TECHNICAL REPORT

ISO/IEC TR 30117

Second edition
2021-08

Information technology — Standards and applications for the integration of biometrics and integrated circuit cards (ICCs)

Technologies de l'information — Normes et applications pour l'intégration des données biométriques et cartes à circuits intégrés

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

COPYRIGHT PROTECTED DOCUMENT

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 information on the published documents and relates 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.

This document provides information on the published documents and relates them to the kind of application to be developed.

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 — Standards and applications for the integration of biometrics and integrated circuit cards (ICCs)

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 integrated circuit cards (ICCs). It also provides examples of how biometrics and ICCs are integrated 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 ~~https://www.electropedia .org/~~

NOTE ISO/IEC 2382-37 is freely available at ~~https://standards .iso .org/ittf/ PubliclyAvailable Standards/ 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
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 the ISO/IEC 17839 series) 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 takes several decisions in order 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 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.

Table 1 — Biometric modality standardized data formats (publication year)

Part number	Title	1st Generation (ISO/IEC 19794 ed1)	2nd Generation (ISO/IEC 19794 ed2)	3rd Generation (ISO/IEC 39794)
2	Finger minutiae data	2005	2011	Planned 2022
3	Finger pattern spectral data	2006	-	-
4	Finger image data	2005	2011	2019
5	Face image data	2005	2011	2019
6	Iris image data	2005	2011	2021
7	Handwritten signature/sign time series data	2007	2014	
8	Finger pattern skeletal data	2006	2011	
9	Vascular image data	2007	2011	2021
10	Hand geometry silhouette data	2007	-	-
11	Handwritten signature processed dynamic data	-	2013	
12	Face identity data	-	-	-
13	Voice data	-	2018	
14	DNA data	-	2013	
15	Palm crease image data	-	2017	
16	Full body image data	-	-	2021
17	Gait image sequence data	-	-	2021

For some of these modalities, more than one biometric data interchange format is defined. The main differences between these biometric data for one modality are the amount of data and computational effort. For ICC's limited resources, i.e. size of storage and computational power, consideration of selecting biometric data and its format are required.

The differences between the ISO/IEC 19794 (and ISO/IEC 39794) generations mainly relate to two aspects:

— Elements to be included and whether they are mandatory or optional. In between generations, the need of adding/removing fields (typically adding), and making them either mandatory or optional was detected. Sometimes the decision on making a field mandatory changed several times between generations (e.g. some fields can be mandatory in the 2nd generation and then changed to optional in the 3rd generation).

— How the information is coded into the BDIR:

  — 1st generation: The coding was made purely binary, with no tags indicating which field is being coded. Therefore, the order and length of fields was fixed, with no possible dynamic change. This way of coding required adding some length fields and, in some cases, fields indicating the presence or absence of further optional fields. Compact card formats are defined in ISO/IEC 19794-2 and ISO/IEC 19794-7.

  — 2nd generation: Two different kinds of coding are considered in this generation. The first one is a binary one, similar to the one defined in the 1st generation. Unfortunately, as new fields were included, and also some others changed their specification (including length), this binary coding is incompatible with the one of the 1st generation. The second coding defined is an XML coding, where all specified fields are defined within an XML schema. XML formats are unlikely to be utilized within on-card comparison or other ICC-related systems due to common restrictions on memory consumption within such ICCs.

  — 3rd generation (specified in ISO/IEC 39794 instead of a new edition of ISO/IEC 19794): Noting the lack of compatibility between the 1st and the 2nd generation, this 3rd generation has been

defined to allow future backward compatibility. This is the reason for calling this series of standards "Extensible biometric data interchange formats". The formats are specified using ASN.1, allowing implementations in TLV, and using XSDs.

6.3 Encapsulation of multiple modalities and/or security mechanisms

In addition to the data formats defined in ISO/IEC 19794 and ISO/IEC 39794 which are defined as to include the information from a single user and a single modality, ISO/IEC JTC1 SC37 has also defined a meta-structure called CBEFF (i.e. the ISO/IEC 19785 series of standards), that allows:

— the coding of biometric information from more than a single user;

NOTE 1 When multiple CBEFF BIR structures for multiple users are supported, new functions for an ICC have to be required.

— the coding of biometric information from more than one modality; and

NOTE 2 When multiple CBEFF BIR structures are supported, new functions for an ICC have to be required.

— protecting biometric data by using security mechanisms that can cipher and/or authenticate the data included in the CBEFF BIR structure.

A CBEFF BIR is composed of a

— standard biometric header in a particular patron format (as defined in ISO/IEC 19785-1 and being the patron formats defined in ISO/IEC 19785-3). This header introduces the information embedded into the BIR;

— the biometric data block (BDB), which can be a BDIR defined in ISO/IEC 19794 or ISO/IEC 39794; and

— an optional security block (as defined in ISO/IEC 19785-1 and ISO/IEC 19785-4) that embeds the data needed for protecting the biometric information.

CBEFF also allows multiple BDB, such as a multiple CBEFF BIR structure and complex CBEFF BIR structure. The former can contain multiple BIRs and the latter can contain multiple BDBs, each having its own standard biometric header plus additional standard biometric headers that express the relations among the BDBs.

