INTERNATIONAL STANDARD

ISO/IEC 39794-1

First edition
2019-12

Information technology — Extensible biometric data interchange formats —

Part 1: Framework

Reference number
ISO/IEC 39794-1:2019(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (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 37, *Biometrics*.

A list of all parts in the ISO/IEC 39794 series can be found on the ISO website.

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.

The purchase of this ISO/IEC document carries a copyright licence for the purchaser to use ISO/IEC copyright in the schemas in the annexes to this document for the purpose of developing, implementing, installing and using software based on those schemas, subject to ISO/IEC licensing conditions set out in the schemas.

Introduction

Biometric data interchange formats enable the interoperability of different biometric systems. The first generation of biometric data interchange formats was published between 2005 and 2007 in the first edition of the ISO/IEC 19794 series. From 2011 onwards, the second generation of biometric data interchange formats was published in the second edition of the established parts and the first edition of some new parts of the ISO/IEC 19794 series. In the second generation of biometric data interchange formats, new useful data elements such as those related to biometric sample quality were added, the header data structures were harmonized across all parts of the ISO/IEC 19794 series, and XML encoding was added in addition to the binary encoding.

The second generation of the biometric data interchange formats turned out to be syntactically incompatible with their first generation. The second generation, however, did not cancel and replace the first generation because the first generation has been adopted widely, e.g. for biometric data stored in machine-readable travel documents, which will be in the field for a long time. Therefore, the first editions of the ISO/IEC 19794 series are expected to be retained in the standards catalogue as long as needed alongside their second editions.

In anticipation of the need for additional data elements, and in order to avoid future compatibility issues, the ISO/IEC 39794 series provides standard biometric data interchange formats capable of being extended in a defined way. Extensible specifications in ASN.1 (Abstract Syntax Notation One) and the Distinguished Encoding Rules of ASN.1 form the basis for encoding biometric data in binary tag-length-value formats. XSDs (XML schema definitions) form the basis for encoding biometric data in XML (eXtensible Markup Language).

This document defines what is common for the extensible biometric data interchange formats considered in the specific parts of the ISO/IEC 39794 series, i.e. the common content, meaning and representation of biometric data interchange formats.

The ISO/IEC 39794 series is one of a family of international standards being developed by ISO/IEC JTC 1/SC 37 that supports interoperability and data interchange among biometric applications and systems. This family of standards specifies requirements on a wide variety of biometric recognition applications, whether such applications operate in an open systems environment or consist of a single, closed system. Open systems are built on standards-based, publicly defined data formats, interfaces and protocols to facilitate data interchange and interoperability with other systems, which may include components of different design or manufacture. A closed system can also be built on publicly defined standards, and may include components of different design or manufacture, but inherently has no requirement for data interchange and interoperability with any other system.

The ISO/IEC JTC 1/SC 37 biometric standards family includes a layered set of standards consisting of biometric data interchange formats and biometric interfaces, as well as biometric profiles that describe the use of these standards in specific application areas. Figure 1 shows the interrelation of biometrics-related areas of standardization. Biometric data complying with one of the biometric data interchange formats defined in the ISO/IEC 19794 series[7] and the ISO/IEC 39794 series represent the core component of biometric interoperability. The formats defined in the ISO/IEC 19785 series[4] may be used as a wrapper around biometric data. Since biometric data are sensitive data and subject to attack, cryptographic protection is required in interchange environments. Biometrics-related profiles, security evaluation and performance evaluation also play an important role. Biometric interfaces are essential to facilitate easy integration and usage of biometric components. The harmonized biometric vocabulary is recommended for use in describing biometric technology. The deployment of applications using biometric verification or identification takes place within the context of societal and cross-jurisdictional requirements.

The ISO/IEC 19794 series and the ISO/IEC 39794 series specify biometric data interchange formats for different types of biometric characteristics. Parties that agree on a biometric data interchange format specified in the ISO/IEC 19794 series or the ISO/IEC 39794 series should be able to decode each other's biometric data.

