ISO/IEC JTC 1 /SC 17 N 2006

Date: 2001-10-02

ISO/IEC CD2 7816-11

ISO/IEC JTC 1 /SC 17/WG 4

Secretariat: AFNOR

Information technology — Identification cards - Integrated circuit(s) cards with contacts — Part 11: Personal verification through biometric methods

Technologies de l´information – Cartes d´identification – Cartes à circuit(s) intégré(s) à contacts – Parte 11 : Verification personelle par méthodes biométriques

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (30) Commitee
Document language: E

P:\struif\ISO\Bio\ISO-IEC 7816-11 (E).doc STD Version 1.0

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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 part of ISO/IEC 7816 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

ISO/IEC 7816 consists of the following parts, under the general title *Information technology — Identification cards - Integrated circuit(s) cards with contacts*:

— *Part 1: Physical characteristics,*

— *Part 2: Dimensions and location of contacts,*

— *Part 3: Electronic signals and transmission protocols,*

— *Part 4: Interindustry commands for interchange*

— *Part 5:Numbering system and registration procedure for application identifier*

— *Part 6: Interindustry data elements*

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

— *Part 8: Security related interindustry commands*

— *Part 9: Additional interindustry commands*

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

— *Part 11: Personal verification through biometric methods*

Annexes A, B, C and D are for information only.

Information technology — Identification cards - Integrated circuit(s) 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 data elements to be used with biometric methods. Identification is outside the scope of this standard.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 7816. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 7816 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of ISO and IEC maintain registers of currently valid international standards.

- ISO/IEC 7816-4: 1995, *Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange*
- ISO/IEC 7816-5: 1994, *Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifier*
- ISO/IEC 7816-6: 1996, *Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements*
- ISO/IEC 7816-8: 1999, *Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 8: Security related interindustry commands*
- ISO/IEC 7816-9: 2000, *Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 9: Additional interindustry commands*
- NISTIR 6529: *Common Biometric Exchange File Format, January 3, 2001*
- BioAPI Consortium: *BioAPI Specification, Version 1.1, March 16, 2001*

3 Terms and definitions

For the purpose of this part of ISO/IEC 7816, the following 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
template
as defined in ISO/IEC 7816-6

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 Symbols and 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
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
FCI	File Control Information
ID	Identifier
L	Length
OID	Object Identifier
PBD	Proprietary Biometric Data
RD	Reference Data
SBD	Standard Biometric 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

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.

5.1 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.

5.2 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 clause 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 query prior to a verification process. Table 1 defines biometric information DOs.

Table 1 — Biometric information DOs

Tag	L	Value		
‘7F60’	x	Biometric Information Template (BIT)		
‘80’ ’83’	1 1	Algorithm Identifier for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SE command Reference data identifier for use in the VERIFY / EXT. AUTH. / MANAGE SE command		
‘A0’	x	Biometric information DOs defined in this standard		
‘A1’	x	Biometric information DOs specified by a tag allocation authority, see annex C		
				Tag allocation authority (see ISO/IEC 7816-6):
		‘06’	x	- Object identifier (OID)
		’41’	x	- Country authority (see ISO/IEC 7816-4)
		’42’	x	- Issuer (see ISO/IEC 7816-4)
		’4F’	x	- Application Identifier (AID), identifies the application and its provider (see ISO/IEC 7816-5)
				DOs defined by the tag allocation authority
		‘8x’	x	...
		’9x’	x	…
		‘Ax’	x	…
		‘Bx’	x	…

The indication of the tag allocation authority is mandatory in a template with tag ‘A1’. All context specific tags within such a template are defined by the tag allocation authority.

NOTE - In case the card does not perform the verification process, the Biometric Information Template may also contain the biometric reference data (see table 2) and possibly discretionary data (tag ‘53’ or ‘73’) e.g. for data to be delivered to a service system, if verification is positive.

6.2 Biometric data

Biometric data (verification data, reference data) may be sent 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 2.