The way that CBEFF records can be coded can change from one architecture to another. This is why ISO/IEC 19785-3 defines several ways to code CBEFF records in what is called a patron format. There are patron formats defined for binary coding, with different system word lengths, others for XML coding, etc. Most of them are defined using ASN.1 formal language.

ISO/IEC 19785-3 defines two CBEFF TLV-encoded patron formats for use with ICCs or other tokens (with either biometric off-card or biometric on-card comparison), which use different tag allocation authority encoding approaches within Biometric Information Template data element.

— The first is ISO/IEC 19785-3:2020, Clause 11 "TLV-encoded patron format, for use with smartcards or other tokens (with implicit tag allocation authority)" available since the first CBEFF edition of the ISO/IEC 19785-3 edition dated in 2007. It is a legacy format, as it restricts the independent tag assignment by different ISO/IEC JTC1 SC37 and SC17 tag allocation authorities. It is used for backwards compatibility with deployed and currently widely used off-card comparison (e.g. ePassport) and old on-card comparison biometric solutions. This legacy CBEFF TLV-encoded patron format does not utilize either card level (configuration data) or application level (biometric algorithm parameters) optional on-card comparison data elements from ISO/IEC 24787. The format uses ISO/IEC 19794 series modality-specific biometric algorithm parameters optional data elements instead. The format itself is referenced by the preceding first editions of the ISO/IEC 7816-11 and ISO/IEC 24787 on-card comparison dedicated standards.

— The second is ISO/IEC 19785-3:2020, Clause 19 "TLV-encoded patron format for ICCs and other tokens (with explicit tag allocation authority)" introduced since the third CBEFF edition of ISO/IEC 19785-3:2020 to resolve the preceding format restrictions. It is recommended to be used in all future biometric on-card or off-card comparison solutions. This state of art TLV-encoded patron format incorporates the current and possible future ISO/IEC 24787 on-card comparison enabled card level (e.g. biometric functionality information) and application level (e.g. biometric comparison parameters) optional data elements. It is also referenced by the most recent ISO/IEC 7816-11 and ISO/IEC 24787 on-card comparison dedicated standards.

6.4 ICC-specific definitions on biometric data formats

ISO/IEC 7816-11 defines PERFORM BIOMETRIC OPERATION (PBO) command and supplemental specification of VERIFY command for biometric operation. The instruction byte (INS) of PBO command and the specification of VERIFY command are defined in ISO/IEC 7816-4. ISO/IEC 7816-11 also defines biometric information template for encapsulating CBEFF BIR. It includes the use of ICCs either in on-card biometric comparison, as well as store-on-card solutions. It specifies a Biometric Information Template through the use of standard TLV-encoded data elements.

As mentioned above, ISO/IEC 7816-11 specifies two different ways of representing that data. The first one, defined from the 1st edition of the standard and kept for legacy reasons, is devoted to those cases where the tags used are allocated implicitly. The second one is by explicitly indicating the tag allocation authority used, which is to be used for all new developments. Both of them are specified in conformance with ISO/IEC 19785-3:2020, Clause 11 for the implicit case, while Clause 19 is to be used for the explicit tag allocation authority.

On the other hand, ISO/IEC 24787 introduces one off-card biometric comparison architecture and three on-card biometric comparison architectures. It defines framework for on-card biometric comparison, e.g. biometric data, enrolment and comparison. It also defines security policies for on-card biometric comparison. ISO/IEC 24787 enhances the specifications in ISO/IEC 7816-11, by providing requirements for the biometric comparison while using a compliant on-card biometric verification. The system has to encode public biometric information and private biometric data in an ISO/IEC 19785-3 and ISO/IEC 7816-11 (also optionally ISO/IEC 19794 or the ISO/IEC 39794 series) standards compatible manner. That biometric data is managed between IFD and ICC, and also internally within ICC (e.g. verification retry counters) in an ISO/IEC 7816-11 and ISO/IEC 7816-4 compatible manner. ISO/IEC 24787 also defines additional data elements for encoding of the on-card comparison enabled card level (biometric functionality) information or application level (biometric comparison parameters) information for appropriate security policies.

7 Privacy and security

Biometric data are considered in many scenarios as personal data, and protection of such data is required. As already mentioned, CBEFF (i.e. ISO/IEC 19785-1) defines a security block. Such a security block is intended to hold information for protecting the biometric data, e.g. cryptographic checksum which provides integrity (authenticity). Furthermore, ISO/IEC 19785-4 specifies the format for the security block. But in order to reach interoperability the international standards and reports developed by ISO/IEC JTC1 SC27 have to be considered. ISO/IEC JTC1 SC27 encompasses security and privacy in all information technology fields. Within its standards portfolio, the main ones related to biometrics are:

— Dealing with application design and security and privacy scenarios the following standards are initiated, which will be further referenced in ~~Clause 9~~:

  — ISO/IEC 29100 on the privacy architecture framework;

  — ISO/IEC 29101 on the privacy reference architecture;

  — ISO/IEC 29146 on framework for access management;

  — ISO/IEC 24760 on framework for identity management;

- ISO/IEC 29115 on entity authentication assurance framework;
- ISO/IEC 29191 on requirements for partially anonymous, partially unlinkable authentication;
- ISO/IEC 29190 on privacy capability assessment model;

— ISO/IEC 19792 on security evaluation of biometrics, which is also mentioned later in ~~Clause 10~~. —

ISO/IEC 24761 on authentication context for biometrics (ACBio). It specifies the way that security mechanisms are to be used, and how information is to be coded into the security block (as defined in ISO/IEC 19785-1).

