TECHNICAL REPORT

ISO/IEC TR 30117

Second edition

Information technology — Guidance on standards and applications for the integration of biometrics and ICC

PROOF/ÉPREUVE

Reference number
ISO/IEC TR 30117:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

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 www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

This second edition cancels and replaces the first edition (ISO/IEC TR 30117:2014) which has been technically revised.

The main changes compared to the previous edition are as follows:

— Addition and update of references to the related projects in all relevant standardization bodies.

— Addition to the Scope, to include not only on-card biometric comparison, but all other interactions of biometrics and integrated circuit cards (ICCs).

— Addition of the example of the ePassport, which is a widely-deployed application using off-card biometric comparison.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

There are a large number of applications where the need for implementing jointly integrated circuit cards (ICC) and biometrics can arise. In those cases, system designers and integrators need to be aware of the range of international standards and technical reports that are applicable. All of these potential reference documents have been developed by different standardization bodies and committees. ISO/IEC JTC1 (Joint Technical Committee) subcommittees develop standards in the following areas:

ICCs:

ISO/IEC JTC 1 SC 17 (*Information technology — Cards and security devices for personal identification*)

Security aspects:

ISO/IEC JTC 1 SC 27 (*Information technology — Information security, cybersecurity and privacy protection*)

Biometrics:

ISO/IEC JTC 1 SC 37 (*Information technology — Biometrics*)

Other regional or sectoral standardization bodies are also applicable.

In this context, the system designer and developer have a large number of documents at their disposal, but with little information about which of them is really applicable. There are no general rules, as depending on the application, different alternatives are available.

This document provides guidelines to those developers by enumerating and referring to those published standards and reports and relating them to the kind of application to be developed. When referring to different applications, these will be classified attending to the verification 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 document places special emphasis on providing recommendations and policies needed by developers to integrate the use of both biometrics and ICCs in applications.

The structure of this document is as follows:

— Clause 5 provides a first overview to the different decisions that have to be taken when developing an application that can involve the use of ICCs and biometrics.

— Clauses 6 to 10 provide an overview to the different International Standards and Technical Reports that can be applicable to the application to be developed.

— Clause 11 provides examples of implementations that can be used by application designers and developers as guidelines.

All ISO/IEC documents mentioned in this document are listed in the Bibliography at the end of this document.

NOTE Future editions of this document will add more information about Biometric System-on-Card technology and the use of the PBO command.

Information technology — Guidance on standards and applications for the integration of biometrics and ICC

1 Scope

This document summarizes how some of the main international standards and recommendations approach personal identification and its related information security, with regard to the integration of biometrics and ICCs. It also provides guidance for developers on how to integrate biometrics and ICCs in applications.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

3 Terms and definitions

For the purpose of this document, the terms and definitions given in ISO/IEC 2382-37 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

NOTE ISO/IEC 2382-37 is freely available at https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

3.1
biometric template
set of stored biometric features comparable directly to probe biometric features

Note 1 to entry: In the ISO/IEC 7816 series, the term "template" has a completely different meaning, being in that case the “value field of a constructed data object”, regardless to whether the data object relates to biometrics or not.

4 Symbols and abbreviated terms

APDU	Application Protocol Data Unit
API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
BAC	Basic Access Control
BDB	Biometric Data Block (as defined in the ISO/IEC 19785 series)
BDIR	Biometric Data Information Record

BFP	Biometric Function Provider
BIAS	Biometric Identity Assurance Services
BioAPI	Biometric Application Programming Interface
BIR	Biometric Information Record
BSoC	Biometric System-on-Card
BSP	Biometric Service Provider
CA	Certification Authority
CBEFF	Common Biometric Exchange Format Framework (defined in the ISO/IEC 19785 series)
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
COS	Card Operating System
DNI	Documento Nacional de Identidad (Spanish National ID Card)
DO	Data Object
EAC	Extended Access Control
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
IFD	Interface Device
LDS	Logic Data Structure
MRTD	Machine Readable Travel Document
NIST	National Institute of Standards and Technology
PAD	Presentation Attack Detection
PBO	Perform Biometric Operation (command defined in ISO/IEC 7816-11)
PIV	Personal Identity Verification (US Federal government-wide credential)
PKI	Public Key Infrastructure
PP	Protection Profile
REST	Representational State Transfer
SC17	ISO/IEC JTC 1/SC 17
SC27	ISO/IEC JTC 1/SC 27
SC37	ISO/IEC JTC 1/SC 37
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol

