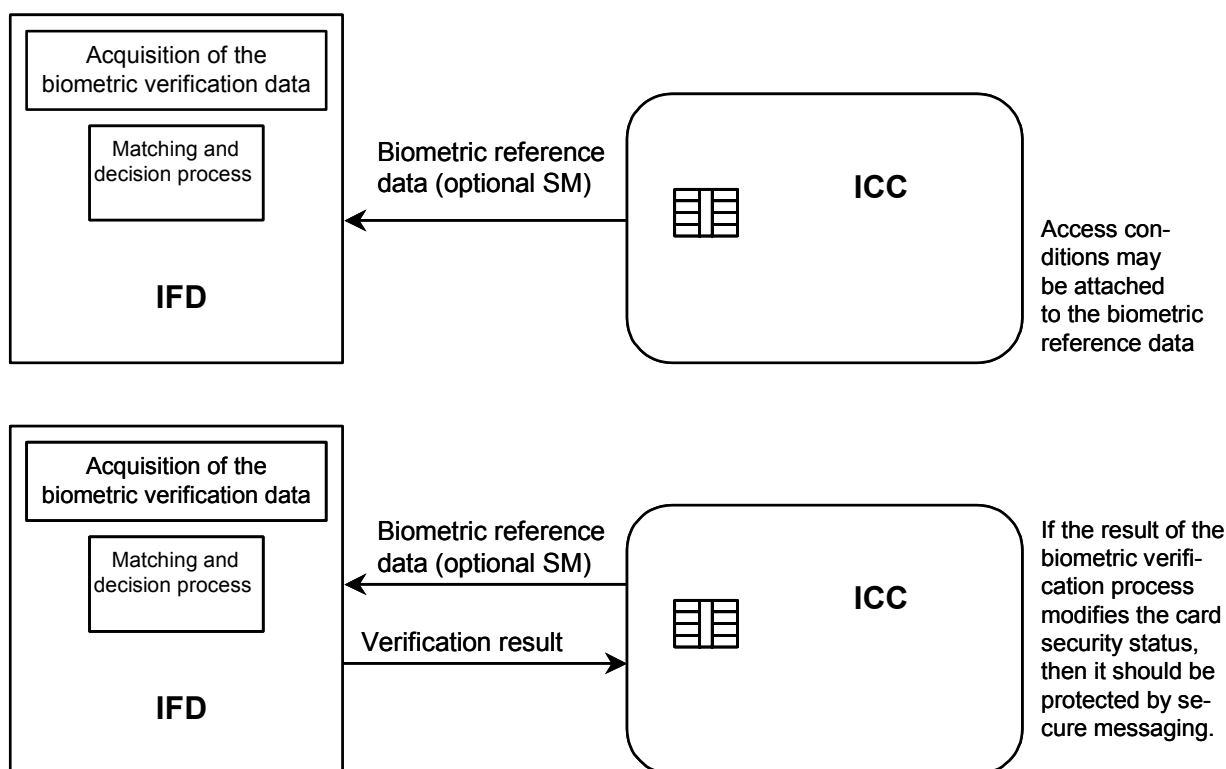
Figure A.6 — Scenarios with matching and decision process outside the card

A.5 Retrieval of information relevant for the biometric verification process

The IFD may need information related to the verification process. The following list contains information items which may be required by the IFD:

— biometric type (e.g. fingerprint, face features, ...)

— biometric subtype, if appropriate (e.g. left pointer finger)

— format owner and format type of biometric data

— algorithm reference, if any, as used, e.g., in the MANAGE SECURITY ENVIRONMENT command

— biometric reference data identifier (qualifier of reference data in the VERIFY command or EXTERNAL AUTHENTICATE command)

— discretionary data, if any.

Annex B
(informative)

Examples for enrollment and verification

B.1 Abbreviations

AID   Application Identifier
AT   Authentication Template
BIT   Biometric Information Template
BT   Biometric Type
CRT   Control Reference Template
DO   Data Object
DST   Digital Signature Template
FCI   File Control Information
FO   Format Owner
FT   Format Type
ID   Identifier
IFD   Interface Device
OID   Object Identifier
RD   Reference Data
SM   Secure Messaging
TAT   Tag allocation Authority Template
UQ   Usage Qualifier
VIT   Verification Requirement Information Template
|| Concatenation

B.2 Enrollment

For this example, it is assumed, that the card

— is totally personalized except the storing of the biometric reference data and the related Biometric Information Template (this includes also the presence of a biometric record in a key file with the related attributes for the biometric reference data, i.e. retry counter with initial value, resetting code with retry counter and initial value, flags for enabling/disabling verification requirement and changeability, ...)

— has password verification in addition to biometric verification.

With the CHANGE REFERENCE DATA command, the empty reference data are replaced by the user´s reference data computed in the enrollment process. The execution of the CHANGE REFERENCE DATA command has to be bound to security conditions, e.g. setting the required security status after successful completion of a cryptographic based authentication procedure or a successfully presented password.

NOTE   The security conditions for the CHANGE REFERENCE DATA command, after the enrollment has taken place, may be different due to the security policy of the application provider (e.g. change of reference data is no longer allowed after enrollment).

After the biometric reference data have been stored, the Biometric Information Template BIT has to be stored, which is used by the IFD in a verification process in this example. The BIT is stored after all types and subtypes of biometric reference have been enrolled.