— ISO/IEC 24745 on biometric information protection, which specifies the way biometric information can be used to achieve cancellable biometric references, i.e. what is also known in the industry as "biometric template protection".

— ISO/IEC 20889 on privacy enhancing data de-identification techniques.

— ISO/IEC 19989 series on criteria and methodology for security evaluation of biometric systems. This series has the following parts:

- Part 1 specifying the framework.
- Part 2 specifying the performance in biometric recognition.
- Part 3 specifying the presentation attack detection (PAD).

— ISO/IEC 27553-1[1] on the security requirements for authentication using biometrics on mobile devices.

In addition to CBEFF, ISO/IEC JTC1 SC37 has developed several standards related to security in biometrics. The first one is a Technical Report (ISO/IEC TR 29156) on performance requirements to meet security and usability needs in applications using biometrics. Also, API-related standards, such as Object Oriented BioAPI (ISO/IEC 30106 series) also provides requirements for securing biometric data.

But one of the most important series of standards related to security (from the point of view of ISO/IEC JTC1 SC37), is the ISO/IEC 30107 series on biometric presentation attack detection (PAD), which has been used by ISO/IEC JTC1 SC27 as a basis for the definition of ISO/IEC 19989-3. This series, currently composed of four parts, provides specifications on how to detect those attacks at the presentation level (e.g., spoofing samples or obfuscating attempts).

— Part 1 gives the framework, with the general definitions on the topic.

— Part 2 defines an interchangeable data format for enclosing PAD-related data, in case the PAD decision has to be shared in between systems.

— Part 3 provides the methodology to evaluate PAD capabilities of a biometric system.

— Part 4 refines such methodology to be applied to mobile systems.

For an ICC, ISO/IEC JTC1 SC17 provides ISO/IEC 7816-4 specifying security architecture mainly for protecting data in an ICC, secure messaging for protecting command/response and basic security handling commands. It also provides ISO/IEC 7816-8 specifying commands and mechanisms for security operations. ISO/IEC 24787 defines security policies for global biometric comparison parameters, and application-specific biometric comparison parameters.

The methods outlined in this clause can be implemented in a variety of ways. It is out of the scope of this document to define those implementations. Such implementations are to be defined at specific profiles related to the final application targeted.

---

1) Under preparation. Stage at the time of publication: ISO/IEC CD 27553-1.2.

The developer of an on-card biometric comparison related application can be interested in considering other security related standards, such as the ones developed by ISO/IEC JTC1 SC27.

8 Outside-ICC application development

8.1 General overview

Developing an application involving ICCs and biometrics, usually needs the integration of several modules. In order to ease that integration, the use of standardized Application Program Interfaces (APIs) is recommended. The API is different depending on whether the application is expected to be executed locally in a computer, or if the solution is to be implemented using a client-server architecture, where not only local applications are involved, but also commands and data exchange through a communication channel.

8.2 Local applications

Biometric applications and modules can be developed using BioAPI, which is specified in the ISO/IEC 19784 series, where ISO/IEC 19784-1 is the main definition of the API. BioAPI in its initial definition is based on a framework that interconnects the different modules, which are developed as Biometric Service Providers (BSPs), which can be composed of units (algorithms, sensor or archive units), and/or Biometric Function Providers (BFPs) that group units. In a simplified way of understanding BioAPI, BSPs are like drivers in an operating system, while the Framework is the operating system. The application is programmed considering only the operating system (i.e. the Framework), so the system can change the particular drivers used (i.e. the BSPs) without having to change the application.

Within ISO/IEC 19784-1 there is also the possibility of implementing a framework free version of BioAPI, as to allow its deployment in devices with an operating system but limited processing capabilities. Furthermore, when the application is intended to be developed under low cost, low performance devices, such as embedded systems, a simplified version of BioAPI is defined in ISO/IEC 29164, called Embedded BioAPI.

BioAPI is specified in C language, which causes it to lack an object-oriented approach to its implementation. In order to overcome this inconvenience, the ISO/IEC 30106 series provides a specification of an object-oriented version of BioAPI (also referred as OO BioAPI) that is composed of a general framework with a Unified Modelling Language (UML) description (ISO/IEC 30106-1), a Java language reference implementation (ISO/IEC 30106-2), a C# language reference implementation (ISO/IEC 30106-3) and a C++ implementation (ISO/IEC 30106-4). OO BioAPI is not a direct translation of ISO/IEC 19784, but an adaptation which adjusts BioAPI to the new needs of application development, as well as the new capabilities of the hardware involved.