The biometric interface standards include the Common Biometric Exchange Formats Framework (CBEFF) series (ISO/IEC 19785[4]) and the Biometric Application Programming Interface (BioAPI) series (ISO/IEC 19784[3]). These standards support exchange of biometric data within a system or among systems. The CBEFF series specifies the basic structure of a standardized biometric information record (BIR) which includes one or more biometric data blocks (BDB) with added metadata, such as date and time when it was captured, its expiry date, whether it is encrypted, etc. The BioAPI series specifies an open system API that supports communications between software applications and underlying biometric technology services.

The biometric profile series (ISO/IEC 24713[8]) facilitates implementations of the base standards (e.g. biometric data interchange format standards and biometric interface standards and possibly non-biometric standards) for defined applications. These profiles define the functions of an application (e.g. physical access control for employees at airports) and then specify use of options in the base standards to ensure biometric interoperability.

The ISO/IEC 24779[10] series specifies a family of icons and symbols used in association with devices for biometric enrolment, verification and/or identification. The symbols and icons are intended to show the type of biometric characteristics and to advise on the appropriate preparation and behaviour required when using a biometric system. They are also intended to assist capture subjects by guiding them as they use the biometric system.

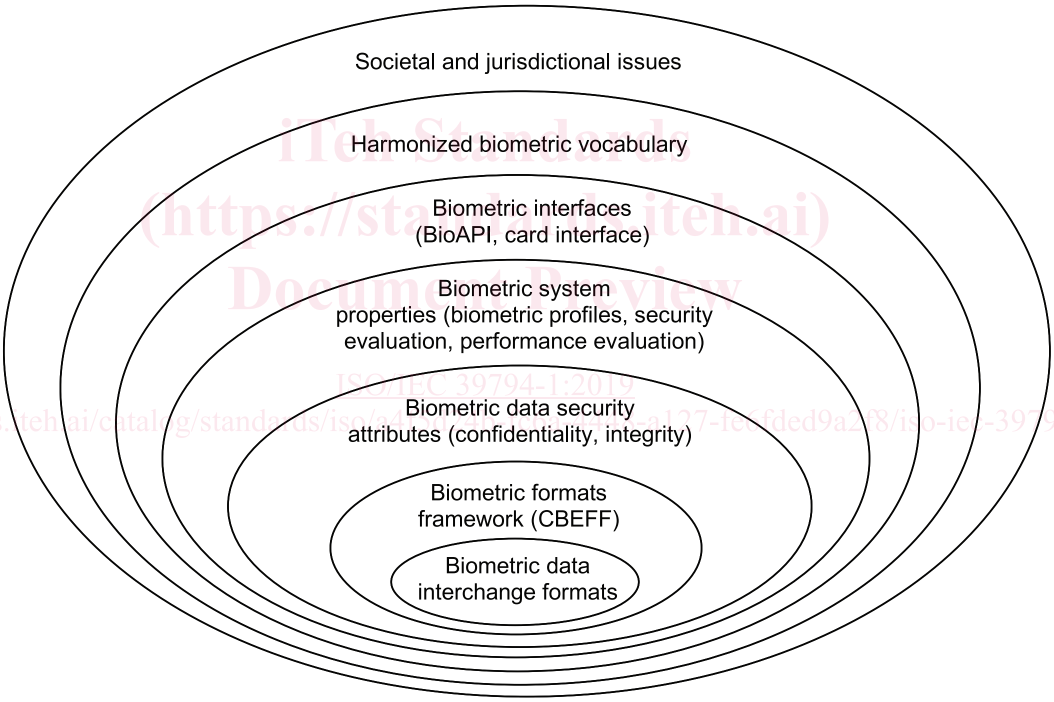

Figure 1 — General interrelation model of biometric issues

Information technology — Extensible biometric data interchange formats —

Part 1: Framework

1 Scope

This document specifies:

— rules and guidelines for defining extensible biometric data interchange formats that are extensible without invalidating previous data structures;

— the meaning of common data elements for use in extensible biometric data interchange formats;

— common data structures for tagged binary data formats based on an extensible specification in ASN.1;

— common data structures for textual data formats based on an XML schema definition; and

— conformance testing concepts and methodologies for testing the syntactic conformance of biometric data blocks.