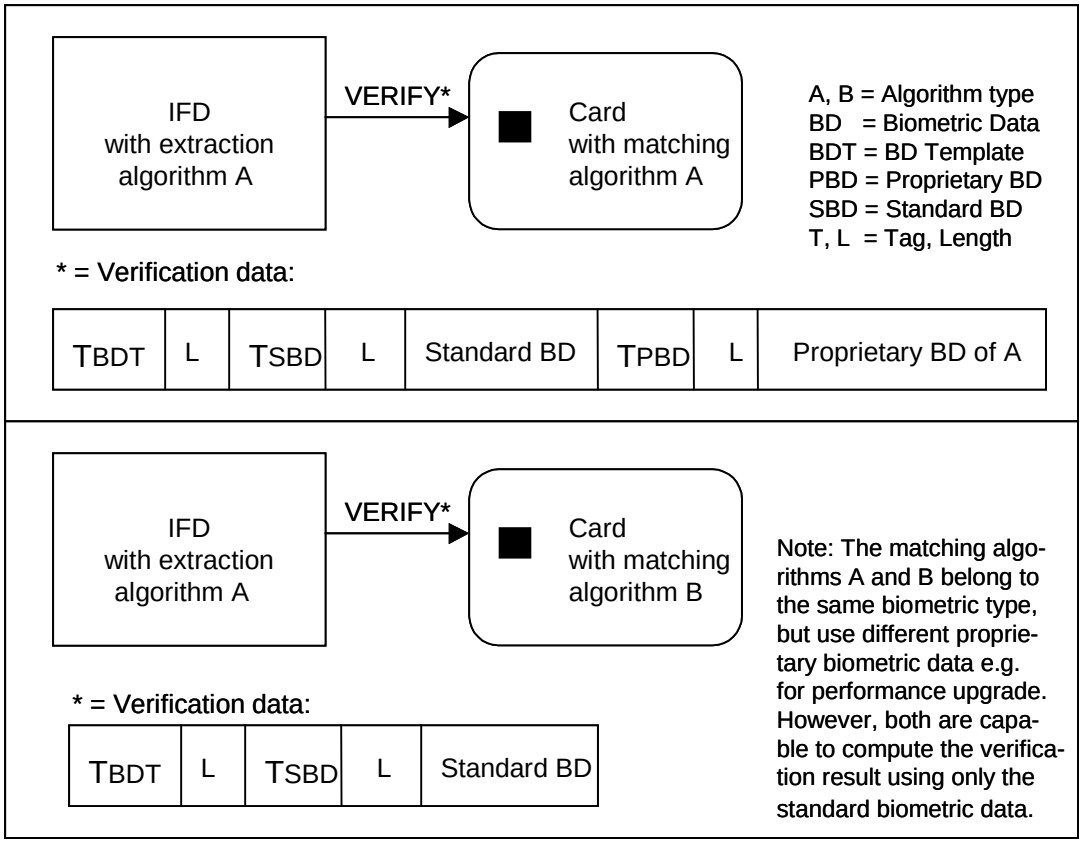
Table 2 — Biometric data DOs

Tag	L	Value		
'5F2E'	x	Biometric data		
'7F2E'	x	Biometric data template		
		DOs which may be embedded in the biometric data template		
		'5F2E'	x	Biometric data
		'81' / 'A1'	x	Standard biometric data (primitive / constructed)
		'82' / 'A2'	x	Proprietary biometric data (primitive / constructed)
		'06'	x	OID denoting the format of the biometric data

As shown in tab. 2, biometric data may be split up in a standard part and in a proprietary part, whereby the proprietary part may be used e.g. for achieving a better performance. The usage of standard and proprietary data is shown in fig. 1.

Structure and coding of standard biometric data are biometric type dependent and out of scope of this standard.

Figure 1 – Use of standard biometric data and proprietary biometric data



6.3 Verification requirement information

6.3.1 Purpose

The current status of verification data 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. 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 3) indicates by bit map which keys (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 3 — VIDO structure

VIDO Tag	L	Enabled / disabled Flags	Usable / unusable Flags	Key Ref.	Key Ref.	...
‘96’	‘xx’	‘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 4.

Table 4 — Verification requirement information template (VIT) and embedded DOs

Tag	Length	Value
‘A6’	x	Verification requirement information template
’90’	1	Verification requirement indication (Flag DO)
’95’	1	Usage qualifier (see table 8)
’83’	1	Key reference

The general VIT structure is shown in table 5.

Table 5 — Example of the VIT structure

Verification requirement information template DO (VIT-DO)												
		Flag DO			Key Reference DO			Usage Qualifier DO (opt.)			Key Ref. DO	
VIT Tag	L	Flag Tag	L	Enabled/ disabled Flags	Key Reference Tag	L	V	Usage Qualifier Tag	L	V	Key Reference Tag	...
'A6'	‘xx’	'90'	‘xx’	‘xx’	'83'	'01'	‘xx’	‘95’	‘xx’	‘xx’	‘83’	...

The relation of the flags to the key references is the same as in the VIDO. A usage qualifier DO (see table 6), if present, belongs to the subsequent key reference DO. If no usage qualifier DO appears immediately before a key reference DO, then the usage of the key is implicitly known.

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.

Table 6 — Coding of the usage qualifier based on ISO/IEC 7816-9

b8 b7 b6 b5 b4 b3	**b2 b1**	**Meaning**
0 0 0 0 0 0	0 0	associated key not to be used
1 - - - - -	- -	- use: verification (DST, CCT) - use: encipherment (CT) - use: external authentication (AT)
- 1 - - - -	- -	- use: computation (DST, CCT) - use: decipherment (CT) - use: internal authentication (AT)
- - 1 - - -		use: SM response (CCT, CT, DST)
- - - 1 - -	- -	use: SM command (CCT, CT, DST)
- - - - 1 -	- -	use: user verification, knowledge based (AT)
- - - - - 1	- -	use: user verification, biometric based (AT)
- - - - - -	x x	RFU (default = ’00’)

NOTE – The meaning of the usage qualifier set to ‘00’ has been added.

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.