ST	Security Target
TLV	Tag Length Value (data coding format)
TR	Technical Report
TS	Technical Specification
WG	Working Group
XML	Extensible Markup Language
XSD	XML Schema Definition

5 Relationships between biometrics and ICCs

5.1 Architectures for the joint use of biometrics and ICCs

ISO/IEC 24787 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 document. When integrating biometrics into ICCs, four different approaches can be followed:

— Off-card biometric comparison (see ISO/IEC 24787): The ICC stores the biometric reference but is not directly involved in comparison processing. The IFD application reads the biometric reference from the ICC, as needed, with biometric verification occurring external to the ICC.

— On-card biometric comparison (see ISO/IEC 24787): The ICC both stores the biometric reference, and performs biometric comparison against biometric problems supplied by the IFD. Security controls employed by the ICC for this process include:

  — Use of cryptography or other controls to prevent unauthorised access to the biometric reference and associated processes; and

  — Limiting the number of consecutive unsuccessful comparisons and blocking further comparison attempts once a specified threshold has been reached.

— Work-sharing on-card biometric comparison (see ISO/IEC 24787): An implementation in which comparison processing, and potentially sample pre-processing, is shared between ICC and external system components.

— Biometric system-on-card (see ISO/IEC 24787 and ISO/IEC 17839 all parts): The ICC contains a complete reference storage, biometric sample capture and biometric comparison subsystem. Such implementations are limited to modalities using small sensors and constrained processing capabilities.

5.2 Considerations to be addressed when designing the application

With these four architectures in mind, the designer and/or developer has to take several decisions to define the whole system and the relationship between biometrics and ICCs. The following considerations have to be taken into account. They are outlined in the following paragraphs and discussed further in subsequent clauses in this document.

a) Is the system going to be implementing a verification 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 for a further relationship between biometrics and ICCs, and in such case this document 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 verification attempt, then the need for a further relationship between biometric information and ICC is not needed. Therefore, this document is not applicable. The ICC will act only as a means 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 can already be taken, such as the possibility of using on-card biometric comparison, work-sharing on-card comparison or biometric 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 6).

4) Once the modality is chosen, it can also be important to address whether the ICC is expected to also support other biometric verification types on ICC (e.g. off-card comparison) for the same modality.

NOTE NIST SP 800-76-2 (see 5.4 Finger selection for details) specification for PIV card (further also referenced within Clause 9 of this document) describes ICC platform with optional fingerprint on-card comparison and mandatory storage of the off-card comparison dedicated fingerprint templates. It also addresses the subject stated above, that using the same reference finger positions for both enrolled for off-card comparison and enrolled for on-card comparison biometric data can lead to security vulnerabilities, if off-card templates would be read-out by an inappropriate party. Therefore, it recommends using different positions for off-card and on-card comparison reference templates. However, it also does not prohibit using the same positions because of usability (the same two positions have to be presented by the cardholder despite the off-card or on-card verification method utilized).

5) In practice, multiple modalities can be used to address a higher level of security, flexibility and also interoperability, i.e. face + fingerprints, where the latter enables interoperability at compact format feature (minutiae) set level if face proprietary feature set encoding is used.

6) Although theoretically possible, the use of multiple biometrics in on-card biometric comparison or in BSoC can raise usability issues. Not only can an excessive interaction be requested, but also delays in decision taking can appear due to the increase in computational needs.

7) In either case, data quality control has to be considered for both the biometric reference and the biometric probe, prior to applying any biometric operation.

d) What are the initial requirements of ICC's resources?

1) If there is the requirement of using an ICC with insufficient processing capability, then alternatives such as off-card comparison or work-sharing on-card comparison can be compromised.

2) If there is the requirement of using an ICC with limited storage capacity, then the number of references to be stored on the ICC, or the modalities to be used can be limited and/or the use of compact data formats can become a major requirement (see Clause 6). Attention is drawn to the face that the limitations imposed by compact data formats also have to be considered (e.g.