When considering ICCs, within a BioAPI structured product, an on-card biometric comparison ICC will be another biometric service provided to the system, i.e. it is a BSP. In this case, the BSP is providing two main functionalities: storage and comparison, although from the storage functionality, only storage is provided and no reading of the information is allowed. In those cases when an off-card biometric comparison ICC is used, then the ICC will be provided as another BSP, but in such case the BSP is only providing support for storage (and reading) capabilities.

8.3 Client-server implementations

In some other cases, local applications are needed as well as remote connections between devices. Typical implementations use client-server architectures, and ISO/IEC JTC1 SC37 decided to define a standard to allow an interoperable way of implementing this kind of solution, using BioAPI, ISO/IEC 24708.

Client-server technologies have evolved hugely making BIP outdated. Nowadays it is more frequent to talk about web-service based solutions, and in order to address this need BIAS (Biometric Identity Assurance Services) was originally created by OASIS, becoming ISO/IEC 30108-1. This first part of BIAS was developed as an XML-based specification for allowing the exchange of identity information

(including also non-biometric data) in Service Oriented Architectures (SOAs). It was intentionally created as implementation independent, although it is close to Simple Object Access Protocol (SOAP), the Microsoft approach to web services.

But recently, many applications prefer to use REST (Representational State Transfer), due to being simpler and lighter. Therefore, ISO/IEC JTC1 SC37 decided to develop ISO/IEC 30108-2 for the specification of BIAS in accordance to a REST-based implementation.

9 Use cases profiles

There are several standards and technical reports published, that are a reference for a system designer and/or developer, when defining certain applications:

— Standards in relation to biometric application profiles developed by ISO/IEC JTC 1 SC 37:

  — ISO/IEC TR 20027, *Biometric interoperability profiles — Best practices for slap tenprint fingerprint capture*

  — ISO/IEC TR 30125, *Biometrics used with mobile devices*

  — ISO/IEC TR 29195, *Traveller processes for biometric recognition in automated border control systems*

  — ISO/IEC TR 29196, *Guidance for biometric enrolment*

  — ISO/IEC 24713-1, *Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles*

  — ISO/IEC 24713-2, *Biometric profiles for interoperability and data interchange — Part 2: Physical access control for employees at airports*

  — ISO/IEC 24713-3, *Biometric profiles for interoperability and data interchange — Part 3: Biometric based verification and identification of seafarers*

— Standards in relation to jurisdictional and social issues around the use of biometrics developed by ISO/IEC JTC 1/SC 37:

  — ISO/IEC 24779 series, *Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems*

    which specifies a family of icons and symbols used in association with devices for biometric enrolment, verification and/or identification. The series includes four parts:

    — Part 1: *General principles*

    — Part 4: *Fingerprint applications*

    — Part 5: *Face applications*

    — Part 9: *Vascular applications*

  — ISO/IEC TR 20322[2] , *Information technology — Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and elderly people*

  — ISO/IEC TR 21419[3] , *Information technology — Cross jurisdictional and societal aspects of implementation of biometric technologies — Use of biometrics for identity management in healthcare*

2) Under preparation. Stage at the time of publication: ISO/IEC CD TR 20322.3.

3) Under preparation. Stage at the time of publication: ISO/IEC WD TR 21419.

— ISO/IEC TR 24714-1, *Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance*

— Standards in relation to a correct application of ICCs and/or biometrics:

— FIDO Alliance, defining a simpler, stronger authentication, in particular with its application to mobile devices. Their documents can be found at: ~~https://fidoalliance .org/~~

— CEN/CENELEC TC224 based on user interface for identification focuses on two projects: —

The EN 1332 series (four parts), *Identification card systems — Human-machine interface* —

CEN/TS 15291, *Identification card system — Guidance on design for accessible card-activated devices*

In the case of off-card biometric comparison, there are some widely deployed applications with standardized specifications, such as:

— Machine Readable Travel Documents (MRTD), with the particular case of ePassports. You can find the definitions in:

— ICAO 9303 multipart specification, available at ~~https://www.icao .int/publications/pages/publication .aspx?docnum= 9303~~

— The ISO/IEC 18745 series, developed by ISO/IEC JTC1/SC 17, which is closely related to the ICAO 9303 documents,

— The ISO/IEC 18013 driving licence series developed by ISO/IEC JTC1/SC17.

When considering the technology of on-card biometric comparison, there are some multi-national, national or even sector-restricted specifications that refer to this technology. Some examples of this kind of specification:

— European Citizen Card (CEN/TS 15480), developed by CEN TC224, specifies the requirements for a citizen card, that includes not only the physical identity verification, but also the electronic identity of the citizen. Within its specifications it allows the implementation of the citizen card using on-card biometric comparison products. This specification has already been followed by several countries in Europe to issue their national ID cards, and some of them (e.g. Spain) have included on-card biometric comparison.