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*

ISO 8601 (all parts), *Date and time — Representations for information interchange*

ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

ISO/IEC 19785-2,[1)] *Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the biometric registration authority*

ISO/IEC 29794-1, *Information technology — Biometric sample quality — Part 1: Framework*

ISO/IEC 30107-2, *Information technology — Biometric presentation attack detection — Part 2: Data formats*

IETF RFC 5141, *A Uniform Resource Name (URN) Namespace for the International Organization for Standardization (ISO)*

IETF RFC 5234, *Augmented BNF for Syntax Specifications: ABNF*

W3C Recommendation, *XML Schema Part 1: Structures* (Second Edition), 28 October 2004, http://www.w3.org/TR/xmlschema-1/

1) Second edition under preparation. Stage at time of publication: ISO/IEC DIS 19785-2:2018.

W3C Recommendation, *XML Schema Part 2: Datatypes* (Second Edition), 28 October 2004, http://www.w3.org/TR/xmlschema-2/

3 Terms and definitions

For the purposes 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:

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

— ISO Online Browsing Platform available at http://www.iso.org/obp.

3.1
biometric behavioural data
biometric data representing behavioural biometric characteristics of an individual

EXAMPLE Data resulting from writing, speaking or typing.

3.2
biometric data block
BDB
block of data conforming to a defined format

Note 1 to entry: The BDB is normally opaque to the processing of a standard biometric header (SBH) and is not required to be self-delimiting.

Note 2 to entry: This definition is aligned with ISO/IEC 19875-1.

3.3
biometric feature data unit
smallest individual unit of extracted biometric feature data

EXAMPLE Minutiae of a fingerprint.

3.4
biometric image data
biometric data that results from the presentation of biological biometric characteristics of an individual and is represented by pixels in a spatial coordinate system

EXAMPLE Fingerprint image data.

3.5
bit depth
number of bits used to represent a data element

3.6
octet
byte
contiguous sequence of 8 bits processed as a single unit of information

3.7
pixel
picture element
point in an image that is represented by an *n*-by-*m* matrix of points, where *n* is the number of horizontal rows and *m* is the number of vertical columns

4 Abbreviated terms

ABNF Augmented Backus-Naur Form

API application programming interface

ASN.1 Abstract Syntax Notation One

BDB biometric data block

BIR biometric information record

CBEFF Common Biometric Exchange Formats Framework

DER Distinguished Encoding Rules

HTTP Hypertext Transfer Protocol

ICS implementation conformance statement

IUT implementation under test

NSS namespace-specific string

PAD presentation attack detection

SBH standard biometric header

TLV tag-length-value

URI uniform resource identifier

URN uniform resource name

UTC Coordinated Universal Time

XML eXtensible Markup Language

XSD XML schema definition

5 Conformance

A binary biometric data interchange format conforms to this document if it satisfies the requirements specified within Clauses 7, 8, 9, and A.1.

A textual biometric data interchange format conforms to this document if it satisfies the requirements specified within Clauses 7, 8, 10, and A.2.

A general BDB embedding BDBs in formats defined elsewhere conforms to this document if it satisfies the requirements specified in Annex B.

A biometric data interchange format conformance test conforms to this document if it satisfies the requirements specified in Annex C.

6 General biometric system

6.1 Conceptual representation of general biometric system

Given the variety of applications and technologies, it can seem difficult to draw any generalizations about biometric systems. All such systems, however, have many elements in common. Captured

biometric samples are acquired from a subject by a biometric capture device. The biometric capture device output is sent to a processor that extracts the distinctive but repeatable measures of the sample (the biometric features), discarding all other components. The resulting features can be stored in the biometric enrolment database as a biometric reference. In other cases, the sample itself (without biometric feature extraction) may be stored as the reference. A subsequent query or probe biometric sample can be compared to a specific reference, to many references, or all references already in the database to determine if there is a match. A decision regarding the biometric claim is made based upon the similarities or dissimilarities between the features of the probe and those of the reference or references compared.