Usually, an IFD (e.g. a PC, a public internet terminal or a cash terminal) does not know, whether the card presented
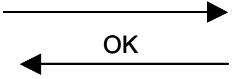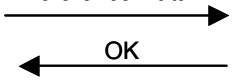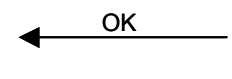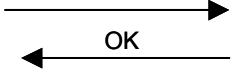
— belongs to a user who applies biometrics

— has a biometric algorithm supported by the IFD

— which biometric type is used for which it should prompt

— which value the related key reference (i.e. the reference data qualifier) has

— which implementation specific matching algorithm parameters have to be observed (e.g. limitation of the amount of minutiae to be sent in the verification data).

Therefore the Biometric Information Template BIT should provide information such as:

— the biometric reference data qualifier

— the OID of the tag allocation authority and indication of the format for the verification data

— the biometric type and possibly the biometric subtype enrolled (e.g. right thumb)

— further data objects, if any

— repetition of the respective DOs, if e.g. a second biometric type is enrolled.

Figure B.1 shows the commands which may be performed in this way in an enrollment process.

Command / Response	Meaning
VERIFY <Password> → ← OK	Setting the Security Status for storing the biometric reference data
CHANGE RD <Biometric Reference Data> → ← OK	Replacing the empty reference data by the enrolled biometric reference data
SELECT <File ID> → ← OK	Selection of the elementary file for storing the Biometric Information Template BIT (to be retrieved with GET DATA)
UPDATE BINARY <BIT> → ← OK	Storing the Biometric Information Template BIT

Figure B.1 — Commands for enrollment (example)

NOTE 1   There may be a need to protect the enrollment with secure messaging.

NOTE 2   For information storage and retrieval also other commands as described in ISO/IEC 7816-4 may be used. This is also valid for the Figures B.4, B.6 and B.7.

Figure B.2 shows the BIT and its DOs.

| T.BIT | L | T.RD | L | ... | T.OID | L | ... | T.TAT | L | T.BT | L | ... | T.FO | L | ... | T.FT | L | .. | ... |

Tag of Biometric Information Template ('7F60')

Reference data qualifier as used in P2 of VERIFY

Object identifier of tag allocation authority

Tag of Tag Allocation Authority Template ('A1')

Biometric Type e.g. fingerprint

Format owner

Format type
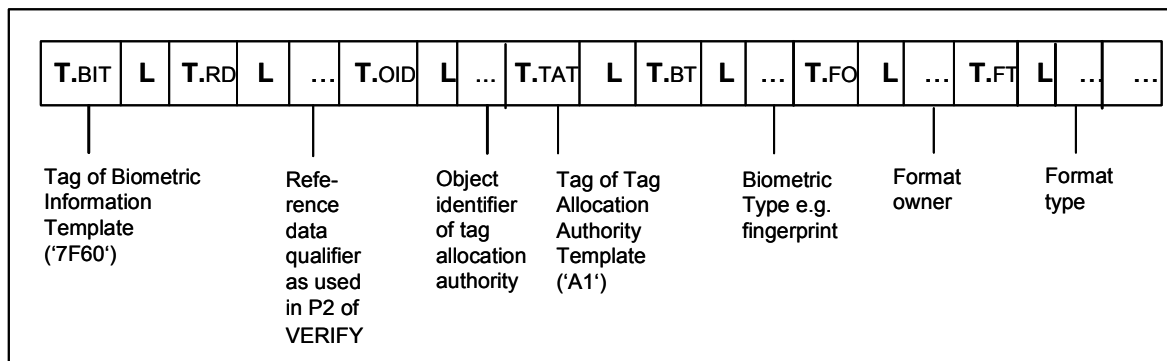
Figure B.2 — Example of a Biometric Information Template (BIT), tags assigned by the specified Tag Allocation Authority

NOTE   The tags inside the template 'A1' are defined the denoted tag allocation authority.

B.3 Verification with a single biometric method

The verification process starts with the retrieval of the Biometric Information Template, e.g. by applying the GET DATA command. If the IFD supports the required format for the biometric verification data as indicated in the BIT and the user has presented the related biometric object, the verification data are computed and delivered to the card by using the VERIFY command (see Figure B.3).

Command/Response	Meaning
SELECT <AID> → ← OK	Application selection with application identifier (AID)
GET DATA <Tag BIT> → ← Bio. Information Template	Retrieval of the Biometric Information Template BIT.
VERIFY <Biometric Verification Data> → ← OK	Verification of the user

Figure B.3 — Commands for verification without secure messaging (example)

NOTE   If the Biometric Information Template is not present, it means in this example that the respective user does not use biometrics.

If the biometric verification data are public (e.g. face, fingerprint, ear shape), then there is a need to protect them with secure messaging (see Figure B.4).

Command/Response	Meaning
SELECT <AID> → ← OK	Selection of the application with Application Identier (AID)
GET DATA <Tag BIT> → ← Bio. Information Template	Retrieval of the Biometric Information Template (BIT).
MANAGE SE <DO Key Ref> → ← OK	Setting the CRT DST with the public key for certificate verification
VERIFY CERTIFICATE <certificate> → ← OK	Verification of the certificate belonging to the biometric unit
GET CHALLENGE → ← Random Number	Requesting a challenge to be used for secure messaging
EXTERNAL AUTHENTICATE <authentication related data> → ← authentication related data	External authentication with establishing of SM keys
VERIFY <Biom. Verification Data, SM protected> → ← OK	User verification with SM protected verification data; response can also be SM protected

Figure B.4 — Commands for verification with secure messaging (example)

NOTE   Secure Messaging (SM) is outlined in ISO/IEC 7816-4.