— Federal Information Processing Standards (FIPS) 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, provides requirements for a government-wide interoperable identity credential for issuance and use by United States (US) Federal Government employees and contractors. This US standard defines on-card biometric comparison as an optional mechanism for card activation and user verification. Agencies that implement this option enable cardholders to present their biometrics to activate the PIV Card instead of using the PIN. Moreover, the use of the on-card biometric comparison as a verification mechanism (named OCC_AUTH), which enables relying systems to achieve a high assurance level multi-factor user verification.

10 Technology evaluation

In addition to the above documents, it is important to know which standards and reports have been developed to test the technology involving ICCs and biometrics. Starting with the ICC-based test methods, the ISO/IEC 10373 series defines the test methods for all technological specifications of identification cards, including ICCs with contact and contactless ICCs. For on-card biometric comparison products (i.e. those based on ISO/IEC 24787), ISO/IEC 18584 allows testing the conformance with the base standard.

Within ISO/IEC JTC1 SC37 a working group is dedicated to developing standards in the evaluation of biometrics including of significant importance the ISO/IEC 19795 series, which defines the principles for the evaluation of biometrics, as well as some specific application of those principles to certain scenarios.

One of those scenarios is the on-card biometric comparison. In ISO/IEC 19795-7, a methodology is provided for evaluating how a biometric solution behaves differently when it is implemented inside a card, or when it is implemented in a conventional computer. This standard was developed as a result of the MINEX II evaluation that NIST initiated to evaluate the level of performance of the on-card biometric comparison, with the idea of deciding if such a technology was suitable for being implemented into an on-card biometric comparison-based solution. It is important to highlight that ISO/IEC 19795-7 does not evaluate the algorithm performance. ISO/IEC 19795-7 evaluations aim to confirm that the accuracy of the algorithm executed inside the ICC is the same as the accuracy of such algorithm being executed in a computer. In addition to such evaluation, a technology evaluation on the algorithm in a computer can be performed (following ISO/IEC 19795-1 and ISO/IEC 19795-2). It is also important to note that in order to ease the evaluation process, the cards will have to provide information about the comparison result, which is usually not available in commercial products to avoid hill-climbing attacks.

Other biometric performance evaluation standards have been developed by ISO/IEC JTC 1 SC37:

— ISO/IEC 21472[4] : *Evaluation methodology for user interaction influence in biometric system performance*

— ISO/IEC 29197: *Evaluation methodology for environmental influence in biometric system performance*

— ISO/IEC 30136: *Performance testing of biometric template protection schemes*

When evaluating either the performance or the PAD in BSoC products, there are no standards or technical reports currently published. Until this kind of document is published, it is recommended to study the current specifications for evaluating biometrics in mobile devices. Therefore, documents that can be referenced are ISO/IEC TS 19795-9 for functional evaluation and ISO/IEC 30107-4 for PAD.

In order to evaluate the security level achieved with the developed solution, Common Criteria is the major reference. The works in Common Criteria are subsequently standardized under the ISO/IEC 15408 series. In relation to biometrics, ISO/IEC JTC 1 SC27 has developed ISO/IEC 19792 that specifies a methodology for evaluating security in biometric systems. Within the Common Criteria Portal (~~http://www. commoncrit eriaportal .org/~~) there are some Protection Profiles (PPs) and Security Targets (STs) that are applicable to on-card biometric comparison products, and in the future, some PPs and/or STs can appear specifically to this technology.

11 Implementing solutions merging the use of ICCs and biometrics

11.1 Spanish national ID card (DNIe)

11.1.1 General

Spain has a long tradition of using national ID cards, dating from the first half of the 20th century. The card (also known as DNI "Documento Nacional de Identidad"), used to be a laminated paper-based document with physical security mechanisms. The card can be used at any time for proving the cardholder identity, and it is even accepted as a travel document within the Schengen area.

From that basis, the Spanish government decided to improve the document adding electronic ID capabilities through the incorporation of PKI-based key pairs within the document. Therefore, it was decided to change the technology to an ICC-based document, with both electronic and physical protections, as to allow both the face-to-face identification of the cardholder, and the electronic authentication and signature mechanisms for remote identification.

When defining the new generation of the Spanish national ID card (also known as DNIe for the electronic version of the traditional DNI), it was decided to add on-card biometric comparison capabilities to the card.

4) Under preparation. Stage at the time of publication: ISO/IEC PRF 21472.

Later, compatibility with ICAO 9303 (i.e. ePassport) was added. Technically that meant the addition of a dual interface to the ICC (both contact and contactless), as well as adding the internal data structure to fit the specification of the LDS within ICAO 9303-10.

In the following subsections the details of such implementation are provided.

11.1.2 Biometric services provided

The on-card biometric comparison supplements the secure access to certain resources embedded in the ICC of the DNIe. These resources are:

— Electronic signature keys;

— Authentication keys;

— Electronic signature certificate;

— Authentication certificate;

— Certificates for the intermediate Certification Authority (CA);

— Cardholder's affiliation data;

— Cardholder's handwritten signature image;

— Cardholder's facial image;

— Non-readable cardholder's fingerprint minutiae.

Due to the access conditions defined, the on-card biometric comparison mechanism is currently only available for citizens at police stations to perform the following operations:

— Identity verification;

— Unblocking PIN code;

— Change of PIN code.

