INTERNATIONAL STANDARD

ISO/IEC 19795-7

First edition
2011-01-15

Information technology — Biometric performance testing and reporting —

Part 7: Testing of on-card biometric comparison algorithms

Technologies de l'information — Essais et rapports de performance biométriques —

Partie 7: Essais des algorithmes de comparaison biométrique sur carte

Reference number
ISO/IEC 19795-7:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Figures

Tables

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 19795-7 was prepared by Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 37, *Biometrics*.

ISO/IEC 19795 consists of the following parts, under the general title *Information technology — Biometric performance testing and reporting*:

— *Part 1: Principles and framework*

— *Part 2: Testing methodologies for technology and scenario evaluation*

— *Part 3: Modality-specific testing* [Technical Report]

— *Part 4: Interoperability performance testing*

— *Part 5: Access control scenario and grading scheme*

— *Part 7: Testing of on-card biometric comparison algorithms*

The following part is under preparation:

— *Part 6: Testing methodologies for operational evaluation*

Introduction

Biometric recognition algorithms have been ported to ISO/IEC 7816 integrated circuit cards to realize the privacy enhancing benefits asserted for the on-card biometric comparison paradigm. While the most common commercial realization of this capability has been the comparison of fingerprint minutiae templates on card, comparison of data from other modalities has been implemented also. Indeed the relevant card standards have been explicitly drafted to support arbitrary biometric modalities. Further information on modality-specific aspects can be found in ISO/IEC 19795-3. In any case, while the computational capability of such cards has increased in recent years, there remains the question of whether verification accuracy needs to be traded off for speed or data size or both. For fingerprint templates, the goal of improved efficiency has led to the development of the ISO/IEC 19794-2:2005 compact-size card formats specifically for on-card biometric comparison.

This part of ISO/IEC 19795 specifies a mechanism for measuring both accuracy and speed of ISO/IEC 7816 integrated circuit cards processing data from arbitrary modalities. It includes examples for the data structures and commands needed to match conformant ISO/IEC 19794-2:2005 minutiae templates on cards.

Information technology — Biometric performance testing and reporting —

Part 7:
Testing of on-card biometric comparison algorithms

1 Scope

This part of ISO/IEC 19795 establishes a mechanism for measuring the core algorithmic capabilities of biometric comparison algorithms running on ISO/IEC 7816 integrated circuit cards. Specifically, this part of ISO/IEC 19795

— instantiates a mechanism for on-card biometric comparison testing;

— standardizes procedures for the measurement of the accuracy of on-card biometric comparison implementations running on object-based, test-specific sample cards;

— standardizes procedures for the measurement of durations of the various operations; and

— gives examples for matching ISO/IEC 19794-2:2005 compact card minutiae templates.

The following are specifically not within the scope of this part of ISO/IEC 19795:

— procedures for securing the communications channel, including cryptographic protection of the biometric templates;

— procedures for protection of sample or template integrity using digital signatures;

— authentication of the card and reader;

— selection or use of transmission protocols (e.g. contactless);

— profiles of specific data interchange standards;

— procedures for evaluation of readers, including performance, conformance and interoperability;

— procedures for evaluation of ruggedness or durability of the card;

— on-card template generation (e.g. extraction of minutiae from images),

— template update or adaptation;

— formal conformance tests of ISO/IEC 7816-4 and ISO/IEC 7816-11;

— testing of devices not conforming to ISO/IEC 7816, including all system-on-card devices.

2 Conformance

A test is conformant to this part of ISO/IEC 19795 if it conforms to the normative requirements of Clauses 5 and 6.

An on-card comparison implementation is conformant to the test specification of Clause 7 if it supports all the requirements of Clause 7.

3 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 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-6:2004, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*

ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 19785-3:2007, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19795-1:2006, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

ISO/IEC 19795-2:2007, *Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19795-1 and the following apply.

4.1
on-card comparison
execution of a comparison algorithm on a ISO/IEC 7816 integrated circuit card

NOTE The informal term match-on-card is deprecated in this part of ISO/IEC 19795 in favour of on-card biometric comparison as used in ISO/IEC 24787. The terms matcher and matching algorithm are deprecated in favour of comparison subsystem and comparison algorithm respectively. These terms are taken from SC 37's Standing Document 2, Harmonized Biometric Vocabulary.

5 Abbreviations

For the purposes of this document, the following abbreviations apply.

— APDU Application Protocol Data Unit as used in ISO/IEC 7816-4

— BIT Biometric Information Template as defined in ISO/IEC 7816-11

— DET Detection error tradeoff characteristic – a plot of FNMR vs. FMR

— FMR False match rate

— FNMR False non-match rate

— IC Integrated circuit

— IDMS Identity management system

— ISO/IEC 7816 Multipart standard for “Identification cards - Integrated circuit(s) cards with contacts”

— ISO/IEC 19794 Multipart standard of “Biometric data interchange formats”

— PC/SC Generic interface specification for PC to IC card connectivity

— SC 17 Subcommittee 17 of Joint Technical Committee 1 – developer of IC card standards

— SC 37 Subcommittee 37 of Joint Technical Committee 1 – developer of biometric standards

— SDK Software Development Kit (as library software)

6 Requirements on test planning

6.1 Fundamental concept of the test

The on-card comparison capability shall be tested in one or two stages, as listed below. Stage 2 is optional.

— Stage 1: Measure the speed and accuracy of the on-card comparison algorithm by executing biometric sample comparisons on the card under test. This shall be achieved by repeatedly storing reference templates on the card and sending verification templates to the card for comparison according the requirements of Clause 8. Accuracy shall be computed from either or both of

  — the comparison scores computed on the card, and

  — the verification decisions computed on the card.

— Stage 2 (optional): Measure the accuracy of the on-card comparison algorithm by executing biometric sample comparisons on an implementation running on a general purpose (e.g. PC class) computer. This stage shall not be used to state the accuracy of on-card comparison implementations unless the comparison scores retrieved from the card in stage 1 are exactly equal to those generated in this stage for all given pairs of reference and verification templates.