In this example, the verification process starts with the retrieval of the Verification Requirement Information Template (VIT) and the corresponding Biometric Information Template (BIT), which may be stored e.g. in the FCI extension File (File ID is implicitly known).The VIT contains information, whether biometric and/or password verification is available and enabled or disabled and which corresponding qualifiers of the reference data (KeyRef) have to be used at the interface to the card. The BIT contains in this example (see Figure B.5) information about the card specific algorithm reference (AlgID), the qualifier of the reference data (KeyRef) and additional information like biometric type, format owner and format type.

T.BIT	L	T.AlgID	L	…	T.RD	L	…	T.OID	L	…	T.TAT	L	T.BT	L	…	…

Tag of Biometric Information Template ('7F60')

Algorithm reference

Reference data qualifier

OID of Tag Allocation Authority

Tag of Tag Allocation Authority Template ('A1')

Biometric Type e.g. fingerprint

Further DOs:
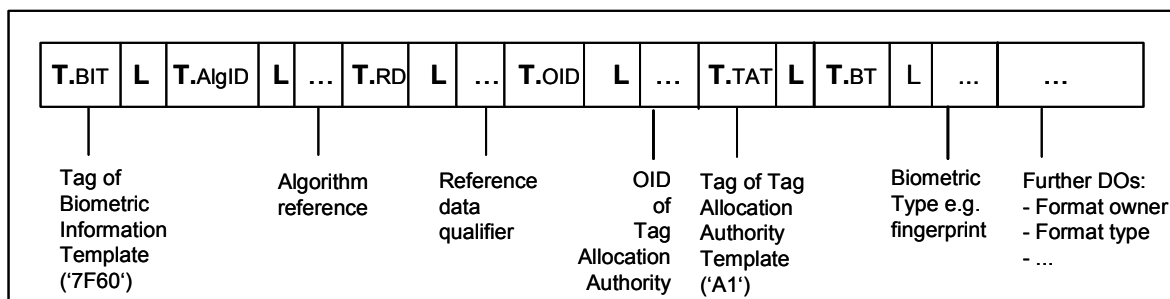- Format owner
- Format type
- ...

Figure B.5 — Example of a Biometric InformationTemplate (BIT)

If IFD and the presented card support the same mechanism and the user has presented the related biometric features, the verification data have to be computed and delivered to the card by using the VERIFY command which is preceeded by a MANAGE SECURITY ENVIRONMENT command to select the special verification method (see Figure B.6).
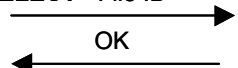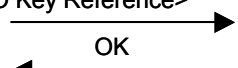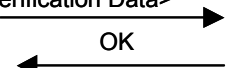
Command/Respone	Meaning
SELECT <File ID> → ← OK	Selection of the FCI extension file
READ BINARY → ← VIT ‖ BIT	Retrieval of the Verification Requirement Information Template VIT and the Biometric Information Template BIT
MANAGE SE <DO UQ ‖ DO Alg. Reference ‖ DO Key Reference> → ← OK	Setting the CRT AT with Usage Qualifier UQ, Algorithm Reference and Key Reference
VERIFY <Biometric Verification Data> → ← OK	Verification of the user

Figure B.6 — Commands for verification without secure messaging (example)

When a static biometric verification needs information from the card prior to verification, such information may be present in the biometric information template.

B.4 Access to the BIT in case of off-card matching

The BIT possibly in combination with other data (e.g. driver license data) may be protected e.g. by a signature of the issuing authority (for examples of protecting those data see Annex D). Therefore the BIT may be retrieved by applying a simple READ BINARY command, see Figure B.7.
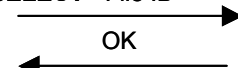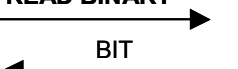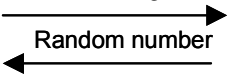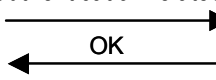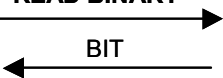
Command/Respone	Meaning
SELECT <File ID> → ← OK	Selection of the file containing the Biometric Information Template
READ BINARY → ← BIT	The DO BIT may contain the Secure Messaging Template e.g. for guaranteeing the authenticity of biometric reference data

Figure B.7 — Commands for retrieval of the BIT (example)

The access to the BIT may be restricted, i.e. prior to reading an authentication procedure has to be performed as shown in Figure B.8.

Command/Respone	Meaning
GET CHALLENGE ⟶ Random number ⟵	Getting a random number
EXT. AUTHENTICATE <authentication related data> ⟶ OK ⟵	Authentication of the entity, which has the access right to the BIT
READ BINARY ⟶ BIT ⟵	Reading the BIT

Figure B.8 — Commands for retrieval of the BIT after performing an authentication procedure (example)

If the BIT has to be transmitted e.g. over the Internet, then it may be necessary to apply secure messaging as shown in Figure B.4 to provide confidentiality and authenticity.

Annex C
(informative)

Biometric information data objects

This annex presents biometric information data objects based on the CBEFF Framework, see ISO/IEC 19785.

C.1 Abbreviations

BDB   Biometric Data Block
BHT   Biometric Header Template
BIT   Biometric Information Template
CBEFF   Common Biometric Exchange Formats Framework
DO   Data Object
IBIA   International Biometric Industry Association
IC   Integrated Circuit(s)
MAC   Message Authentication Code
OID   Object Identifier
PID   Product Identifier
SE   Security Environment
SMT   Secure Messaging Template
TLV   Tag-Length-Value

C.2 Biometric information data objects used in case of on-card matching

C.2.1 Usage of a single biometric type or biometric subtype

Prior to a verification process, information may be retrieved from a card presenting the details to be observed by the outside world when performing the verification process. The relevant data objects are shown in Table C.1.