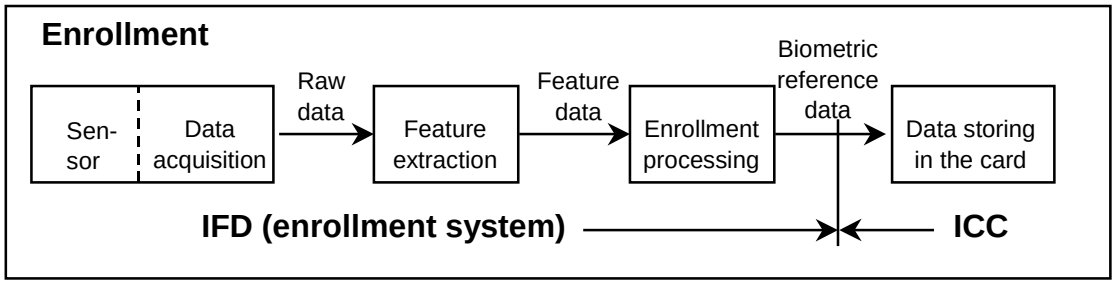


Figure A.1 – General scheme of an enrollment process

The sensor depends on the biometric type (e.g. a camera for face features, a microphone for speech pattern, a fingerprint chip for finger image). The data acquisition module (e.g. a frame grabber or a analog-digital-converter may be a separate module or integrated in the sensor. Since raw data have usually a considerable size not processable in a card, feature extraction is performed. In the enrollment processing the biometric reference data are formatted, whereby several samples of feature data may be taken into account.

Biometric reference data may be stored in the card

- during a card personalisation phase or
- after issuing of 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.

The general (simplified) scheme for a verification

- 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

is shown in figure A.2.

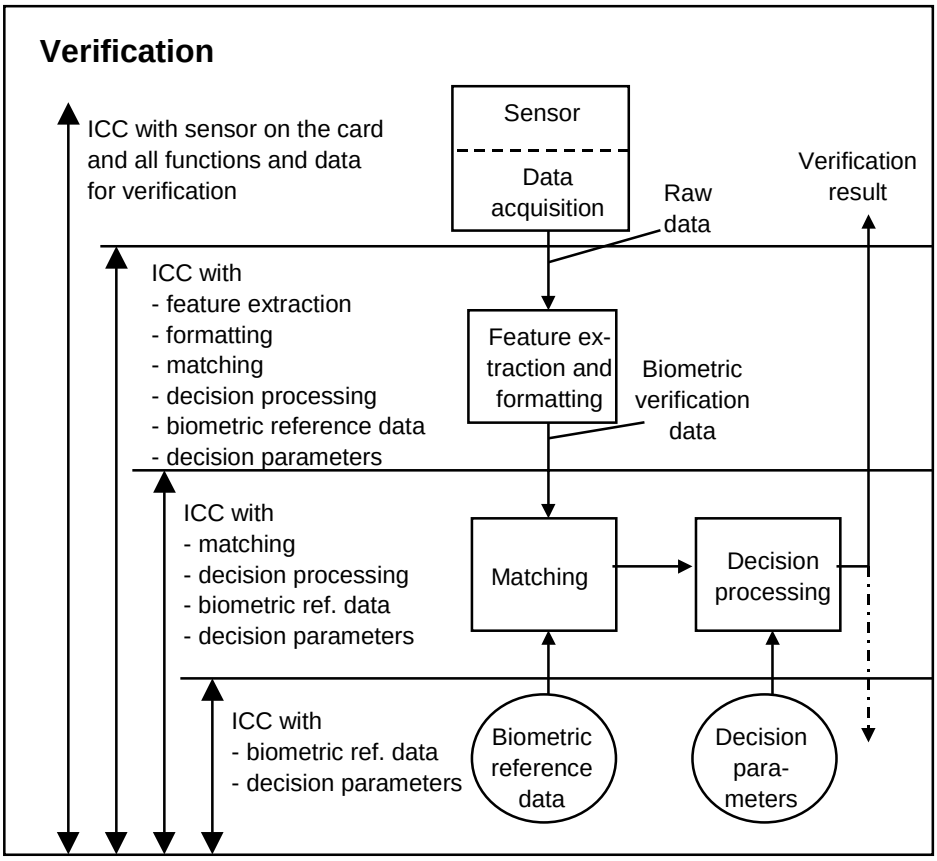


Figure A.2 – General scheme of a verification process

NOTE - Decision parameters are usually bound to the decision processing. When the card provides the biometric reference data (possibly cryptographic 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 challenge, see type B).

Examples of biometric type A:

Ear shape
Facial features
Finger geometry
Finger image (fingerprint)
Hand geometry
Iris features

Palm pattern
Retina pattern
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 features 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. those features have to be presented to the card in an authentic way (see annex B, fig. 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.