The first stage gives assurance that the accuracy of stage 2 is obtainable by the card under test.

NOTE 1 A test in which the card is required to produce comparison scores supports production of a DET characteristic plotting false non-match and false match rates as a function of operating threshold. If, however, a test allows cards to produce only a pass-fail verification decision then only a single point on the DET characteristic can be computed.

NOTE 2 Guidance on the minimum number of comparisons needed to sustain a claimed error rate is given in ISO/IEC 19795-1.

NOTE 3 The second stage allows a larger number of comparisons to be conducted quickly. This allows very large numbers of comparisons to be conducted. This supports, for example, testing of a claim that FMR is less than 0.0001.

NOTE 4 The second stage comparison score identity requirement gives assurance that the off-card and on-card comparison algorithms are the same. The second stage implementation might be tested using the procedures of Annex C and the API of Annex D.

6.2 Specification of interface hardware and software

The test shall be executed using the commands of Clause 8 and the test plan shall state this requirement. The test plan shall establish specifications for the interface to the cards under test. This should include specifications of the card reader. The test may limit scope to ISO/IEC 7816 contact IC cards or to ISO/IEC 14443 contactless cards.

EXAMPLE The test laboratory might state that while it does not currently intend to use undisclosed card readers, it reserves the right to do so for any purpose.

6.3 Specification of the data formats

6.3.1 Format for comparison data

The data format might be a standard format or a proprietary or de facto standard format. The test plan shall identify any allowed variants of the data format in use.

EXAMPLE Clause 9 of the ISO/IEC 19794-2:2005 standard gives the “format type” codes for variants which differ in the encoding and placement requirements on minutiae. Placement variation, such as whether a ridge ending is encoded as the ridge skeleton end-point or as the valley bifurcation, remains an open issue in minutiae interoperability. Thus, cards must return a value for the “format type” in the BIT tag '88', and encoders should follow the ISO/IEC 19794-2:2005, Clause 6 guidance on placement.

The test plan shall specify formats for the biometric enrollment data that resides on the card. The test plan shall specify the allowed formats for the data transmitted to the card for matching. This might include a line-by-line profile of the relevant standards or specifications. Annex A gives an example of such a profile.

NOTE For fingerprints, the test plan may re-iterate the applicable finger position codes given in Annex B.

6.3.2 Format for off-card images and templates

The test plan shall identify the formats for all data that is provided to the implementations running off card. The test plan shall also identify the formats for all data required to be generated by the implementations running off card.

EXAMPLE See the sample text in Annex A.

6.4 Profiling of the BIT

The test plan shall identify one or more BIT structures and their organisation. The test plan shall define the operations that are parameterized by data elements in the BIT.

The test plan and test report shall state required variations or values in the BIT. The test plan shall state whether the BIT(s) are allowed to contain other pieces of information (e.g. as allowed by the standards). This data would be read but likely ignored.

EXAMPLE 1 The test plan will indicate which biometric modality is in use, and define the appropriate data representation standard.

EXAMPLE 2 In ISO/IEC 19794-2:2005 the tag '83' is used to store the “feature handling indicator” i.e. whether the matching algorithm supports ridge counts, cores, deltas and cell quality. A test might require these capabilities to be present or absent, or might require all of them to be optional.

6.5 Card-comparison subsystem combinations

Tests conformant to this part of ISO/IEC 19795 are intended to measure on-card matching capability by measuring algorithm accuracy in the intended environment (i.e. the specific card). It may be appropriate for the test plan to state a policy on the kinds of card-supplier biometric sub-system supplier teams that are allowed to participate, and on how such teams should be contacted and identified.

NOTE It may be possible for a matching algorithm to be tuned to be more accurate when it is implemented on a more capable card, or is tailored to the card.

6.6 Phased testing

The test plan should state whether the test will be conducted in phases. A first phase might allow a smaller and faster evaluation of submitted software and cards which would support bug-fixes and development by the vendor. A second phase might be the formal test. In any case, the test plan should state a policy on the following

— The number of phases

— Whether participation in phase N is required for participation in phase N+1

— Whether to allow the supplier to update the cards and software between any two phases

— What measurements and results will be released to whom, on what schedule

6.7 Options for participation

The test plan shall state what hardware and software components are required for each phase.

EXAMPLE A test plan could state: “All implementations submitted to the test must provide the components identified in one or more of the rows of Table 1.”

Table 1 — Classes of participation

Class of Participation	ISO/IEC 7816 Card + Comparison subsystem	PC-based Template Comparison subsystem	PC-based Template Generator
Class A	+	+	
Class B	+	+	+

6.8 Metrics

The test plan shall disclose what performance metrics it intends to measure and report. The test shall measure and report false non-match rates at one or more specific false match rates. The test plan shall state a primary target false match rate. This allows implementers to conduct any necessary alteration of their implementations for the test.

False match rates and false non-match rates shall be rendered in the form of a receiver operating characteristic (ROC) or detection error trade-off (DET) curve.

EXAMPLE The test report will include full detection error tradeoff (DET) characteristics for all implementations tested. In addition the report will include performance interoperability matrices as standardized in ISO/IEC 19795-4:2008. Such tables will report false non-match rates at fixed false match rates of 0.0001 as the primary figure of merit. The report may include other metrics also.

6.9 Comparison results

For each VERIFY command, the card shall make either or both of a comparison score and a verification decision available to the test harness. The production of comparison scores supports computation of a full DET characteristic. The production of a verification decision supports computation of a single point on the DET.

NOTE 1 Some matching algorithms produce only a small number of unique comparison scores (naturally or otherwise). This may have operational consequences. It will also influence the smoothness of the DET characteristic.

NOTE 2 Some requirements of this part of ISO/IEC 19795, for example the requirements to return comparison scores and to have stateless behaviour (clause 8.8.5) are often not desirable in commercial and operational use for security or other reasons.