Table C.1 — Biometric information data objects in case of on-card matching

Tag	L	Value				Presence
'7F60'	Var.	Biometric Information Template (BIT)				
		Tag	L	Value		
		'80'	1	Algorithm reference for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SE command as defined in ISO/IEC 7816-4; see note 5		Optional
		'83'	1	Reference data qualifier for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SE command as defined in ISO/IEC 7816-4		Optional
		'06'	Var.	OID of CBEFF standard body, see note 6		Mandatory, if default not used
		'A1'	Var.	Biometric Header Template (BHT) in compliance with CBEFF		Mandatory
				Tag	L	Value
				'80'	2	Patron header version (default '0101') / Mandatory, if default not used
				'90'	Var.	Index, unique identifier used for referencing this biometric data set in an application context outside the card / Optional
				'81'	1-3	Biometric type, see Table C.2 / Optional
				'82'	1	Biometric subtype, see Table C.3 / Optional, use with biometric type only
				'83'	7	Creation date and time of biometric data (CCYYMMDDhhmmss) / Optional
				'84'	Var.	Creator / Optional
				'85'	8	Validity period (from CCYYMMDD, to CCYYMMDD) / Optional
				'86'	2	Identifier of product (PID) that created the biometric reference data, value assigned by IBIA, see www.ibia.org / Optional
				'87'	2	Format owner of the biometric verification data, value assigned by IBIA, see www.ibia.org / Mandatory
				'88'	2	Format type of biometric verification data, specified by format owner / Mandatory
				'91' / 'B1'	Var.	Biometric matching algorithm parameters (primitive / constructed), see notes 2 and 7 / Optional

NOTE 1   Only those data objects from CBEFF are present, which are relevant for on-card matching.

NOTE 2   Additional data object, which is not present in the main CBEFF structure.

NOTE 3   In Table C.1 the biometric data block as defined in ISO/IEC 19785 is not present, since the biometric reference data are stored separately in the card and not in this BIT, and the biometric verification data have to be presented using e.g. a VERIFY command.

NOTE 4   In Table C.1 no payload is present, since usually access to a payload, if used by the application, is granted after successful completion of the biometric verification. The payload may be retrieved using access commands like GET DATA or READ BINARY.

NOTE 5   The outside world (i.e. the IFD) uses format owner / format type for identifying the required structure for the verification data. The matching algorithm in the card is addressed by the algorithm reference.

NOTE 6   If the ISO standard version of CBEFF (ISO/IEC 19785) is used, then the OID of the related ISO standard body (ISO/IEC JTC1/SC37) is the default value, i.e. the DO with tag '06' may be absent. 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: '608648016503').

NOTE 7   This DO provides any special parameters of an on-card matching algorithm implementation, e.g. maximum number of minutiae expected in the biometric verification data. The content of this DO is defined by the format owner.

Table C.2— Biometric Type as defined in ISO/IEC 19785

Name of Biometric Type	Value
No information given	'00'
Multiple Biometrics Used	'01'
Facial Features	'02'
Voice	'04'
Fingerprint	'08'
Iris	'10'
Retina	'20'
Hand Geometry	'40'
Signature Dynamics	'80'
Keystroke Dynamics	'0100'
Lip Movement	'0200'
Thermal Face Image	'0400'
Thermal Hand Image	'0800'
Gait	'1000'
Body Odor	'2000'
DNA	'4000'
Ear Shape	'8000'
Finger Geometry	'010000'
Palm Print	'020000'
Vein Pattern	'040000'
Foot Print	'080000'
Other values RFU	

NOTE   Some biometric types may be irrelevant for applications using cards.

Table C.3 — Biometric Subtype as defined in ISO/IEC 19785

b8	b7	b6	b5	b4	b3	b2	b1	Biometric Subtype
0	0	0	0	0	0	0	0	No information given
						0	1	Right
						1	0	Left
			0	0	0			No meaning
			0	0	1			Thumb
			0	1	0			Pointer finger
			0	1	1			Middle finger
			1	0	0			Ring finger
			1	0	1			Little finger
								Other values RFU

C.2.2 Usage of standardised and proprietary biometric data formats

In cases where the biometric verification data consist of biometric verification data with standardized structure followed by biometric verification data with a manufacturer specific structure, a nested BHT structure should be applied as shown in Table C.4.

Table C.4 — BIT with nested BHTs for biometric data of standardized and proprietary format (example)

Tag	L	Value					
'7F60'	Var.	BIT					
		Tag	L	Value			
		'80'	1	Algorithm reference			
		'83'	1	Reference data qualifier			
		'06'	Var.	OID of CBEFF standard body, see note 6 of Table C.1			
		'A1'	Var.	BHT (level 1)			
				Tag	L	Value	
				...		Common DOs , see Table C.1	
				'A1'	Var.	BHT 1 (level 2)	
						Tag	L	Value
						'87'	2	Format owner of the biometric verification data, e.g. format owner identifier of ISO/IEC JTC1/SC37
						'88'	2	Format type of biometric verification data, specified by format owner
				'A2'	Var.	BHT 2 (level 2)	
						Tag	L	Value
						'87'	2	Format owner of the biometric verification data, e.g. a card manufacturer
						'88'	2	Format type of biometric verification data, specified by format owner

C.2.3 Usage of several biometric types or biometric subtypes

If within the same application several type of biometrics or biometric subtypes are independently used and referenced by different reference data qualifiers (similar to a password for signature and a separate password for authentication), then a group BIT structure with nested BITs is applied, see Table C.5.