In addition to those services, the inclusion of the ICAO 9303-10 compatibility added the following services:

— Basic Access Control (BAC) scheme to allow contactless access to personal data;

— Storage of the cardholder's facial photograph, for off-card biometric comparison.

11.1.3 Biometric modalities and data formats

The biometric modality chosen for the on-card biometric comparison in the DNIe is a fingerprint. The DNIe is capable of verifying the identity by using any of the two index fingers of the cardholder. Therefore, the following specifications were implemented for the system:

— During enrolment, rolled fingerprints of both index fingers are taken, accepting them after a quality threshold has been successfully passed.

— At the verification stage, the cardholder inserts the card and when prompted by the application, places the requested index finger on a plain fingerprint sensor. The minutiae are extracted, coded following ISO/IEC 19794-2 on-card comparison (compact) card format, and sent to the ICC in a secure way. Then the ICC compares those minutiae with the ones stored at the ICC, and a decision is taken. If the comparison is successful, an OK feedback is provided. If not, a NO-OK feedback is given. No further information is provided from the comparison in order to avoid hill climbing attacks.

For the off-card biometric comparison, both facial and static handwritten signature were chosen. In the case of static handwritten signature, a plain image file has been used, as there was no international

standard defined for this biometric modality. In the case of facial image, ISO/IEC 19794-5 first generation was chosen. This also allowed full compatibility with ICAO 9303-10.

11.1.4 Security mechanisms and operations

In order to use the on-card biometric identity verification mechanism, the access conditions are based in a previous establishment of a Secure Administrative Channel. This is due to the fact that the Certification Bodies currently do not accept fingerprint biometrics as a strong authentication mechanism. Using strong security mechanisms is a requirement for obtaining an EAL4+ certification under Common Criteria. At the same time, that is also a requirement for the DNIe, as it has to be considered as a Secure Signature Creation Device, under the European legislation.

Therefore, the solution was to protect the use of the on-card biometric comparison mechanism, by using previously a verification of other key(s), for which the validation algorithm can be considered as strong.

Several operations within the card are involved within the biometric verification:

— RSA Key renewal: biometrics + PIN + Secure Administrative Channel;

— Certificate renewal: biometrics + PIN + Secure Administrative Channel;

— Unblocking the PIN code: there is no PIN unblocking key (PUK) mechanism, but the unblocking is performed by the combination of:

  — biometrics,

  — Secure Administrative Channel, and

  — a diversified administrative application key that ensures that the whole process is performed within a controlled and secure environment defined by the Spanish Police.

— Change of the PIN code: if the PIN is not blocked, it can be changed by any of the following access conditions combinations:

  — current PIN code + Secure Administrative Channel, or

  — biometrics + Secure Administrative Channel + diversified administrative application key. The

on-card biometric comparison is performed using the VERIFY command, as specified in ISO/IEC 7816-11 and using the on-card comparison (compact) format from ISO/IEC 19794-2.

For the off-card biometric comparison, the security mechanism is based on the BAC defined by the ICAO 9303 series, which can be considered equivalent to the need to present a secret code, before reading the file content containing the face image.

11.1.5 Evaluations and results

The Spanish DNIe obtained the Common Criteria EAL4+ certification.

11.2 ePassport

11.2.1 General

ICAO started to work on machine readable travel documents in 1968. In 1984, ICAO established the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), also known today as the Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP). Later, in 1998, the New Technologies Working Group (NTWG) of the TAG/MRTD began to work on establishing the most effective biometric identification system and associated means of data storage for use in MRTD applications, particularly in relation to document issuance and immigration considerations. But the events on September 11, 2001 boosted the finalization of these works and a few years later, a new generation of passports started to be issued. That new passport contained, among many other new

features, the possibility of contactless electronic access, the inclusion of ICC technology, and the use of biometric technologies.

This technology is specified within the multiple parts of the ICAO 9303 series. The ICAO 9303 series contains 12 parts:

— Part 1: Introduction

— Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs

— Part 3: Specifications Common to all MRTDs (Amendment for New Part B in Page 28 and Part D in page 29)

— Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs

— Part 5: Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs)

— Part 6: Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)

— Part 7: Machine Readable Visas

— Part 8: Emergency Travel Documents

— Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs

— Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)

— Part 11: Security Mechanisms for MRTDs

— Part 12: Public Key Infrastructure for MRTDs

The ICAO 9303 series defines three different types of documents, referred to as TD1, TD2 and TD3, where TD3 is the typical passport booklet, while the other sizes are reserved for other official travel documents. Today, due to several reasons including world-wide interoperability, passports have to use the booklet form factor. This is why, even though the technology included is based on ICCs, the ID1 card form factor is not used, and a contactless interface is chosen. The implementation of ICAO 9303 as a TD3 document is typically known as "ePassport" or "biometric passport".

In the following subsections, the details of this specification are provided.

11.2.2 Biometric services provided

An ePassport contains only off-card biometric verification. The biometric information is read as the content of a file inside the contactless ICC, and then submitted to the system for a post-processing and biometric comparison. The elements contained are:

— Authentication keys;

— Cardholder's affiliation data;

— Mandatory cardholder's facial image;

— Optional cardholder's fingerprint image;

— Optional cardholder's iris image.