7 Requirements on test execution

7.1 General

The test shall adhere to the requirements of ISO/IEC 19795-1:2006 and of Clause 6 of ISO/IEC 19795-2:2007.

7.2 Conditions for demonstrating equivalence of on-card and off-card algorithms

To verify that the on-card comparison algorithm is identical to that running on the general purpose computer the test laboratory shall execute at least 100 genuine and 100 impostor comparisons on the card and replicate those on the general purpose computer. The minimum number of individuals used in those comparisons shall be 50. The testing laboratory shall check that the resulting comparison scores are exactly equal.

NOTE 1 The values 100 and 50 are somewhat arbitrary. They are present because it is unlikely that card-based and PC-based algorithms could produce identical outputs (from randomly selected inputs) if they were actually different.

NOTE 2 A test laboratory may supplement the requirements of this subclause with other test methods.

7.3 BIT Processing

The test harness shall read one or two ISO/IEC 7816-11 BITs from each card under test. The BITs shall be read as a group per the card APDU in 8.6. The BITs shall be used to parameterize the conversion of the raw sample to the format required by the card.

The same conversion shall be applied to data sent to the implementation of the on-card comparison algorithm running on the general purpose computer.

EXAMPLE For fingerprint minutiae matching, the BIT includes parameters for the conversion of INCITS 378 templates to ISO/IEC 19794-2 compact-size card templates. The conversion occurs before the data are sent to the card-based comparison implementations. The same conversion would be applied for templates passed to the PC-based implementation.

7.4 Measurement of speed of execution

7.4.1 Quantities to be measured

The test shall measure and report the duration of the execution of the VERIFY command. The duration of all VERIFY commands shall be measured. The test shall record duration with an indication of whether the VERIFY was an impostor or genuine attempt. The test shall record the duration with a number indicating the size of the authentication data, in bytes, sent during the VERIFY command. Operationally the end-to-end time may be the most important measurement.

The test shall also measure and report the duration of all other functions. If the following actions are conducted then statistics for the execution times shall be reported.

— The template generation operations.

— Any off-card template comparisons.

— The storage of the reference template on the card.

7.4.2 Methods for measuring duration

The test plan shall establish and document the mechanism of measuring duration of each command for which timing was measured.

EXAMPLE 1 A protocol analyzer might be used. This would allow timing of specific APDU commands to be measured. This might be via manual observation or instrumentation of the process to run in a batch mode over many APDU calls.

EXAMPLE 2 Each APDU call from the host driver can be wrapped in a pair of timing calls. For example to measure end-to-end wall time using the IEEE Std 1003.1, 2003 Edition, Standard for Information Technology – Portable Operating System Interface (POSIX) function “gettimeofday” the following code fragment applies:

```
#include <sys/time.h>
struct timeval before, after;
gettimeofday(&before, NULL);
   // call to VERIFY here
gettimeofday(&after, NULL);
const unsigned int microsecs =    after.tv_sec*100000     +    after.tv_usec  -
                                 before.tv_sec*100000     -   before.tv_usec ;
```

7.4.3 Methods for measuring uncertainty

The test report shall state what is being measured (e.g. duration of on-card comparison operation plus the communications overhead). The test report shall state how accuracy of the measurement was determined.

EXAMPLE While the gettimeofday() call offers better than microsecond resolution on the LINUX platform used for testing, the measured durations include more than just the elemental card operations. The overhead includes these:

— all the calls to the PC/SC library,

— communication from the card driver process to the PC/SC smartcard daemon,

— USB communication, and

— data transmission to the smart card.

8 On-card biometric comparison interface specification

8.1 Overview

All cards shall be accessed using the mechanisms of this clause. The test report shall document any deviations from these requirements.

This includes selection of the application, reading and use of the Biometric Information Template (BIT), installation of a reference template, verification, recovery of comparison scores, and retrieval of identifiers.

NOTE The interface specification here is one possible interface for accessing IC cards. It is included here as being a clear, exact and sufficient procedure for measurement of the core algorithmic accuracy and speed of the implementation under test.

8.2 Approach to the use of ISO/IEC 7816

This interface was designed with the following criteria in mind.

— Adherence to the provisions of ISO/IEC 7816-4:2005, ISO/IEC 7816-11:2004 and the relevant part of ISO/IEC 19794 (e.g. ISO/IEC 19794-2 for finger minutia).

— To select odd INS values, indicating that the command data fields contain TLV objects.

— To only define new elements when existing standards are silent on a necessary functionality.

8.3 Establish Communications

An Answer-to-Reset shall be obtained from the card to determine the transmission protocol (T=0, T=1 or T=CL).

8.4 Selection of the test application

The test lab shall establish an Application ID. This card shall be supplied with a dedicated testing application. It shall be invoked once by using the SELECT command in Table 2. The response shall be as in Table 4.

Table 2 — Command APDU for selection of on-card comparison application

Command Parameter	Required Value	Meaning
CLA INS P1-P2	'00' 'A4' '04 0C'	 SELECT AID follows, 1100b
L_c field	16	Length of AID
Data field	See EXAMPLE below	See EXAMPLE below
L_e field	Absent	

EXAMPLE See the hexadecimal value of Table 3.

Table 3 — Example Application ID

Command Parameter	Required Value	Meaning
Data field	'F0 4E 49 53 54 20 4D 4F 43 20 54 53 54 20 50 31'	AID In ASCII, "≡NIST MOC TST P1" where P1 connotes Phase 1

Table 4 — Response APDU from selection of comparison application

Response Parameter	Meaning
Data field	Empty
SW1-SW2	See ISO/IEC 7816-4:2005

8.5 Store enrollment template on the card

For replacing the sample or template on the card the APDU of Table 5 shall be used. It uses the PUT DATA instruction to overwrite the existing reference template.

