TECHNICAL REPORT

ISO/IEC TR 30117

First edition
2014-03-15

Information technology — Guide to on-card biometric comparison standards and applications

Technologies de l'information — Guide des normes et applications de comparaison biométrique sur carte

Reference number
ISO/IEC TR 30117:2014(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

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 17, *Cards and personal identification*.

Introduction

There are a large number of applications where the need of implementing jointly integrated circuit cards – ICC (i.e. smart cards) and biometrics can arise. In those cases, system designers and integrators have to be aware of the whole range of international standards and technical reports that may be applicable. All these potential reference documents have been developed by different standardization bodies and different subcommittees. For example, those standards dealing with ICCs are defined within ISO/IEC JTC 1/SC 17, while those dealing with biometrics are developed in ISO/IEC JTC 1/SC 37. Furthermore, when security aspects are to be considered, the works in ISO/IEC JTC 1/SC 27 have to be referenced.

In this context, the system designer and developer have in their hands a large number of documents, and on some occasions little information about which of them are really applicable to the application to be developed, and which alternatives can be faced.

This Technical Report provides a guide to those developers by enumerating and referring to those published standards and reports, relating them to the kind of application to be developed. When referring to different applications, these will be classified attending to the authentication needs of the application, not to the final sector where the application is to be deployed.

Interactions among standards cover different implementation levels, from data formats to be used to the application profiles, including application programming interfaces (APIs) and security mechanisms.

This Technical Report places special emphasis on providing recommendations and policies needed by developers to integrate applications related to on-card biometric comparison.

The structure of this Technical Report is as follows.

— Clause 4 provides a first overview to the different decisions that have to be taken when developing an application that may involve the use of ICCs and biometrics.

— Clauses 5 to 9 provide an overview to the different International Standards and Technical Reports that may be applicable to the application to be developed.

— Clause 10 will provide examples of implementations that may be used by application designers and developers as guidelines.

Information technology — Guide to on-card biometric comparison standards and applications

1 Scope

This Technical Report summarizes how the international standards, recommendations and technical reports dealing with identification cards, biometrics and/or information security relate to each other with regard to the joint use of biometrics and integrated circuit cards. It also provides further recommendations and policies needed by developers to integrate applications related to on-card biometric comparison.

2 Terms and definitions

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

2.1
biometric probe
biometric query
biometric sample or biometric feature set input to an algorithm for use as the subject of biometric comparison to a biometric reference(s)

Note 1 to entry: The term comparison refers to comparison in the biometric sense.

Note 2 to entry: The subject/object labelling in a comparison might be arbitrary. In some comparisons a biometric reference might be used as the subject of the comparison with other biometric references or incoming samples used as the objects of the comparisons. For example, in a duplicate enrolment check a biometric reference will be used as the subject for comparison against all other biometric references in the database.

Note 3 to entry: Typically in a biometric comparison process, incoming biometric samples serve as the subject of comparison against objects stored as biometric references in a database.

[SOURCE: ISO/IEC 2382-37:2012]

Note 4 to entry: In the scope of ISO/IEC 7816-11, these two terms are used under the more generalized term of “biometric verification data”.

2.2
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison

EXAMPLE Face image stored digitally on a passport; Fingerprint minutiae template on a National ID card; Gaussian Mixture Model for speaker recognition, in a database.

Note 1 to entry: A biometric reference may be created with implicit or explicit use of auxiliary data, such as Universal Background Models.

Note 2 to entry: The subject/object labelling in a comparison might be arbitrary. In some comparisons a biometric reference might be used as the subject of the comparison with other biometric references or incoming samples used as the objects of the comparisons. For example, in a duplicate enrolment check a biometric reference will be used as the subject for comparison against all other biometric references in the database.

[SOURCE: ISO/IEC 2382-37:2012]

Note 3 to entry: In the scope of ISO/IEC 7816-11, this term is used under the more generalized term of “biometric reference data”.

2.3
biometric feature
numbers or labels extracted from biometric samples and used for comparison

Note 1 to entry: Biometric features are the output of a completed biometric feature extraction.

Note 2 to entry: The use of this term should be consistent with its use by the pattern recognition and mathematics communities.

Note 3 to entry: A biometric feature set can also be considered a processed biometric sample.

Note 4 to entry: Biometric features may be extracted from an intermediate biometric sample.

Note 5 to entry: Filters applied to biometric samples are not themselves biometric features, however the output of the filter applied to these samples may be. Therefore, for example, eigenfaces are not biometric

[SOURCE: ISO/IEC 2382-37:2012]

2.4
biometric sample
analog or digital representation of biometric characteristics prior to biometric feature extraction

EXAMPLE A record containing the image of a finger is a biometric sample.