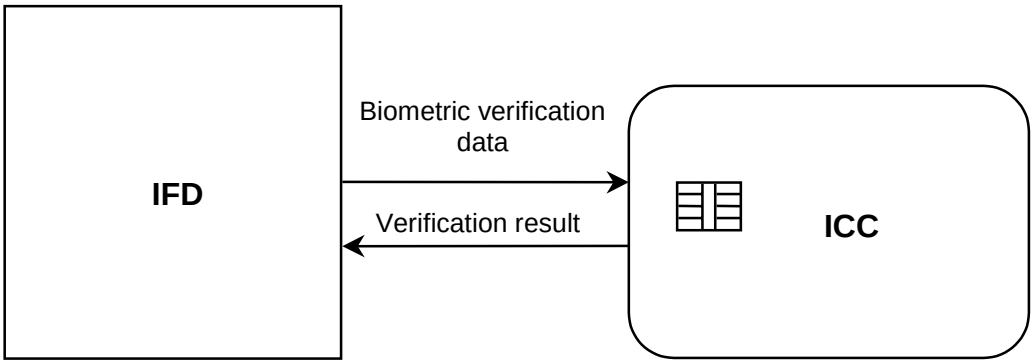


Figure A.3 – Messages for static biometric verification

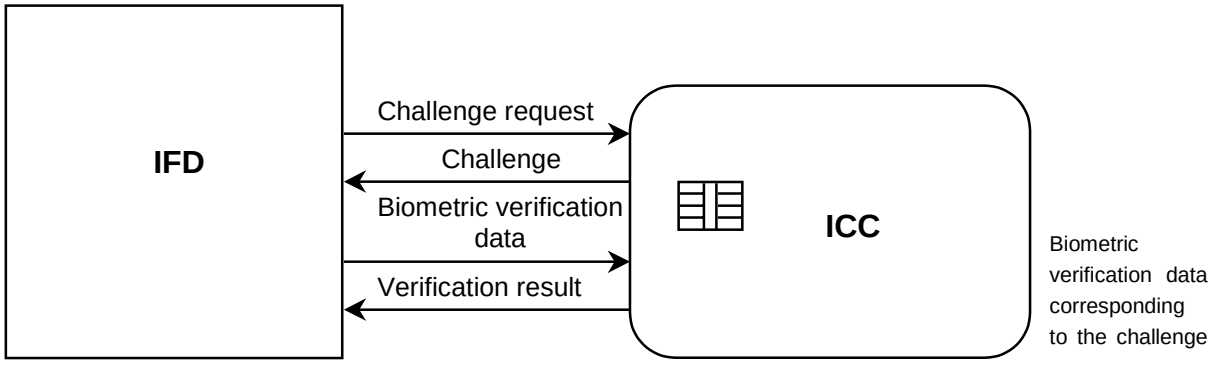


Figure A.4 – Messages for dynamic biometric verification

A.4 Scenarios

The fig. A.5 and A.6 illustrate some scenarios relevant to biometric user verification.