Table 5 — Command APDU for storage of reference template

Command Parameter	Required Value	Meaning
CLA INS P1-P2	'00' 'DB' '3F FF'	 PUT DATA Store anywhere in the current Dedicated File (Application DF)
L_c field	Length of command data field	
Data field	EXAMPLE: Table A.3	Data Object in BER-TLV format to be stored (tag '7F 2E')
L_e field	Empty	

Table 6 — Response APDU from storage of reference template

Response Parameter	Meaning
Data field	Empty
SW1-SW2	See ISO/IEC 7816-4:2005

If the biometric reference is too long for a single command APDU, then command chaining shall be used to send the biometric reference to the card in subsequent APDUs.

NOTE 1 Bit 5 of CLA set to 0 indicates that the command is the last or only command of a chain. Bit 5 of CLA set to 1 indicates that the command is not the last command of a chain.

NOTE 2 ISO/IEC 7816-4 does not standardize an APDU for enrollment. PUT DATA is required here, but note that some implementations use '24' CHANGE REFERENCE DATA.

NOTE 3 Operationally the process of putting the reference data on the card would ordinarily be accompanied by a writing the BIT to the card also. This would contain the biometric subtype information (for fingerprints, this is the finger position). Such data is not required here because no standard regulates the transmission of such data and because the test laboratory would usually only conduct comparisons of same-subtype templates (e.g. right index fingers).

NOTE 4 Operationally, putting reference data onto the card would generally be preceded by user authentication and establishment of a trusted channel to the card.

8.6 Read of the BIT

The test harness shall use the command of Table 7 to retrieve the BIT group template of Table 9 per the response of Table 8.

Table 7 — Command APDU for retrieval of biometric information template

Command Parameter	Required Value	Meaning
CLA INS P1-P2	'00' 'CB' '3F FF'	 GET DATA Retrieve from anywhere in the current Dedicated File (Application DF)
L_c field	'04'	
Data field	'5C' '02' '7F 61'	 Data Object identifier to be retrieved (group of BIT)
L_e field	'00'	

Table 8 — Response APDU from retrieval of biometric information template

Response Parameter	Meaning
Data field	Biometric Information Template (see Table 9)
SW1-SW2	See ISO/IEC 7816-4:2005

8.7 Use of the BIT

The test harness shall parameterize the production of enrollment samples or templates using the first BIT. The test harness shall parameterize the production of verification samples or templates using the second BIT. If only one BIT is present it shall apply it to both the enrollment and verification templates. Whether there are one or two BITs, they shall be included in a BIT group template.

All instances of a submitted card type shall have the same BIT group.

EXAMPLE Table 9 contains two BITs. These BITs have been adapted from ISO/IEC 19785-3 and ISO/IEC 19794-2:2005 for minutia template comparison. A test using these BITs would need to establish or reference the meaning of the matching algorithm parameters under 'B1'. This might be done via reference to appropriate standards.

Table 9 — Biometric Information Template based on ISO/IEC 19785-3 and ISO/IEC 19794-2 (EXAMPLE)

Tag	Len.	Value									Allowed
'7F61'	Var.	BIT group template									Values
		Tag	Len.	Value							
		'02'	1	2 (Number of BITs in the group)							1-2
		'7F60'	Var.	Biometric Information Template (BIT)							For enrollment
				Tag	Len.	Value					
				'A1'	Var.	Biometric Header Template (BHT) conforming to ISO/IEC 19785-3:2005					
						Tag	Len.	Value			
						'81'	1	biometric type (e.g. 08 = fingerprint)			
						'82'	1	biometric subtype (e.g. finger position) - These values shall be from ISO/IEC 19785-3:2007, NOT from ISO/IEC 19794-2:2005			See NOTE below
						'87'	2	CBEFF BDB format owner			0101 i.e. JTC1/SC37
						'88'	2	'00 05' (CBEFF BDB format type)			'00 05' or '00 06'
						'B1'	Var.	Biometric matching algorithm params. ISO/IEC 19794-2 Table 14			
								Tag	Len.	Value	
								'81'	2	Min. and max. numbers of minutiae, see ISO/IEC 19794-2 (subclause 8.3.3, Table 10)	
								'82'	1	Minutiae order, see ISO/IEC 19794-2"2005 (subclause 8.3.4 and Tables 11 and 12)[1)]	Native, see sec. A.6
								'83'	1	Feature handling indicator, see ISO/IEC 19794-2:2005 (Table 15)	
		'7F60'	Var.	Biometric Information Template (BIT)							For verification
				Tag	Len.	Value					
				'A1'	Var.	Biometric Header Template (BHT)					
						Tag	Len.	Value			
						'81'	1	biometric type (e.g. 08 = fingerprint)			
						'82'	1	biometric subtype (e.g. finger position) - These values shall be from ISO/IEC 19785-3:2007,NOT from ISO/IEC 19794-2:2005			See NOTE below
						'87'	2	CBEFF BDB format owner			0101 i.e. JTC1/SC37
						'88'	2	CBEFF BDB format type			0005 see sec. 0
						'B1'	Var.	Biometric matching algorithm params. ISO/IEC 19794-2 Table 14			
								Tag	Len.	Value	
								'81'	2	Min. and max. numbers of minutiae, see ISO/IEC 19794-2 (subclause 8.3.3, Table 10)	
								'82'	1	Minutiae order, see ISO/IEC 19794-2:2005 (subclause 8.3.4 and Tables 11 and 12)	Native, see sec. A.6
								'83'	1	Feature handling indicator, see ISO/IEC 19794-2:2005 (Table 15)	

NOTE Operationally the BIT tells the reader which subtype to send. But for testing it is expensive to change the BIT every time a new reference template of a new subtype is placed on the card. The test laboratory might require the tag to be present, per ISO/IEC 19785-3:2007, but should not test its value. The test laboratory may choose to never update the BIT when the reference data is changed. Values for fingerprints are given in Annex B.

1) The text in this line is a corrected version of that in ISO/IEC 19794-2:2005, Table 14, second-to-last line, which should reference subclause "8.3.4" not "8.33".

8.8 Verification

8.8.1 APDU specifications

The verification data shall be sent to the card using the VERIFY command of Table 10. The status code shall be returned per Table 11. The required comparison score is returned in a separate GET DATA command, see 8.8.4.