In addition to these elements, ICAO 9303-10 includes the following services:

— Mandatory Basic Access Condition (BAC) scheme to allow contactless access to cardholder's data;

— Optional Extended Access Control (EAC) scheme, which adds the functionality to check not only the authenticity of the ICC, but also the IFD.

11.2.3 Biometric modality and data formats

As already mentioned, the biometric modalities included in ePassports are the following:

— Facial image: this is the mandatory biometric modality. It has been declared as the most interoperable biometric modality, as it can be used world-wide. In particular, the facial image is used instead of any kind of feature set or biometric model, as the image is independent of the biometric recognition algorithm used. The face image data used is based on the 1st generation of ISO/IEC 19794-5 (the 1st edition published in 2005).

— Fingerprint biometrics: this biometric modality is optional (i.e. to be decided by each of the issuing states). There are different ways of storing fingerprint data: image, minutiae and pattern. Each State can decide which data to be stored, but if fingerprint data is chosen, the image (based on ISO/IEC 19794-4:2005) is mandatory, and that information can be extended with any of the other two ways of representing fingerprints.

— Iris biometrics: this biometric modality is also optional (i.e. to be decided by each of the issuing States). If chosen, the storage of the iris image is mandatory to permit global interoperability. The standard defining the data format is ISO/IEC 19794-6:2005, even though this standard does not really represent the image of the iris (in contradiction to the 2nd generation, i.e. the 2nd edition of ISO/IEC 19794-6 (2011). The storage of an associated template is optional at the discretion of the issuing State.

Data is stored in specific EFs and DFs, as stated in ICAO 9303-10, which defines the Logical Data Structure (LDS). In LDS, data is organized in Data Groups (DGs). DG1 encloses the administrative data, also present in the MRZ. The biometric information is stored in three different DGs, being DG2 the one for facial image, DG3 for the optional fingerprint data, and DG4 for the optional iris image. The whole LDS is stored in a DF whose AID is 0x7A0000002471001. Within this application, all the LDS files are defined, and from those, the following are of special relevance:

— EF.DG1, including the MRZ data, with file identifier 0x0101, and short file identifier 01.

— EF.DG2, including the facial image data, with file identifier 0x0102, and short file identifier 02.

— EF.DG3, including fingerprint data, with file identifier 0x0103, and short file identifier 03.

— EF.DG4, including iris data, with file identifier 0x0104, and short file identifier 04.

11.2.4 Security mechanisms and operations

Also, due to the need of world-wide interoperability, and the particular interests of each of the issuing States, the ePassport security mechanisms include a range of complexity levels, from the simplest one (fully interoperable and mandatory for all ePassports), to the very complex ones (optional). ICAO 9303-11 defines these security mechanisms, which can be summarized as follows:

— Baseline security method:

  — Passive Authentication: proves that the contents of the SOD and the LDS are authentic and not changed. But it does not prevent an exact copy or IC substitution, unauthorized access, and skimming. (Mandatory).

— Advanced security methods:

  — Comparison of conventional MRZ(OCR-B) and IC-based MRZ(LDS): proves that contactless IC content and physical eMRTD belong together. It adds (minor) complexity and does not prevent an exact copy of contactless IC and conventional document.

  — Active Authentication and Chip Authentication: prevent copying the SOD and prove that it has been read from the authentic contactless IC. Prove that the contactless IC has not been substituted. Does not prevent unauthorized access. Add complexity. (Both are optional).

— Basic Access Control (BAC) and Password Authenticated Connection Establishment (PACE): prevent skimming and misuse. Prevent eavesdropping on the communications between eMRTD and inspection system (when used to set up encrypted session channel). Do not prevent an exact copy or IC substitution (requires also copying of the conventional document). Add complexity. If PACE is supported by the MRTD and inspection system, PACE is the one to be used. PACE offers better protection against eavesdropping than BAC. (BAC is recommended for the contactless ICC and mandatory for the inspection system; PACE is recommended for both).

  — In summary, BAC is based on calculating a secret code using the data contained in the MRZ and a simple and public algorithm published in ICAO 9303-11. Then this code is verified by the ICC, and if it is correct, access to data is granted. This mechanism allows reading the ICC only if a physical access to the document is granted and the document is opened to get the MRZ data.

— Extended Access Control (EAC): Prevents unauthorized access to additional biometrics. Prevents skimming of additional biometrics. Requires additional key management. Does not prevent an exact copy or IC substitution (requires also copying of the conventional document). Adds complexity. (Optional).

— Data Encryption: Secures additional biometrics. Does not require processor-ICs. Requires complex decryption key management. Does not prevent an exact copy or IC substitution. Adds complexity. (Optional).