[SOURCE: ISO/IEC 2382-37:2012]

2.5
biometric template
set of stored biometric features comparable directly to probe biometric features

Note 1 to entry: In the scope of ISO/IEC 7816, the term template has a completely different meaning, being in that case the “value field of a constructed data object”, no matter if the data object relates to biometrics or not.

2.6
intermediate biometric sample/probe
biometric sample/probe resulting from intermediate biometric sample processing

EXAMPLE Biometric samples that have been cropped, down-sampled, compressed or enhanced are examples of intermediate biometric samples.

[SOURCE: ISO/IEC 2382-37:2012]

2.7
intermediate biometric sample processing
any manipulation of a biometric sample that does not produce biometric features

EXAMPLE Examples of intermediate biometric sample processing include cropping, down-sampling, compression, conversion to data interchange formats standard and image enhancement.

[SOURCE: ISO/IEC 2382-37:2012]

2.8
processed sample/probe
biometric sample/probe resulting from biometric sample processing that is ready to be used for storage as a biometric reference, or to be compared with a previous biometric reference

EXAMPLE Fingerprint minutiae or iris codes are examples of processed biometric samples.

2.9
captured biometric sample
raw biometric sample (deprecated)
biometric sample resulting from a biometric capture process

[SOURCE: ISO/IEC 2382-37:2012]

3 Symbols and abbreviated terms

API	Application Program Interface
BIR	Biometric Information Record
CBEFF	Common Biometric Exchange Format Framework
ICC	Integrated Circuit Card
IFD	Interface Device
SB	Security Block, as defined in CBEFF standard ISO/IEC 19785-1
COS	Card Operating System

4 Relationships between biometrics and ICCs

ISO/IEC 24787[16] provides a comprehensive introduction to the different ways that biometrics and ICCs can be integrated into a final application. This is summarized as follows as to provide a brief introduction to the reader of this Technical Report. When integrating biometrics into ICCs, four different approaches can be followed:

— Store on card: In this case, the ICC is used to store the biometric reference. The application will read from the ICC the biometric reference, as needed, and execute all the authentication process within the IFD or rest of the system. The COS has no extra control on the biometric data, apart from using the same kind of mechanisms that when storing any other kind of data into the ICC.

— On-card biometric comparison: In this approach the ICC not only stores the biometric reference, but also performs the biometric comparison inside the card, once an external biometric probe has been received by the ICC. With this approach, the COS can use the same control with the biometric reference, as with those administrative keys stored in the card (e.g. not allowing the reading of the biometric reference, controlling the number of consecutive unsuccessful comparisons carried out, blocking the authentication mechanism if a certain number of consecutive unsuccessful comparisons is reached, etc.). Also the COS can control de access to other information in the card, or commands within the card, considering the result of a previous on-card biometric comparison. In this technology the biometric probe is usually considered to be a biometric feature set, instead of a raw sample.

— Work-sharing mechanism for on-card biometric comparison: the previous approach may not be able to be fully integrated into the ICC due to several reasons, being the most frequent, the lack of processing capabilities of the ICC. In such a case, it might be possible that part of the process is executed in the IFD or system, and the results transmitted to the ICC to end the comparison process. Although this is initially defined for sharing the work on the comparison algorithm, this same schema can be used for the pre-processing and the feature extraction phases of the biometric process. In the former case, the biometric probe to be sent to the card is to be a biometric feature set, while in the latter case the biometric probe can be a raw sample, an intermediate sample or a processed sample.

— System-on-Card: this approach is based on the inclusion of all the steps of the biometric process within the ICC, including the sample acquisition, i.e. the sensor is embedded into the ICC. Due to this definition, only certain modalities can be considered with the technology existing nowadays, being restricted to those where the sensor is small and flexible as to allow the ICC to pass the physical and mechanical test methods defined in ISO/IEC 10373-1. If the physical restrictions are removed and other kind of embodiments are selected (keeping conformance to the rest of applicable ICC standards), then the number of biometric modalities can be increased.

With these initial concepts, the application designer or developer is to take several decisions as to define the whole system and the relationship to be established between biometrics and ICCs. The following decision tree is provided for illustration purposes, where the subsequent clauses in this Technical Report are referenced.

a) Is the system going to be implementing an authentication scheme (i.e. the user claims his/her identity and the comparison is only made between the sample provided and the biometric reference of the claimed user), or an identification scheme (i.e. the biometric sample is to be compared to the whole database of users enrolled)?

   1) If an identification scheme is used, then there is no need to a further relationship between biometrics and ICCs, and in such case this Technical Report is not applicable.

b) Is the system considering the use of a centralized database, or is it going to be implemented in a distributed way?