Table C.5 — BIT group template with nested BITs for applications with several reference data having its own reference data qualifier (example)

Tag	L	Value						
'7F61'	Var.	Biometric information group template						
		Tag	L	Value				
		'02'	1	'02' = Number of BITs				
		'7F60'	Var.	BIT 1				
				Tag	L	Value		
				'80'	1	Algorithm reference		
				'83'	1	Reference data qualifier		
				'06'	Var.	OID of CBEFF standard body, see note 6 of Table C.1		
				'A1'	Var.	BHT		
						Tag	L	Value
						...		
						'81'	1-3	Biometric type, e.g. fingerprint
						'82'	1	Biometric subtype e.g. right pointer finger
						'87'	2	Format owner of the biometric verification data
						'88'	2	Format type of biometric verification data, specified by format owner
		'7F60'	Var.	BIT 2				
				Tag	L	Value		
				'80'	1	Algorithm reference		
				'83'	1	Reference data qualifier		
				'06'	Var.	OID of CBEFF standard body, see note 6 of Table C.1		
				'A1'	Var.	BHT		
						Tag	L	Value
						...		
						'81'	1-3	Biometric type, e.g. fingerprint
						'82'	1	Biometric subtype, e.g. left pointer finger
						'87'	2	Format owner of the biometric verification data
						'88'	2	Format type of biometric verification data, specified by format owner

C.2.4 Usage of multimodal biometrics

In cases where several biometric features (in the sense of multimodal or combined biometrics) shall be verified e.g. in order to get access to certain data or a specific key, the group BIT with nested BITs is applied and the verification performed by sending e.g. several VERIFY commands. The access conditions attached to the related protected object define, which combination of biometric features have to be successfully verified.

C.2.5 Presentation of the biometric verification data

The coding and format of the commands for biometric verification which convey the biometric verification data to the card, are outlined in ISO/IEC 7816-4. The encoding possibilities for the command data field are outlined in Clause 6.2 of ISO/IEC 7816-11. Figure C.1 shows an example of the command data field related to the example given in Table C.4.
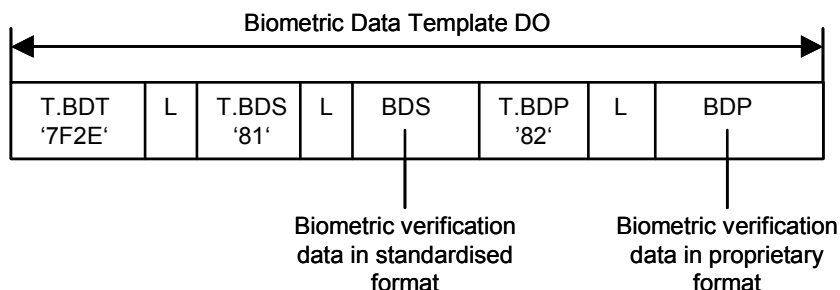

Figure C.1 — Biometric Data Template in the command data field (example)

C.3 Biometric information data objects used in case of off-card matching

C.3.1 General construction and usage

Data objects for off-card matching are presented as BIT, which contains

— the Biometric Header Template BHT,

— the Biometric Data Block BDB consisting of biometric reference data possibly followed by a payload and

— optionally DOs related to security, see C.3.4.

The use of the data structures presented in the subsequent clauses is not restricted to IC cards, i.e. the data structure may also be used in other types of cards, e.g. magnetic stripe cards, optical memory cards or cards with 2-dimensional barcode.

C.3.2 Usage of a single biometric type or biometric subtype

In Table C.7, DOs relevant for matching outside the card are specified, if a single biometric type or subtype is used.

Table C.7 — Biometric information data objects used in case of off-card matching

Tag	L	Value					Presence
'7F60'	Var.	Biometric Information Template (BIT)					
		Tag	L	Value			
		'06'	Var.	OID of CBEFF standard body, see note 6 of Table C.1			Mandatory, if default not used
		'A1'	Var.	Biometric Header Template (BHT) in compliance with CBEFF			Mandatory
				Tag	L	Value	
				'80'	2	Patron header version number (default '0101')	Mandatory, if default not used
				'90'	Var.	Index, unique identifier used for referencing this biometric data set in an application context outside the card	Optional
				'81'	1-3	Biometric type, see Table C.2	Optional
				'82'	1	Biometric subtype, see Table C.3	Optional, use with biometric type only
				'83'	7	Creation date and time of biometric data (CCYYMMDDhhmmss)	Optional
				'84'	Var.	Creator	Optional
				'85'	8	Validity period (from CCYYMMDD, to CCYYMMDD)	Optional
				'86'	2	Identifier of product (PID) that created the biometric re-ference data, value assigned by IBIA,see www.ibia.org	Optional
				'87'	2	Format owner of the biometric verification data, value assigned by IBIA, see www.ibia.org	Mandatory
				'88'	2	Format type of biometric verification data, specified by format owner	Mandatory
		'5F2E' / '7F2E'	Var.	Biometric reference data (primitive / constructed, see Table C.8)			Mandatory
		'53' / '73'	Var.	Discretionary data for payload (primitive / constructed), see notes 2 and 3			Optional

NOTE 1   Only those data objects from CBEFF are present, which are relevant for off-card matching.

NOTE 2   Additional data object, which is not present in the main CBEFF structure.

NOTE 3   Payload, if present, is available to the outside world when the verification succeeds (see BioAPI specification).

The main difference to Table C.1 is, that the DOs for the algorithm reference and the reference data qualifier (key reference as used by the card) are not present and instead the Biometric Data Block (BDB), consisting of the biometric reference data and possibly an attached payload follows the Biometric Header Template (BHT). A so-called Signature Block (SB) may also be present, but is encoded in a ISO/IEC 7816-conform way, see C.3.4.