Table 10 — Command APDU for comparison of biometric templates

Command Parameter	Meaning
CLA INS P1-P2	'00' '21' = VERIFY '00 00'
L_c field	Length of command data field
Data field	Value Field of the template, see for EXAMPLE: Table A.3
L_e field	absent

If the biometric reference is too long for a single command APDU, then command chaining shall be used to send the biometric reference to the card in subsequent APDUs.

NOTE 1 Bit 5 of CLA set to 0 indicates that the command is the last or only command of a chain. Bit 5 of CLA set to 1 indicates that the command is not the last command of a chain.

NOTE 2 The odd INS value allows the use of P1-P2 parameters with a value of 00-00 as the indication of what is to be verified is given by the tag of the data object presented in the data field of the command.

NOTE 3 In ISO/IEC 7816-4 the use of command '21' requires verification data to be present (e.g. minutia template). The alternative INS = 20 allows verification data to be absent. Thus '21' is appropriate for testing.

NOTE 4 Operationally sending biometric probe data to the card would often be preceded by establishment of a trusted channel.

Table 11 — Response APDU from comparison of biometric templates

Response Parameter	Meaning
Data field	Empty
SW1-SW2	'90 00' (normal processing) or '63 CX' (verification failed, 'X' encodes the number of further allowed retries) or '63 00' (verification failed, no further retries allowed) (See ISO/IEC 7816-4:2005)

8.8.2 Locking of the card

A test would usually include execution of arbitrary sequences of genuine and impostor comparisons on the implementation under test. However a sequence of failed verifications (against a card's internal operating threshold) might cause the card to lock. The number of remaining attempts before locking is reported as the '63 CX' counter values. The test procedure shall embed a high-scoring comparison to reset the counter. This might be achieved by verifying the enrollment template against itself. The test plan shall state a policy on locking of cards.

EXAMPLE Every tenth comparison will be a verification of the reference template against itself. This will guarantee a successful verification. The test counter shall reset. The test will include a same-template comparison every 10 and will also attempt to execute high-scoring comparisons with sufficient frequency to ensure that low scoring verification comparisons are infrequent enough to prevent card locking. The testing laboratory might discontinue testing of cards for which these mechanisms are insufficient to prevent locking.

8.8.3 Locking of the PC-based algorithm

PC-based implementations of on-card comparison algorithms shall allow arbitrary sequences of comparisons, and shall never lock.

8.8.4 Comparison scores

The card shall allow retrieval of a two-byte comparison score via the GET DATA APDU of Table 13. Native matching scores outside the range [0,65535] should be internally remapped by the implementation.

Table 12 — Command APDU for retrieval of verification comparison score

Command Parameter	Meaning
CLA INS P1-P2	'00' 'CB' = GET DATA '3F FF' = Retrieve from anywhere in the current Dedicated File (Application DF)
L_c field	'03'
Data field	'5C' '01' 'C0' Data Object identifier to be retrieved (two byte comparison score)
L_e field	'04' (2+2) length of BER-TLV encoded data object to be retrieved

Table 13 — Response APDU for retrieval of verification comparison score

Response Parameter	Required values	Meaning
Data field	'C0' Tag of the score data '02' Length of the score value xx xx Score value	Big-endian score from the last comparison on [0-65535]
SW1-SW2	See ISO/IEC 7816-4	

NOTE Operationally the comparison subsystem rarely returns comparison scores to the application. This is intended to impede hill-climbing attacks [ ]. This motivates the use here of a non-standard tag ('C0') to retrieve the verification comparison score. Its use is a special case intended specifically for testing. It would not normally be available for card applications in operational mode. The tag has a meaning for the test application only.

8.8.5 Prohibition of stateful behavior

Although template update is one potential means of improving operational performance, it is beyond the scope of this test. Cards shall not perform template update. The consequence would likely be to give answers different from those produced in the PC-based testing, where template update is prohibited by C.2.5.1.4.

8.9 Reading card identifier

Table 10 of ISO/IEC 7816-6:2004 provides a structure for card data under constructed data element tag '66'. This structure shall be available to be read using the GET DATA APDU of Table 14.

Table 14 — Command APDU for retrieval of Card identifier

Command Parameter	Meaning
CLA INS P1-P2	'00' 'CB' = GET DATA '3F FF' = Retrieve from anywhere in the current Dedicated File (Application DF)
L_c field	'03' length of command data field
Data field	'5C' '01' '66' Data Object identifier to be retrieved (Card Data)
L_e field	'00'

For administration purposes and to identify the card under test the testing laboratory shall use the information contained in the response field of Table 15 which shall contain a discretionary field, tag '73', containing the card version information in tag '88'.

Table 15 — Response APDU for retrieval of Card identifier

Response Parameter	Meaning	Minimal response value
Data field		73 06 88 04 <4 byte CBEFF ID>
SW1-SW2	See ISO/IEC 7816-4	

8.10 Reading comparison subsystem identifier

Table 12 of ISO/IEC 7816-6:2004 provides a structure for application related data under constructed data element tag '6E'. This structure shall be readable using the APDU of Table 16 and Table 17.

Table 16 — Command APDU for retrieval of Comparison subsystem identifier

Command Parameter	Meaning
CLA INS P1-P2	'00' 'CB' = GET DATA '3F FF' = Retrieve from anywhere in the current Dedicated File (Application DF)
L_c field	'03' length of command data field
Data field	'5C' '01' '6E' Data Object identifier to be retrieved (Application related data)
L_e field	'00'

The response field shall contain a discretionary field, tag '73', containing the comparison subsystem identifier in tag '99'.