ISO/IEC 19794-2 compact card format maximum value for the minutiae x and y coordinate is 25,5 mm).

e) Steps to be followed to reach interoperability:

1) If there is no need, then the designer can decide to create his/her own solution without following any standard. Therefore, this document cannot be applicable. This option is not recommended as the need for interoperability can 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 6. As it will be seen, it can happen that for reaching global interoperability in a specific modality, being independent on the algorithm to be used, the use of captured sample data in standardized format can become the only viable solution (e.g. the face image coded as ISO/IEC 19794-5, instead of a proprietary feature-based information).

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 7 and 8.

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

5) In the use of biometrics, the quality of the data used plays a major role in the performance and usability of the system. Data quality has to be analysed, so as to allow the system to reject the input if a minimum quality threshold is not achieved. This is not only important for the biometric probe, but even more important for the biometric reference. If the reference presents low quality, then the performance of the rest of the verifications is compromised. Therefore, the system designer has to be aware if there are some quality specifications for the application, or if not, to define those for both enrolment and verification. Data quality thresholds can be more restrictive for enrolment than for verification, to ensure a proper operation in the daily use of the system. There are standards devoted to the definition of quality metrics for several biometric modalities, such as the ISO/IEC 29794 series. Additionally, for the case of on-card biometric comparison, there are also definitions in ISO/IEC 24787:2018 regarding Minimal Verification Quality DOs inside Biometric Comparison Parameters DO, as well as considerations on the minimal reference / verification data quality to be addressed for the on-card comparison engine on the ICC for enrolment or verification respectively.

6) When ICCs are in use, it is important to use interindustry APDU command exchange, as to allow a good level of interoperability. The ISO/IEC 7816 series (in particular Part 4) describes those interindustry APDUs. Also, for some applications, there is even a workflow recommended which has to be followed, such as the one described in ISO/IEC 24787 for on-card biometric comparison. For example, when designing an application using on-card biometric comparison, the interindustry APDU commands described in ISO/IEC 7816-4, ISO/IEC 7816-11, and ISO/IEC 24787, are to be used for reaching interoperable on-card comparison implementations.

f) In many parts of the world, biometric data are considered 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 7 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 scenario, standardized APIs are to be used to ease integration. Clause 8 provides further details.

h) For certain applications there is the need of following already defined specifications. Clause 9 describes the current available specifications.

i) 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, an evaluation methodology is required. Clause 10 describes the evaluation-related standards related to ICC, biometrics and security.

In addition to the above information, Clause 11 provides examples that could serve as guidance for implementing ICC-based biometric solutions, based, or not, on ISO/IEC 24787.

6 Data formats

6.1 General

As long as data for exchanging are encapsulated in an ICC according to the ISO/IEC 7816 series, either the biometric information template DO’7F60’ or the biometric information group template DO’7F61’ defined in ISO/IEC 7816-11 are considered.

As biometric data can contain information on one or more modalities, several options have to be considered. The following sub-clauses detail those options, from the mono-modality version, to the specific definitions already written for ICC-based applications.

6.2 Single modality plain biometric data formats

ISO/IEC JTC1 SC37 is in charge of developing standards that provide interoperable ways to code biometric data, depending on the modality. Since its funding, three generations of the biometric data formats have been generated. The two first generations have been published within the ISO/IEC 19794 series, while the third one is being published in the ISO/IEC 39794 series.

It is important to note that the differences introduced in each generation, has made them not fully compatible. The first generation was published in 2005-2007, while the second one was published from 2011 and beyond. The typical process for ISO/IEC international standards is that, when a new edition is published (i.e. a new generation), the previous one is considered deprecated. But for certain parts of ISO/IEC 19794, the first edition (i.e. first generation) has been retained as published, as it is currently used by some world-wide applications, such as the ePassport. In order to try to avoid further deprecations, the third generation has been published under a new standard number, i.e. ISO/IEC 39794 series.

The structure of both the ISO/IEC 19794 series and the ISO/IEC 39794 series is the following:

— Part 1 provides a general framework to be applied to all the other parts. It defines the general structure for the biometric data records and the common elements of such structure. It explains that each biometric data information record (BDIR) is to be composed of a general header that introduces the information to be followed, and one or more representations (i.e. biometric samples from the same user and the same modality), are structured into a representation header and the representation data. Part 1 defines those common elements of each of the headers. In a more generic way, Part 1 specifies the following:

  — general aspects for the usage of biometric data records;

  — the processing levels and types of biometric data structures;

  — a naming convention for biometric data structures;

  — coding scheme for format types.

— Part 2 and successive parts 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. Table 1 shows the relationships between each part and each generation.