Table C.8 — Biometric data template

Tag	L	Value		
'7F2E'	Var.	Biometric data template		
		DOs which may be embedded in the biometric data template		
		Tag	L	Value
		'80' / 'A0'	Var.	Challenge for user prompting (primitive / constructed, see Table C.9) This DO is only relevant for dynamic biometric types.
		'81' / 'A1'	Var.	Biometric data with standardized structure (primitive / constructed)
		'82' / 'A2'	Var.	Biometric data with proprietary structure (primitive / constructed)

Table C.9 — Challenge Template

Tag	L	Value		
'A0'	Var.	Challenge template		
		DOs which may be embedded in the challenge template		
		Tag	L	Value
		'90'	Var.	Challenge qualifier '00' = No information given (unspecified) '01' = UTF8 coding (default) Other values RFU
		'80'	Var.	Challenge

C.3.3 Usage of nested structures

In Table C.10, an example of the usage of nested structures is outlined. The main difference to Table C.5 is, that the pointer to the biometric reference data (i.e. the reference data qualifier) is replaced by the biometric reference data itself.

Table C.10 — BIT group template with nested BITs for applications with biometric reference data of several biometric types (example)

Tag	L	Value						
'7F61'	Var.	Biometric information group template						
		Tag	L	Value				
		'02'	1	Number of BITs in the group template				
		'7F60'	Var.	BIT 1				
				Tag	L	Value		
				'06'	Var.	OID of CBEFF standard body, see note 6 of Table C.1		
				'A1'	Var.	BHT		
						Tag	L	Value
						'81'	1-3	Biometric type, e.g. face features
						'87'	2	Format owner of the biometric reference data
						'88'	2	Format type of biometric reference data, specified by format owner
				'5F2E'	Var.	Biometric reference data		
		'7F60'	Var.	BIT 2				
				Tag	L	Value		
				'06'	Var.	OID of CBEFF standard body, see note 6 of Table C.1		
				'A1'	Var.	BHT		
						Tag	L	Value
						'81'	1-3	Biometric type, e.g. fingerprint
						'82'	1	Biometric subtype, e.g. left pointer finger
						'87'	2	Format owner of the biometric reference data
						'88'	2	Format type of biometric reference data, specified by format owner
				'5F2E'	Var.	Biometric reference data		

C.3.4 Security issues

Some possibilities, how to secure the BIT or how to grant access to the BIT and to transmit it in a secure way are outlined in Annex B and Annex D. The security features described in ISO/IEC 19785 with respect to

⎯ indication of security options

⎯ indication of integrity options

⎯ provision of a field for a signature or MAC

are fully supported by using the Secure Messaging Template (SMT) and the related DOs (see Annex D). The indication of security and integrity options in 2 special fields in the BHT is not needed because the presence of a cryptogram, a digital signature or a MAC is indicated by the respective tags. A simple example of the usage of the SMT is shown in Figure C.2. Further, more complex examples are provided in Annex D.
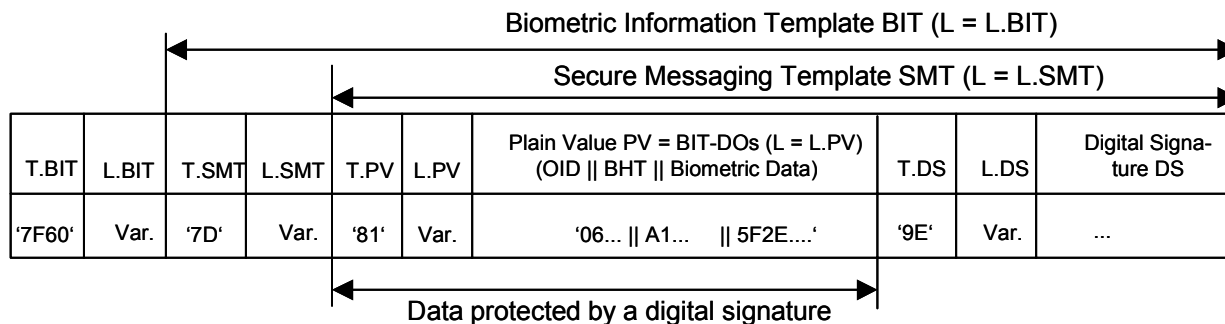
T.BIT	L.BIT	T.SMT	L.SMT	T.PV	L.PV	Plain Value PV = BIT-DOs (L = L.PV) (OID || BHT || Biometric Data)	T.DS	L.DS	Digital Signa- ture DS
'7F60'	Var.	'7D'	Var.	'81'	Var.	'06... || A1... || 5F2E....'	'9E'	Var.	...

Biometric Information Template BIT (L = L.BIT)

Secure Messaging Template SMT (L = L.SMT)

Data protected by a digital signature

Figure C.2 — Secured Biometric Information Template (example)

C.4 IBIA registration information

CBEFF compliance requires that Format Owners register with the IBIA for an assigned unique identifier of the Format Owner. Format Types are assigned by the Format Owner and represents the specific biometric data format as specified by the Format Owner. It is recommended that Format Owners register Format Types in use with the IBIA for archiving and publication purposes. IBIA will also register Product ID values (see Tables C.1 and C.7). The number is guaranteed to be unique.

IBIA will not assign values between ´FFF0´ - ´FFFE´ for Format Owners and Product IDs. These values are available for testing.

For registration information see www.ibia.org.