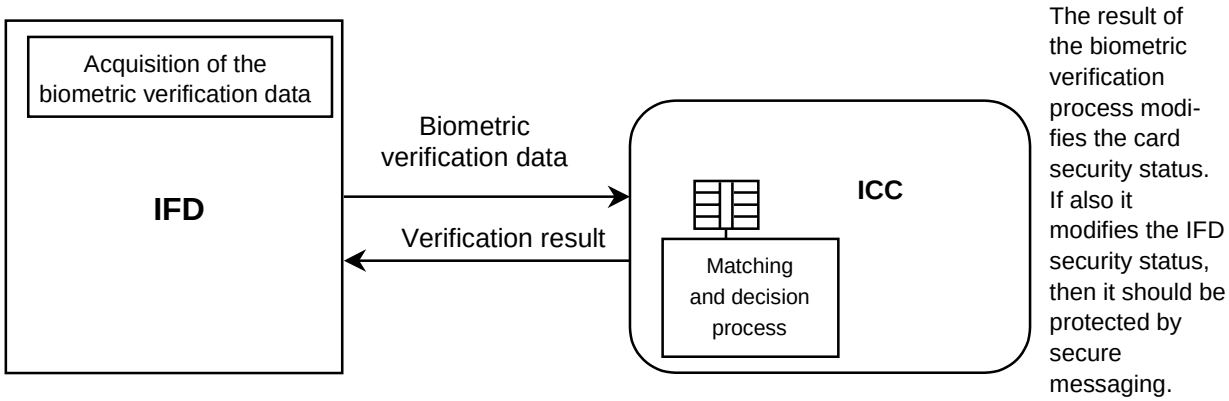


Figure A.5 – Scenario with matching and decision process inside the card

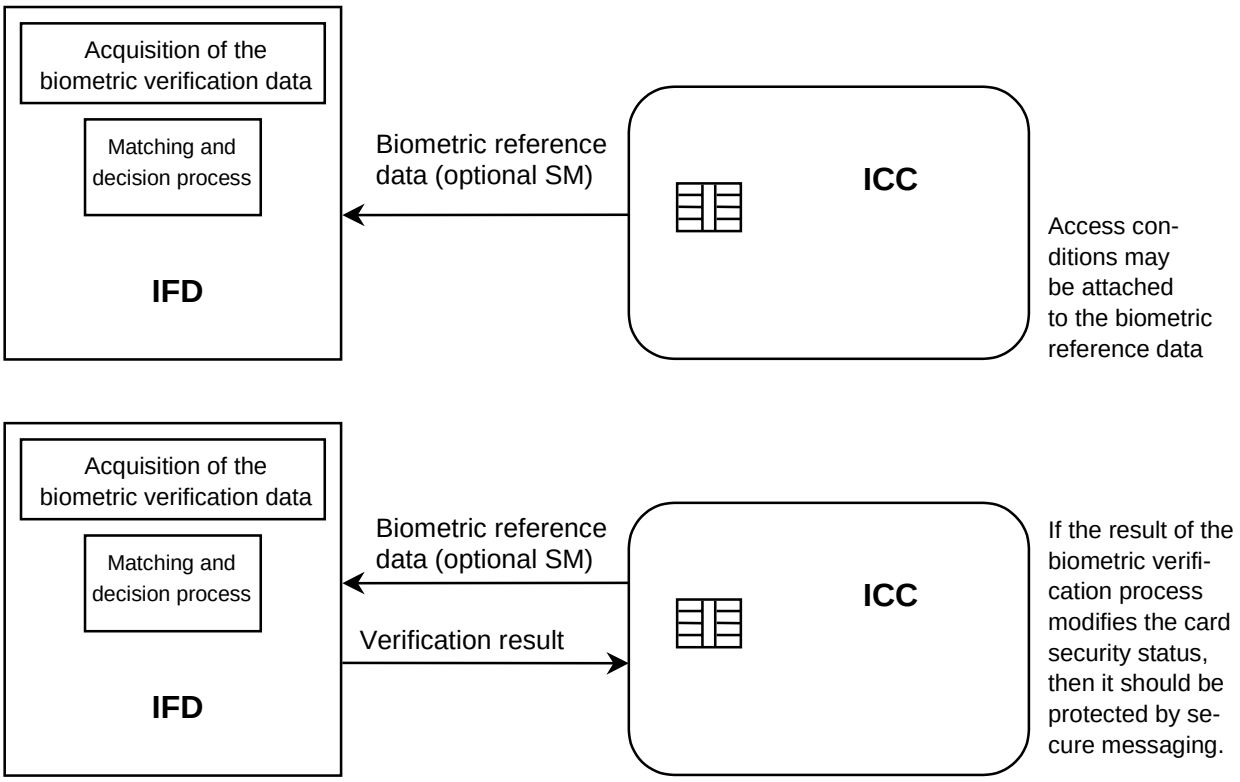


Figure A.6 – Scenarios with matching and decision process outside the card

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. face features, speech pattern, finger image, ...)
- biometric feature, if appropriate (e.g. left pointer finger)
- biometric data template identifier (e.g. object identifier (OID as defined in ISO/IEC 7816-6), manufacturer id with additional information such as algorithm used, version no.)
- algorithm identifier, 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
BF	Biometric Feature
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
I	Issuer
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 beside the biometric verification also password 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 process may be repeated, if reference data of a second biometric feature, e.g. a second finger, shall be enrolled), the Biometric Information Template BIT has to be stored, which is used by the IFD in a verification process in this example.

Usually, an IFD (e.g. a public internet terminal or a cash terminal) does not know, whether the card presented

- belongs to a user which applies biometrics

- has a biometric algorithm supported by the IFD
- which biometric feature is enrolled for which it should prompt
- which value the related key reference has
- which resolution the sensor of the enrollment system has been used for the computation of the verification data.

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

- the key reference for addressing the biometric reference data
- the OID of the tag allocation authority and indication of the format for the verification data
- the biometric feature enrolled (e.g. right thumb)
- further data objects, if any
- repetition of the respective DOs, if a second biometric feature is enrolled.

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

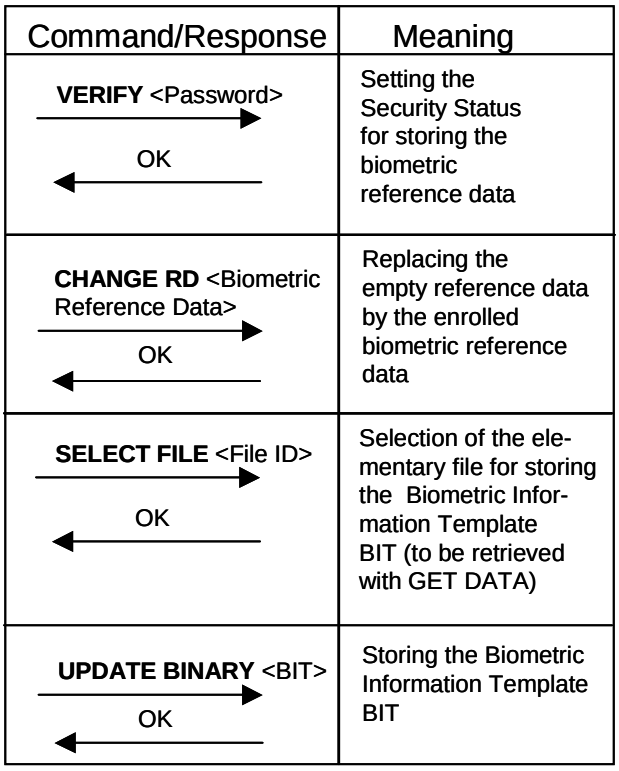


Figure B.1 - Commands for enrollment (example)

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

Figure B.2 shows the BIT and its DOs.

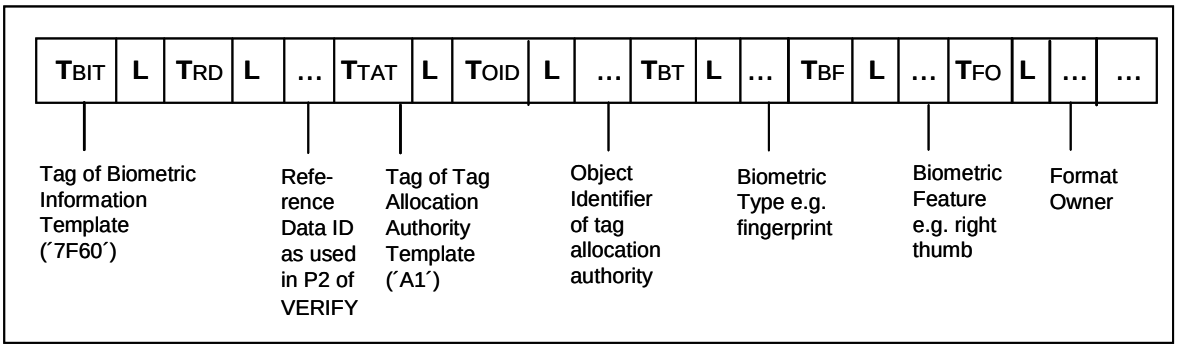


Figure B.2 – Biometric Information Template BIT (example)

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 IFD and the presented card fits together and the user has presented the related biometric feature, the verification data have to be computed and delivered to the card by using the VERIFY command (see figure B.3).