Bibliography

[1] ISO/IEC 7816-4, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

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

[3] ISO/IEC 7816-8, *Identification cards — Integrated circuit cards — Part 8: Commands and mechanisms for security operations*

[4] ISO/IEC 7816-9, *Identification cards — Integrated circuit cards — Part 9: Commands for card management*

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

[6] ISO/IEC 10373 (all parts), *Identification cards — Test methods*

[7] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

[8] ISO/IEC 18013 (all parts), *Personal identification — ISO-compliant driving licence*

[9] ISO/IEC 18584, *Information technology — Identification cards — Conformance test requirements for on-card biometric comparison applications*

[10] ISO/IEC 18745 (all parts), *Test methods for machine readable travel documents (MRTD) and associated devices*

[11] ISO/IEC 17839 (all parts), *Information technology — Identification cards — Biometric System-on-Card*

[12] ISO/IEC 19784 (all parts), *Information technology — Biometric application programming interface*

[13] ISO/IEC 19785 (all parts), *Information technology — Common Biometric Exchange Formats Framework*

[14] ISO/IEC 19792, *Information technology — Security techniques — Security evaluation of biometrics*

[15] ISO/IEC 19794 (all parts), *Information technology — Biometric data interchange formats* ISO/IEC

[16] 19795 (all parts), *Information technology — Biometric performance testing and reporting* ISO/IEC

[17] 19795-7, *Information technology — Biometric performance testing and reporting — Part 7: Testing of on-card biometric comparison algorithms*

[18] ISO/IEC 19989 (all parts), *Information security — Criteria and methodology for security evaluation of biometric systems*

[19] ISO/IEC/TR 20027, *Information technology — Guidelines for slap tenprint fingerprint capture*

[20] ISO/IEC/TR 20322, *Information technology — Cross jurisdictional and societal aspects of implementation of biometric technologies — Biometrics and elderly people*[5)]

[21] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*

5) Under preparation. Stage at the time of publication: ISO/IEC CD TR 20322.3.

[22] ISO/IEC/TR 21419, *Information technology — Cross jurisdictional and societal aspects of implementation of biometric technologies — Use of biometrics for identity management in healthcare* [6)]

[23] ISO/IEC 21472, *Information technology — Scenario evaluation methodology for user interaction influence in biometric system performance*[7)]

[24] ISO/IEC 24708, *Information technology — Biometrics — BioAPI Interworking Protocol*

[25] ISO/IEC 24713 (all parts), *Information technology — Biometric profiles for interoperability and data interchange*

[26] ISO/IEC 24714-1, *Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance*

[27] ISO/IEC 24745, *Information technology — Security techniques — Biometric information protection*

[28] ISO/IEC 24760-1, *IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*

[29] ISO/IEC 24761, *Information technology — Security techniques — Authentication context for biometrics*

[30] ISO/IEC 24779 (all parts), *Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems*

[31] ISO/IEC 24787, *Information technology — Identification cards — On-card biometric comparison*

[32] ISO/IEC 27553-1, *Security and Privacy requirements for authentication using biometrics on mobile devices — Part 1: Local modes*[8)]

[33] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[34] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[35] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

[36] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*

[37] ISO/IEC/TR 29156, *Information technology — Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics*

[38] ISO/IEC 29164, *Information technology — Biometrics — Embedded BioAPI*

[39] ISO/IEC 29190, *Information technology — Security techniques — Privacy capability assessment model*

[40] ISO/IEC 29191, *Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication.*

[41] ISO/IEC/TR 29195, *Traveller processes for biometric recognition in automated border control systems*

[42] ISO/IEC/TR 29196, *Information technology — Guidance for biometric enrolment*

6) Under preparation. Stage at the time of publication: ISO/IEC WD TR 21419.

7) Under preparation. Stage at the time of publication: ISO/IEC PRF 21472. 8)

Under preparation. Stage at the time of publication: ISO/IEC CD 27553-1.2.

[43] ISO/IEC 29197, *Information technology — Evaluation methodology for environmental influence in biometric system performance*

[44] ISO/IEC 29794 (all parts), *Information technology — Biometric sample quality*

[45] ISO/IEC 30106 (all parts), *Information technology — Object oriented BioAPI*

[46] ISO/IEC 30107 (all parts), *Information technology — Biometric presentation attack detection*

[47] ISO/IEC 30108 (all parts), *Information technology — Biometric Identity Assurance Services*

[48] ISO/IEC/TR 30125, *Information technology — Biometrics used with mobile devices*

[49] ISO/IEC 30136, *Information technology — Performance testing of biometric template protection schemes*

[50] ISO/IEC 39794 (all parts), *Information technology — Extensible biometric data interchange formats*

[51] EN 1332, *Identification card systems — User interface*

[52] CEN/TS 15291, *Identification card system — Guidance on design for accessible card-activated devices*

[53] CEN/TS 15480, *Identification card systems — European Citizen Card*

[54] NIST SP 800-76-2, *Biometric Specifications for Personal Identity Verification*

[55] NIST FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors (NIST)*

[56] Li S.Z., Encyclopedia of Biometrics. Springer, 2009

[57] ICAO 9303 (all parts), *Machine Readable Travel Documents*[9]

9) Available at ~~https:// www.icao.int/ publications/ pages/ publication .aspx ?docnum =9303~~.

ICS 35.240.15

Price based on 22 pages