Table 17 — Response APDU for retrieval of Comparison subsystem identifier

Response Parameter	Meaning	Minimal response value
Data field		73 06 99 04 <4 byte CBEFF ID>
SW1-SW2	See ISO/IEC 7816-4	

Annex A
(informative)

Conversion of ISO/IEC 19794-2 record to compact size templates

A.1 Background

A.1.1 Purpose

This informative Annex gives an example of text that might appear in a test plan. It gives explicit definitions of the structures to be used in the testing process. In some cases it may be possible for a test to proceed by just citing an underlying standard or by stating that fully proprietary opaque data records are allowed. In the example in this Annex two profiles of fingerprint minutiae standards are presented.

A.1.2 Overview

The ISO/IEC 19794-2 standard defines a record format for off-card storage of minutiae as templates. It also defines a compact-size format suitable for on-card storage and matching. The off-card format differs from the on-card format in terms of syntactic encoding and semantic aspected including spatial and angular resolution. Clause A.1.3 shows an example profile of the off-card record format. Clause A.1.4 shows the corresponding target profile of the on-card format. The accuracy implications of converting from the former to the latter are small.

A.1.3 The record format

One possible profile of the ISO/IEC 19794-2 record format is shown in Table A.1. Note that the minutia quality field is populated. The use of a minutia quality value is normatively required by clause 8.3.1 of ISO/IEC 19794-2:2005 for the preparation of conformant on-card comparison data objects. This process is described in clause A.5.3.

NOTE Existing minutia standards give poor guidance on what quality means.

NOTE On-card comparison applications may require production of ISO/IEC 19794-2 records instead of compact-size card templates because the following points hold.

— Three-byte ISO/IEC compact card minutia points are strict “semantic children” of six-byte ISO/IEC 19794-2:2005 record format minutia points.

— The quality field of ISO/IEC 19794-2 records is considered an essential mechanism for improving minutia-based interoperability from the state measured prior studies [2][10].

— ISO/IEC 19794-2 compact card templates can exist only as terminal objects, i.e. they cannot be used in the preparation of other standardized minutia records.

With regard to issues of minutia selection and placement see [12].

Table A.1 — Record profile of ISO/IEC 19794-2:2005 standard

	Field name and ISO/IEC 19794-2:2005 clause numbers in parentheses	Values Allowed	Informative Remarks
1.	Format Identifier (7.3.1)	0x464D5200	i.e. ASCII "FMR\0"
2.	Version Number (7.3.2)	0x20323000	i.e. ASCII ' 20' followed by a NULL string terminator.
3.	Record Length (7.3.3)	$32 \leq L \leq 800$	26 record header + 4 view header +2 extended data length + 6K. Max K is 128
4.	Capture Equipment Certifications (7.3.4)	0	
5.	Capture Device Type ID (7.3.5)	0	
6.	Size of Scanned Image in x direction (7.3.6)	MIT	Inherited directly from input data
7.	Size of Scanned Image in y direction (7.3.7)	MIT	
8.	X (horizontal) resolution (7.3.8)	197	
9.	Y (vertical) resolution (7.3.9)	197	
10.	Number of Finger Views (7.3.10)	1	
11.	Reserved Byte (7.3.11)	0	
12.	Finger Position (7.4.1.1)	MIT	Inherited directly from input data
13.	View Number (7.4.1.2)	0	
14.	Impression Type (7.4.1.3)	0 or 2	Inherited directly from input data
15.	Finger Quality (7.4.1.4)	MIT	Inherited directly from input data
16.	Number of Minutiae (7.4.1.5)	$0 \leq K \leq 128$	K minutiae data blocks
17.	Minutiae Type (7.4.2.1)	01b, 10b, or 00b	
18.	Minutiae Position (7.4.2.2)	MIT	
19.	Minutiae Angle (7.4.2.3)	MIT	
20.	Minutiae Quality (7.4.2.4)	0, $1 \leq Q \leq 100$	0 = unsupported
21.	Extended Data Block Length (7.5.1.1)	0	Zero mean no extended data
MIT = mandatory at time of instantiation			

A.1.4 The compact-size format

This clause defines the data to be sent to PC-based and card-based comparison implementations. It is included here because ISO/IEC 19794-2:2005 and its corrigenda and revisions define multiple templates combining

— three encodings (record, card-normal, card-compact),

— versions with and without headers,

— variants differing in their minutia placement semantics,

— presence of standardized extended data (zonal quality etc), and

— presence of non-standard, proprietary, extended data.

Tests might use ISO/IEC 19794-2 compact-size card templates for which

— the record and view headers would be absent,

— both standardized and proprietary extended data would be absent.

The test harness would convert the ISO/IEC 19794-2 record instances of Table A.1 to produce Table A.2 instances known as ISO/IEC 19794-2:2005 compact-card templates.

Table A.2 — Card profile of ISO/IEC 19794-2:2005 standard

	Field name	Size (bits)	Values allowed	Units	**Remark**
1.	X coordinate	8	[0,255]	Expressed in units of 0.1 mm	**View data S instances of the minutiae data would be present**
2.	Y coordinate	8	[0,255]	Expressed in units of 0.1 mm	
3.	Minutiae type	2			
4.	Minutiae angle	6	[0,63]	Resolution is 5.625 degrees	

These would be sent to the on-card biometric comparison implementations in the TLV format of Table A.3. The cards would accept templates in that format.

Table A.3 — ISO/IEC 19794-2 minutiae template DO

Tag	L	Value					Comment
'7F2E'	L1	Biometric data template					
		Tag	L	Value			
		'81'	L2	Finger minutiae data			
				Field	Size (bits)	Valid Values	
				X coordinate	8	[0,255]	S instances
				Y coordinate	8	[0,255]	
				Minutiae type	2		
				Minutiae angle	6	[0,63]	

If a test sought to use zonal quality data the DO would include tag '94' as shown in Table A.4. The cards would accept templates for which optional zonal quality block conforms to Table A.5. This data is a modified version of that inserted into ISO/IEC 19794-2:2005 by Technical Corrigendum 1.