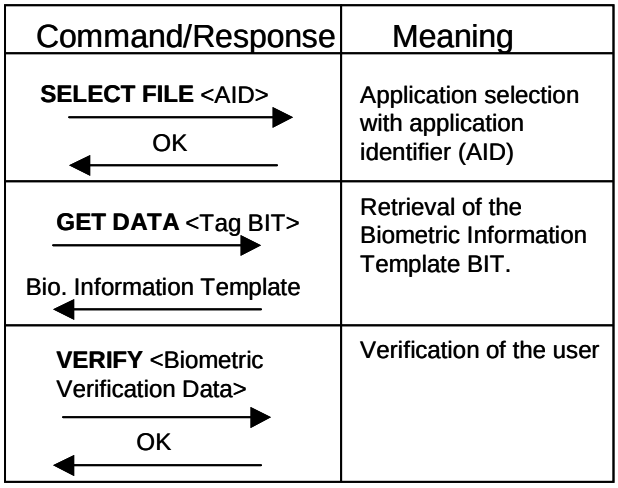


Figure B.3 - Commands for verification without secure messaging (example)

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 FILE <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)

B.4 Verification with more than one verification method

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 implicitely 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) has to be used at the interface to the card. The BIT contains in this example (see figure B.5) information about the issuer of the biometric method and a biometric type indicator as alternative to an OID, the card specific algorithm reference (AlgID), the qualifier of the reference data (KeyRef) and possibly additional information.

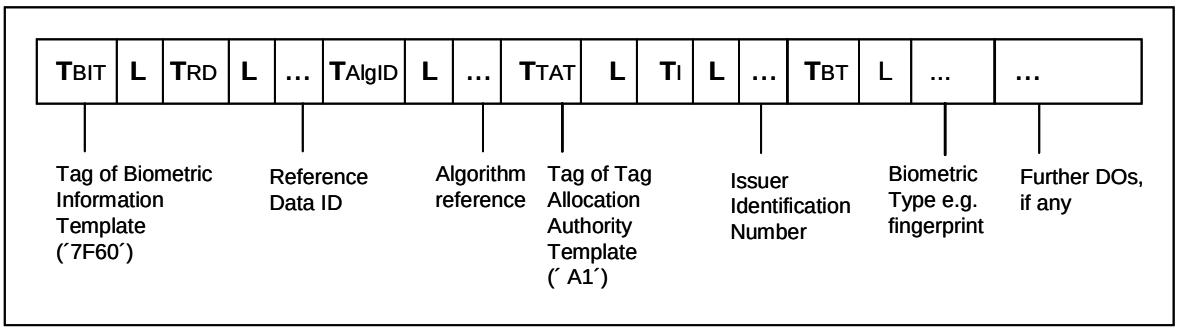


Figure B.5 – Biometric InformationTemplate BIT (example)

If IFD and the presented card support the same mechanism and the user has presented the related biometric feature, 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 specify the special verification method (see figure B.6).

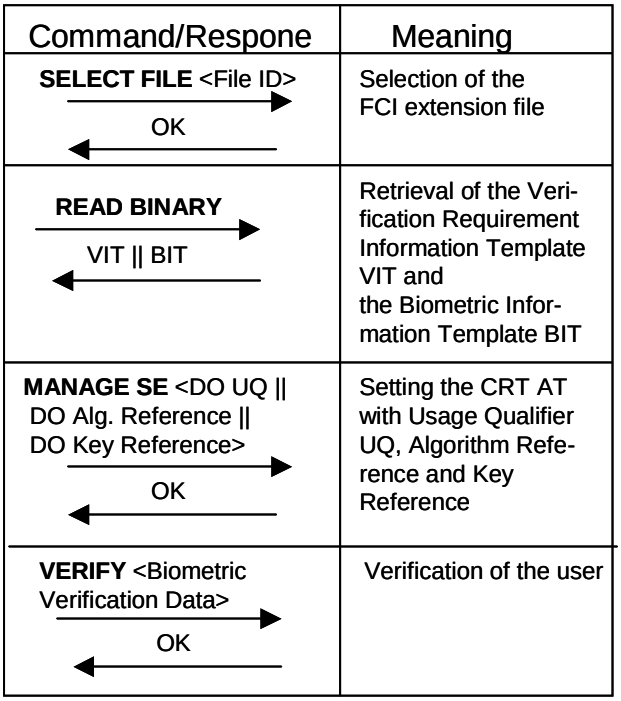


Figure B.6 - Commands for verification without secure messaging (example)

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

Annex C
(informative)

Biometric information data objects

C.1 Abbreviations

BER Basic Encoding Rules
BIT Biometric Information Template
DO Data Object
IBIA International Biometric Industry Association
MAC Message Authentication Code
NIST National Institute of Standards and Technology
OID Object Identifier
TLV Tag-Length-Value

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

In tab. C.1, DOs relevant for on-card matching are specified using data elements defined in NISTIR 6529.