Annex D
(informative)

Usage of Secure Messaging Templates

D.1 Abbreviations

BD   Biometric Data
BER   Basic Encoding Rules
BHT   Biometric Header Template
BIT   Biometric Information Template
CC   Cryptographic Checksum
CCT   Cryptographic Checksum Template
CT   Confidentiality Template
CG   Cryptogram
DE   Data Element
DO   Data Object
DS   Digital Signature
DST   Digital Signature Template
KR   Key Reference
L   Length
MAC   Message Authentication Code
PD   Personal Data
PDT   Personal Data Template
PV   Plain Value
SM   Secure Messaging
SMT   Secure Messaging Template
T   Tag
TLV   Tag-Length-Value
|| Concatenation

D.2 Secure Messaging related data objects and their usage

There may be a need to protect the Biometric Information Template BIT in case that the card is used as carrier of BIT (see also NISTIR 6529 and ANSI X9.84):

⎯ BIT with privacy (Encryption)

⎯ BIT with integrity (Signed or MACed)

⎯ BIT with privacy and integrity.

The means for privacy and integrity in a card context are provided with Secure Messaging (SM) as defined in ISO/IEC 7816-4. There are 2 methods:

1) Before reading the BIT, SM-keys for achieving privacy and integrity are dynamically established with key transport or key agreement mechanisms.

2) The BIT is secured in itself in a static way, i.e. by applying the SM template technique as described below.

If the value field of the BIT has to be secured in a static way, then the value field is embedded in a SM Template, in which

⎯ all data objects remaining as plain text are put into a plain value template,

⎯ all data objects to be enciphered are put in a cryptogram

and, if integrity is needed, a cryptographic checksum DO or a digital signature DO are present. If data objects like algorithm reference and key reference enabling the service system to verify the integrity and to recover the plain value of the enciphered data are needed, then they are presented in control reference templates (see Figure D.1).
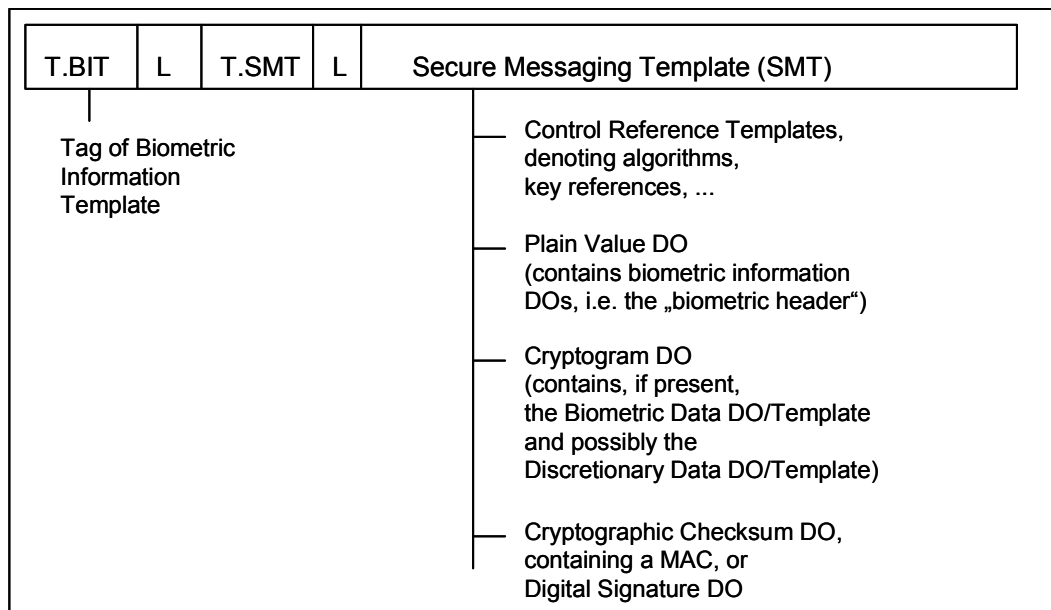
Figure D.1 — Biometric Information Template in combination with the SMT

The coding of DOs relevant for a Secure Messaging Template SMT are shown in Table D.1.

Table D.1 — SMT Data Objects (subset)

Tag	L	Value		
'7D'	Var.	Secure Messaging Template SMT		
		Tag	L	Value
		'xx'	Var.	Control Reference Template, see tab. D.2 (authentication protected)
		'81'	Var.	Plain value (PV), consisting of a sequence of DEs or BER-TLV coded DOs, but not SM related DOs, see note (authentication protected)
		'85'	Var.	Cryptogram (CG), the plain value consisting of BER-TLV coded DOs, but not SM related DOs (authentication protected)
		'8E'	Var.	Cryptographic checksum (CC), i.e. a Message Authentication Code (MAC)
		'9E'	Var.	Digital signature (DS)

NOTE   From the viewpoint of SM, the plain value is always primitive.

The Secure Messaging Template may contain control reference templates:

— Cryptographic Checksum Template (CCT)

— Digital Signature Template (DST)

— Confidentiality Template (CT).

These Control Reference Templates contain further data objects e.g. for specifying the algorithm and a key reference (see Table D.2).

**Table D.2 — Control Reference Templates and related DOs (subset)**

Tag	L	Value		
'B5'	Var.	Cryptographic Checksum Template (CCT)		
'B7'	Var.	Digital Signature Template (DST)		
'B9'	Var.	Confidentiality Template (CT)		
		DOs relevant for CCT, DST and CT		
		Tag	L	Value
		'80'	Var.	Algorithm reference
		'83'	Var.	- Reference to a secret key for direct use (relevant for symmetric algorithms) - Reference of a public key (relevant for asymmetric algorithms)
		'84'	Var.	- Reference to a secret key for key derivation (relevant for sym. algorithms) - Reference of a private key (relevant for asymmetric algorithms)

NOTE   Additional data objects are specified in ISO/IEC 7816-4.