Table A.4 — ISO/IEC 19794-2 zonal quality DO

Tag	L	Value					Comment
'7F2E'	L1	Biometric data template					
		'94'	L3	Zonal Quality Data	5+var	See **Table**	0 or 1 instances

Table A.5 — ISO/IEC 19794-2 zonal quality data

	Field	Length (bytes)	Values Allowed	Informative Remarks
1	Horizontal Resolution of the Quality Map (8.4.1.1.2)	1		See Note 1 and Example 1
2	Vertical Resolution of the Quality Map (8.4.1.1.2)	1		
3	Quality Map Width (8.4.1.1.3)	1		# cells in x horizontal direction
4	Quality Map Height (8.4.1.1.3)	1		# cells in y vertical direction
5	Cell Quality Information Depth (8.4.1.1.4)	1	1, 2, 4, 8	Not 0.
6	Cell Quality Data (8.4.1.1.5)	L		Packed bits

NOTE ISO/IEC 19794-2:2005/Cor.1 has one field for cell quality resolution, i.e. it assumes the x-y resolutions are equal. However, the ISO/IEC 19794-2:2005 record standard (i.e Table) allows different cell resolutions in x and y. Therefore, if the process of converting ISO/IEC 19794-2 record to compact-card templates is to become viable operationally, then card zonal quality data needs to support anisotropic resolutions.

EXAMPLE If the horizontal cell dimension in a ISO/IEC 19794-2 zonal quality block (clause 7.5.4.1 of ISO/IEC 19794-2:2005) is 20 pixels, and the corresponding horizontal resolution is 197 pixels per centimeter (clause 7.3.8 of ISO/IEC 19794-2:2005), then the value of the entry on line 1 of this table (i.e. the number of cells per decimeter) will be round(10 * 197 / 20) = 99, where the rounding operator is nowhere standardized.

A.2 Minutia uniqueness

A non-ISO requirement is for the minutia points to be unique. Template generators should output unique (x, y, and theta) tuples and the testing laboratory might implement checks to detect deviations from such behavior. This requirement is instituted because non-uniqueness impedes some matching algorithms.

A.3 Presence of BITs on card

Each submitted card might be populated with one or two BITs per clause 8.6. These would be treated as read-only data. These would be supplied in the structure given in Table 9 which leverage the BIT and BIT grouping structures of ISO/IEC 7816-11:2004 (Tables 1 and 2).

The BITs parameterize the production of templates that a reader, or other system, should send to the requesting card: For a reference template TR, a verification template TV, and a PC or card-based comparison subsystem, M, the test will compare BIT-processed versions of the templates to produce a comparison score

$$s = M(BR(TR), BV(TV))$$

where BR and BV denote the functions representing the BIT parameterization. Operationally the BIT parameters (e.g. maximum number of minutiae) might be sent *as inputs* to a template generator. Such specialization may be computationally prohibitive in the context of an interoperability test because, for example, if a test used T templates, N template generators and C cards, the O(TNC) image-to-template generations would be needed. An alternative is to standardize the minutiae template reduction process as follows.

A.4 Use of BITs

The test laboratory would use the BITs read from the card to parameterize BOTH the conversion of templates sent to the card and to the PC-based match operation. As depicted in Figure A.1, the conversion operation proceeds with a pruning operation (sec. A.5.3), a sorting operation (sec. A.6), and a re-encoding (conversion from 14 bit to 8 bit position coordinates, quantization of coordinates, and conversion of 8 bit to 6 bit minutia angle).

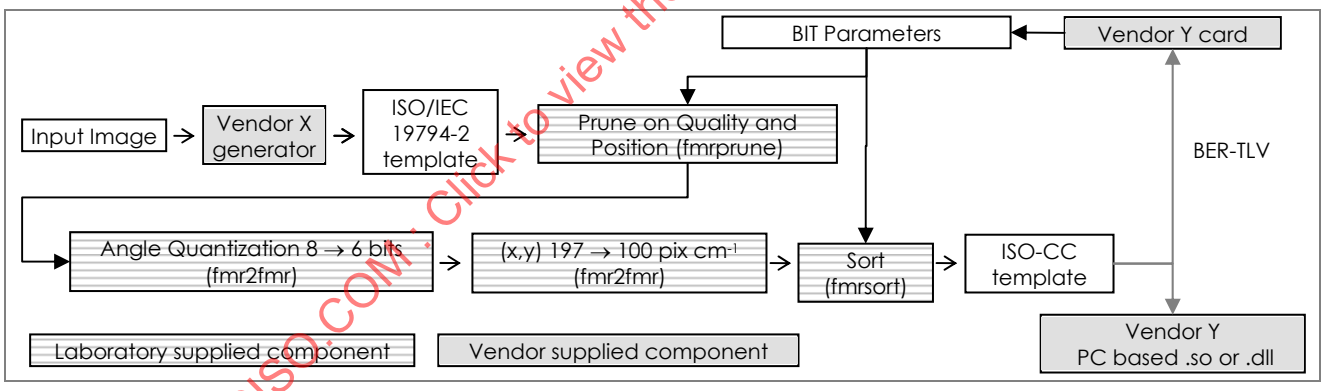

Figure A.1 — Conversion of INCITS 378 data to ISO/IEC 19794-2 data

A.5 Number of minutiae

A.5.1 Limits on number

The testing laboratory should not impose algorithmic constraints. However, the minimum and maximum numbers of minutia a card may accept might be regulated as follows

— The one-byte value implies a range of [0,255],

— Because some templates will naturally contain 0 minutia (i.e. the algorithm does not find any), the card may need to accept values below its needed minimum.

— One trial [2] imposed a 128 minutia maximum. This is arguably too high given that leading systems produced a median of 41 minutiae from each image with the 5 % and 95 % quantiles being 24 and 61 respectively over four large operational single index finger flat-impression datasets [2].

— A short-length APDU command constrains the maximum number of three-byte minutia to 83. ISO/IEC 7816-4 command chaining would be used for larger templates, as necessary.

— Informative Annex D.1.1 of ISO/IEC 19794-2:2005 recommends the minimum number of minutiae for enrollment to be 16, and for verification, 12. It also recommends the maximum number of minutiae for enrollment and verification is 60. These are recommendations only.