Table C.1 — Biometric information data objects (case: on-card matching)

Tag	**L**	**Value**		
'7F60'	x	Biometric Information Template (BIT)		
'80'	'01'	Algorithm Identifier for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SECURITY ENVIRONMENT command		
'83'	'01'	Reference data identifier for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SECURITY ENVIRONMENT command		
'A1'	x	Biometric data objects as specified in NISTIR 6529 (subset relevant for on-card matching)		
		Tag	L	Value
		'06'	x	OID of NIST
		'80'	'02'	Version no. (default: '0100')
		'81'	x	Biometric type, see table A.2
		'82'	'02'	Format owner of the biometric verification data, value assigned by IBIA
		'83'	'02'	Format type of biometric verification data, specified by format owner

Table C.2 — Biometric Type

Name of Biometric Type	Value
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 Geometry	'020000'
Vein Pattern	'040000'
Other values RFU	

C.3 Biometric information data objects used in cards as carrier of biometric data

In tab. C.3, DOs relevant for matching outside the card are specified. The use of the data structure 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.

Table C.3 — Biometric information data objects (case: card used as carrier of BIT)

Tag	L	Value		
'7F60'	x	Biometric Information Template (BIT), in which the subsequent DOs are embedded		
'A1'	x	Biometric data objects as specified in NISTIR 6529 (subset relevant for off-card matching)		
		Tag	L	Value
		'06'	x	OID of NIST
		'80'	'02'	Version no. (default: '0100')
		'81'	x	Biometric type, see table C.2
		'82'	'02'	Format owner of the biometric reference data, value assigned by IBIA
		'83'	'02'	Format type of biometric reference data, specified by format owner
'5F2E' or '7F2E'	x x	Biometric reference data (not BER-TLV structured) or Biometric reference data template (BER-TLV objects), see tab. C.4		
'53' or '73'	x x	Discretionary data for payload (not BER-TLV structured) or Discretionary data template for payload (BER-TLV objects), see note 2		

NOTES -
1. The DOs with tag '06' and '80' – '83' are the card relevant DOs from the Biometric Header (BH) as specified in NISTIR 6529. The biometric reference data and the payload belong to the Biometric Specific Memory Block (BSMB).
2. Payload, if present, are data to be used by the IFD in case that the verification result is positive (see BioAPI specification).

Table C.4 — Biometric reference data template

Tag	L	Value		
'7F2E'	x	Biometric reference data template		
		DOs which may be embedded in the biometric reference data template		
		'80', 'A0'	x	Challenge or challenge template for user prompting, see table C.5 This DO is only relevant for dynamic biometric types.
		'81', 'A1'	x	Standard biometric data (primitive / constructed)
		'82', 'A2'	x	Proprietary biometric data (primitive / constructed)

Table C.5 — Challenge Template

'A0'	x	Challenge template		
		DOs which may be embedded in the challenge template		
		'90'	x	Challenge qualifier '00' = No information given '01' = ASCII coding (default) '02' = UTF8 Other values RFU
		'80'	x	Challenge

Annex D
(informative)

Usage of Secure Messaging Templates

D.1 Abbreviations

BD	Biometric Data
BER	Basic Encoding Rules
BH	Biometric Header
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).

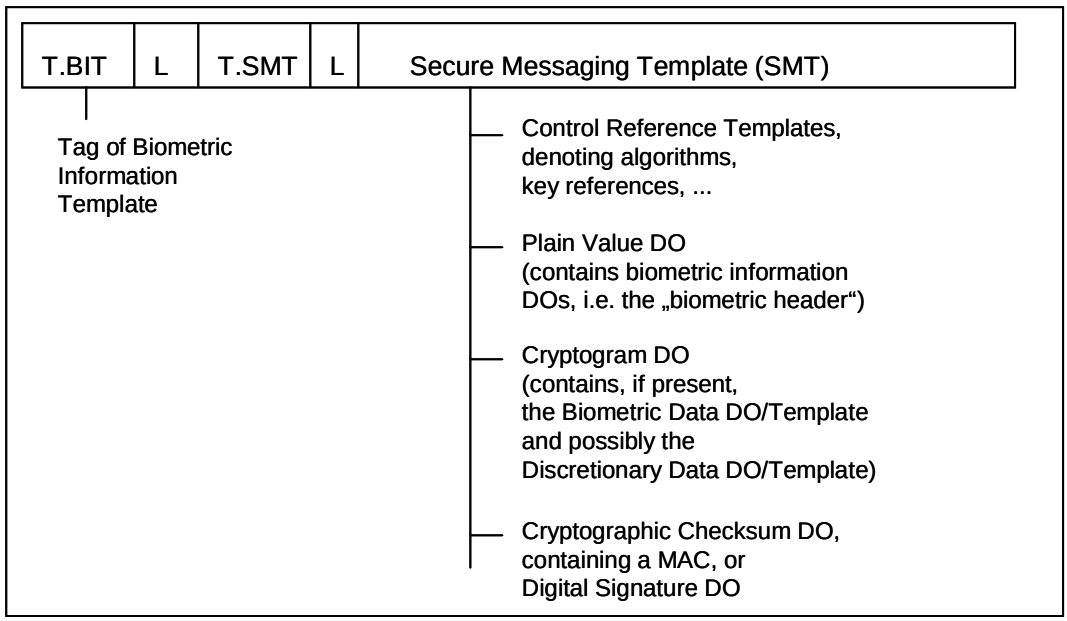


Figure D.1 — Biometric Information Template in combination with the SM Template

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	Length	Value
'7D'	var	Secure Messaging Template SMT
'xx'	var	Control Reference Templates, 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 tab. D.2).