D.3 Encoding examples

The encoding examples show

— a biometric information template, where the biometric information data objects (biometric header) are followed by a cryptogram containing the biometric data and both protected by a MAC (see Figure D.2) and

— some kind of application data (e.g. personal data for identification) are combined with a biometric information template and secured in different ways (see Figures D.3 - D.5).
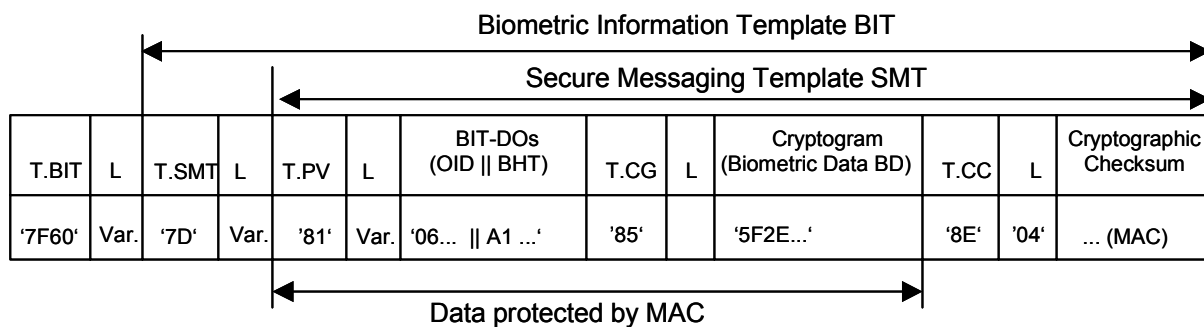
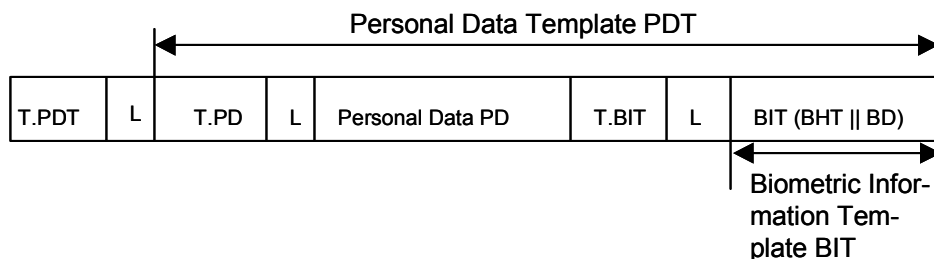**Figure D.2 — BIT Template with embedded SMT (example)**

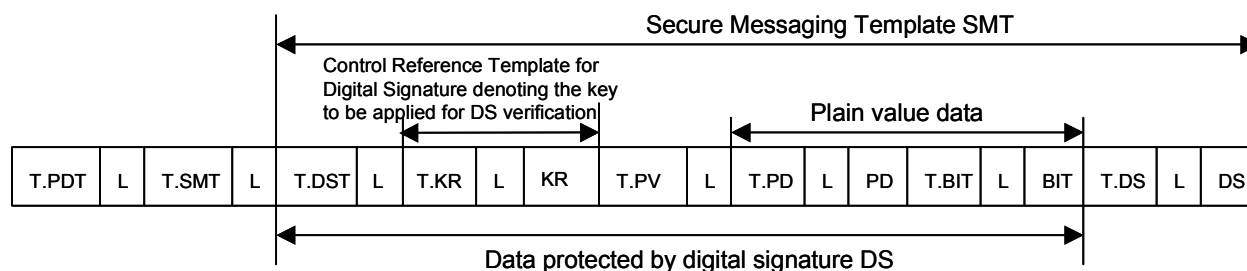**Figure D.3 — Personal Data Template with BIT (example)**

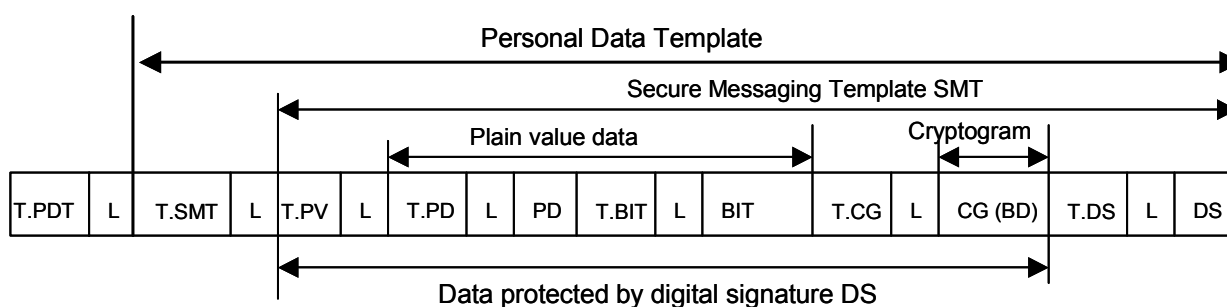**Figure D.4 — Personal Data Template with BIT protected by a digital signature (example)**

Figure D.5 — Personal Data Template protected by a digital signature and containing beside other DOs a cryptogram for the biometric data (example)

Bibliography

[1]   ISO/IEC 7816
Identification cards – Integrated circuit cards – All parts

[2]   ISOIEC 19784
BioAPI Specification

[3]   ANSI X9.84-2001
Biometric Information Management and Security

[4]   NISTIR 6529-A
Common Biometric Exchange Format Framework

ICS 35.240.15

Price based on 33 pages