   1) If a centralized database is going to be used and such database is going to be contacted at every single authentication attempt, then the need of further relationship between biometric information and ICC is not needed. Therefore this Technical Report is not applicable. The ICC will act only as a mean to claim the user identity.

c) Is there an initial requirement of the biometric modality to be used?

   1) With an initial requirement, a set of further decisions may be already taken, such as the possibility of using on-card biometric comparison, work-sharing or system-on-card.

   2) If there is no initial requirement the decision on the modality can be taken as any other requirements are satisfied.

   3) Once the modality is chosen, then the interoperable data formats have to be checked (see Clause 5)

d) Which are the initial cost requirements?

   1) If there is the requirement of using low cost ICCs, then alternatives such as on-card biometric comparison, work-sharing or system-on-card can be compromised.

   2) Furthermore if storage capacity is impacting the ICC cost, then the number of references to be stored on the card, or the modalities to be used can be limited and/or the use of compact data formats may become a major requirement (see Clause 5).

e) Which are the needs for interoperability?

   1) If there is no need, then the designer may decide to create his/her own solution without following any standard. Therefore this Technical Report may not be applicable. This option in not recommended as the need for interoperability may arise at any time during the project, or when applying the development done for the current project to future ones.

   2) If interoperability is required for exchanging data, then refer to Clause 5. As it will be seen, it may happen that for reaching global interoperability, being independent on the algorithm to be used, the use or raw sample data formats may become the only viable solution.

   3) If interoperability is required to have multiple technological providers, then not only data interoperability is requested, but also interoperability at API level and from security mechanisms. See Clauses 6 and 7.

   4) The use of more complex products, such as on-card biometric comparison ones or System-on-Card, contributes to reach interoperability, as there is only the need to focus on data interoperability (and may be security mechanisms), avoiding all technological differences coming from technological solutions at algorithm level.

f) In many parts of the world, biometric data are considered as personal data, and therefore are to be protected, as to ensure citizen's privacy. Depending on the environment where the application is going to be deployed, the use of security mechanisms becomes a major requirement. See Clause 6 for the works already done in this area.

g) The most typical scenario for designing and developing a new project involving ICCs and biometrics, is integrating technological modules from several providers. Furthermore, many project designers require more than one provider for each technological module to be integrated. In this kind of scenarios, standardized APIs are to be used to ease integration. Clause 7 provides further details.

h) For certain applications there is the need of following already defined specifications. Clause 8 will describe the current available specifications.

i) Last but not least, either to select the technological modules to be integrated, or to provide final results to the end user about the behaviour of the whole project, evaluation methodology is required. Clause 9 will describe the evaluation-related standards related to ICC, biometrics and security.

In addition to all this information, Clause 9 provide guidance for implementing on-card biometric comparison solutions, based, or not, on ISO/IEC 24787.[16]

5 Data Formats

ICC related standards do not provide serious constraints about the format of the data to be exchanged and/or stored. As long as these data are encapsulated within the ICC protocol and COS specification (i.e. following ISO/IEC 7816-4[2], ISO/IEC 7816-6[3], ISO/IEC 7816-8[4] and ISO/IEC 7816-9[5], and the manufacturer's restriction to the COS implemented in the ICC), the only standards to be considered for data formats are the ones related to biometrics.

ISO/IEC 19794[11] series of International Standards provide interoperable ways to code biometric data, depending on the modality. This multipart standard provides a framework to be applied to all parts, some data formats for raw sample data (e.g. sample images), and some others for processed sample data (e.g. fingerprint minutiae). This family of standards have currently two different generations defined, that are both still accepted. The first generation of standards is the one published in 2005–2007, and it has been requested to be kept available by ISO/IEC to keep compliance with the standards of some world-wide applications, such as the ePassport. But for new project it is recommended that the second generation of these standards is followed. This generation is composed of those standards being published in 2011 and beyond this date.

The second generation of ISO/IEC 19794[11] is a multipart standard with the following structure:

— Part 1 provides a general framework to be applied to all the other parts. It defines the general structure for the biometric records and the common elements of such structure. It tells that each biometric information record (BIR) is to be composed of a general header that introduces the information to be followed, and one or more representations (i.e. biometric samples), which are structured into a representation header and the representation data. Part 1 defines those common elements of each of the headers. This is defined for both, a binary coding and an XML coding. In addition to this, it also defines the framework for the conformance testing of those BIRs defined within this family of standards.

— Part 2-n provide the information about those extra elements to be added to the different headers, plus the way the representation data are to be coded. This is done for each of the modalities defined. Up to date, the ISO/IEC 19794[11] series of standards defined the following modalities:

  — Part 2: finger minutiae

  — Part 4: finger image

  — Part 5: face image

  — Part 6: iris image

  — Part 7: handwritten signature time series