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.