A.5.2 Effect of the BIT

The test harness would send single-view templates to the PC-based and card-based matching implementations. The reference and verification templates should be parameterized by their respective BITs, as follows. If,

— the value indicated in the BIT for the minimum number of minutiae is 0 ≤ ≤ 255,

— the value indicated in the BIT for the maximum number of minutiae is 0 ≤ M ≤ 255,

— the number of minutia present in a (generally third-party) verification template is K, then

— the number of minutia sent to the card would be S where

$$S = \begin{cases} M & \text{if } K \geq M \\ K & \text{if } K < M \\ K & \text{if } K < N \end{cases}$$

Note that the BIT parameter N is ignored. This is necessary because some input templates will inevitably have zero minutiae. The comparison subsystem should execute successfully when either or both of the input templates contains fewer than N minutiae (an alternative would be to fill with N-K randomly generated minutiae).

The testing laboratory should reject cards for which N > M.

A.5.3 Pruning mechanism

When an on-card biometric comparison implementation indicates the capability to take no more than M minutiae, a refined version of the guidance given in the last paragraph of clause 8.3.1 of ISO/IEC 19794-2:2005

> If the number of minutiae exceeds the maximum number processible by a card, truncation is necessary. The truncation is a 2 step process. At first, finger minutiae of poor quality are eliminated. If still too many minutiae are there, then truncation shall be made by peeling off minutiae from the convex hull of the minutiae set and before sorting into the order required by the card.

should be used. Specifically the test laboratory might replace the convex hull method with one based on the distance of a minutia from a center. This is based on the ISO/IEC 19794-2:2005 8.3.4 guidance for polar ordering. Thus given a INCITS 378 template containing K minutiae and a BIT request for no more than M minutiae test laboratory software will remove K - M minutiae as follows.

Minutiae with the lowest quality value are removed first. If two or more minutia have an equal quality value, then the one with the largest value of the integer quantity

$$r^2 = (x - x_c)^2 + (y - y_c)^2$$

is removed. Finally if those values are tied, then the ISO/IEC 19794-2:2005 polar ordering instruction to prioritize small angle minutiae is applied.

NOTE 1 The ISO/IEC 19794-2:2005 material on polar coordinates was intended for sorting, not pruning, but is suitable for pruning also because the convex hull approach is complex.

NOTE 2 It is clear that a quality algorithm producing many levels of quality will cause the pruning operation to prune on r^2 only occasionally. Conversely, a quality algorithm producing few levels of quality will cause r^2 pruning to be more dominant. A template generator should not return quality values that are dependent solely on r^2 because they would ordinarily indicate utility of the minutia.

A.5.4 Pruning center

Template generators may additionally report the coordinates of an appropriate center about which pruning should be conducted. This differs from the center-of-mass specification for sorting given in ISO/IEC 19794-2:2005. However, this may be particularly inappropriate when large numbers of minutia are reported in a noisy part of the image.

The test harness should conduct pruning about the center coordinates from the template generator, if supplied, otherwise about the center of mass, per ISO/IEC 19794-2:2005.

A.6 Sort order of minutiae

A.6.1 Support for ordering

Although template generators are likely to produce templates whose minutiae have an arbitrary order, ISO/IEC 19794-2 defines several geometric orderings of the minutia. The x-y and y-x sorting methods support extension of the spatial range of a fingerprint (e.g. for rolled prints) in one dimension. The polar method supports a center-first sort.

The unsorted, Cartesian y-x, Cartesian x-y and polar sorting methods would be supported (because the standard defines these as options). Open-source "C" code is maintained here http://www.itl.nist.gov/iad/894.03/nigos/biomdi.html and is called by our on-card biometric comparison application here http://www.itl.nist.gov/iad/894.03/nigos/biomapp.html. The test plan should state whether the test laboratory would accept commercial code for this purpose. The test laboratory might institute a conformance test for implementations that do.

However, commercial readers will need to include such software in addition to the pruning software. This adds complexity and a "degree of freedom" that would better be handled as a natural property of the matching algorithm. Although the European Citizen Card specification, CEN/TS 15480-2, requires implementations to accept arbitrarily sorted data, the SC37/WG3 intent was to allow sorting. The exact requirements of ISO/IEC 19794-2:2005, Clause 8 are unclear.

A.6.2 Modulo sorting for large images

The test plan should indicate whether or not implementations will be required to handle the modulo-sorted minutia records defined in ISO/IEC 19794-2:2005 clause 8.3.4. Such would occur if wide (e.g. rolled) images were to be used.

EXAMPLE Note that archival imagery used is at most 500 pixels in width and height, and is scanned at 19.7 pixels mm^{-1}, and therefore all possible minutiae coordinates can be encoded in 8 bits without modulo sorting (or removal).

Annex B
(informative)

Standardized Finger-Position Codes

The finger position codes differ in the fingerprint standards and the smart-card standards.

For all interactions with the card ISO/IEC 19785-3:2007 finger position codes should be used. For all interactions with PC-based implementations ISO/IEC 19794-2:2005 finger positions should be used. A test laboratory should transcode any values using the Table associations whenever needed. The table summarizes the two base standards and is included here for informative purposes only.

Table B.1 — ISO/IEC 19794-2 and ISO/IEC 19785-3 finger position codes

Finger ID Biometric subtype	ISO/IEC 19794-2:2005		ISO/IEC 19785-3:2007	
	Binary value	Hex Value	Binary value	Hex Value
No information given	00000b	00	00000b	00
right thumb	00001b	01	00101b	05
right index	00010b	02	01001b	09
right middle	00011b	03	01101b	0D
right ring	00100b	04	10001b	11
right little	00101b	05	10101b	15
left thumb	00110b	06	00110b	06
left index	00111b	07	01010b	0A
left middle	01000b	08	01110b	0E
left ring	01001b	09	10010b	12
left little	01010b	0A	10110b	16