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

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

NOTE - Additional data objects are specified in ISO/IEC 7816-8.

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).

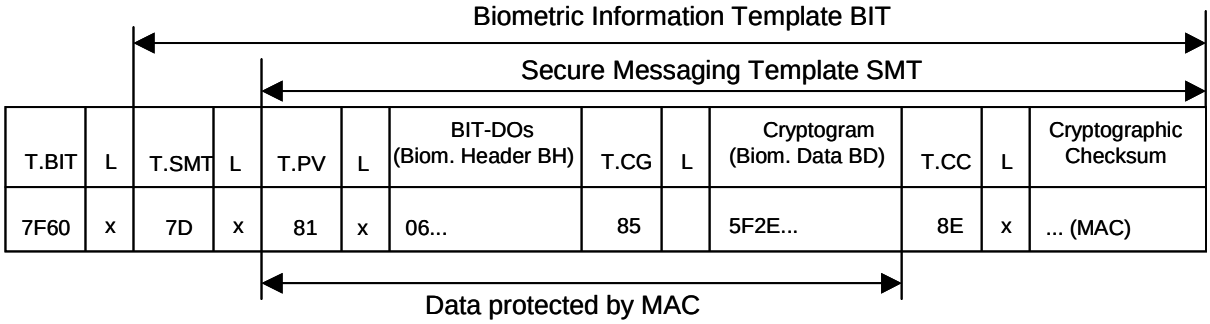


Figure D.2 — BIT Template with embedded SMT Template (example)

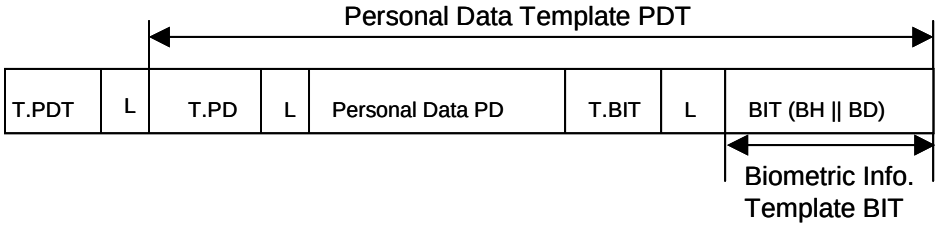


Figure D.3 — Personal Data Template with BIT Template (example)

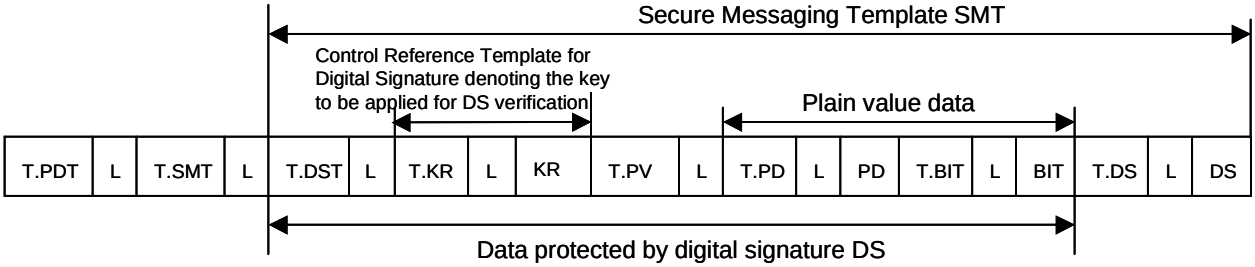


Figure D.4 — Personal Data Template with BIT Template protected by a digital signature (example)

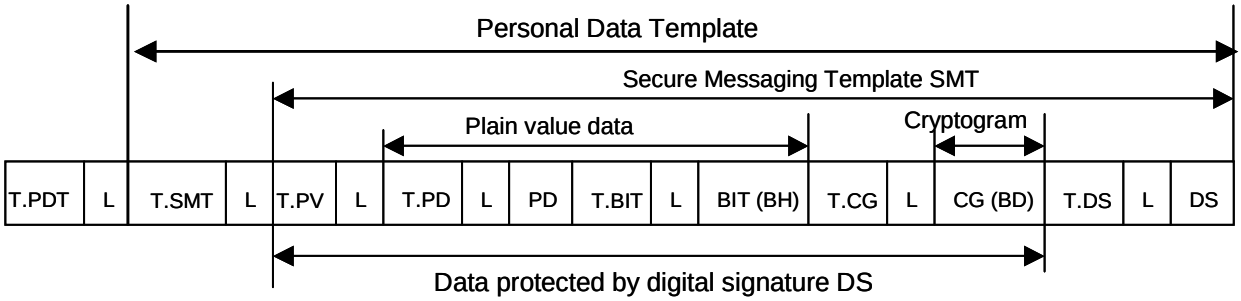


Figure D.5 — Personal Data Template protected by a digital signature and containing beside other DOs a cryptogram for the biometric data (example)