Figure 2 illustrates the information flow within a general biometric system, showing a general biometric system consisting of data capture, signal processing, data storage, comparison and decision subsystems. Figure 2 illustrates both enrolment and the operation of verification and identification systems. The subclauses in Clause 6 describe each of these subsystems in more detail.

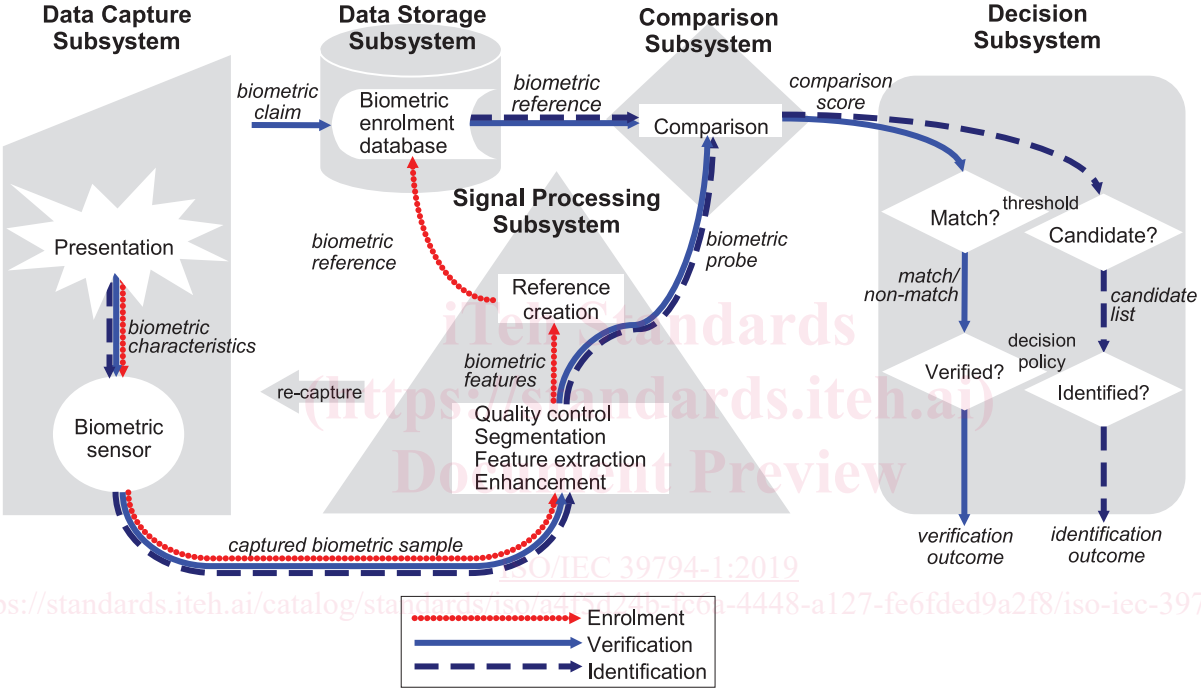

Figure 2 — Components of a general biometric system

NOTE In any implemented system, some of these conceptual components can be absent or could not have a direct correspondence with a physical or software entity.

6.2 Conceptual components of a general biometric system

6.2.1 Data capture subsystem

The data capture subsystem collects an image or signal of a subject's biometric characteristics presented to the biometric capture device (sensor) and outputs this image/signal as a captured biometric sample.

6.2.2 Transmission subsystem

The transmission subsystem (not portrayed in Figure 2; not always present or visibly present in a biometric system) will transmit samples, features, probes and references between different subsystems. The captured biometric sample may be compressed and/or encrypted before transmission and expanded and/or decrypted before use. A captured biometric sample may be altered in transmission due to noise in the transmission channel as well as losses in the compression/expansion process. Data may be transmitted using standardized biometric data interchange formats and cryptographic

techniques may be used to protect the authenticity, integrity and confidentiality of stored and transmitted biometric data.

6.2.3 Signal processing subsystem

Signal processing may include processes such as:

— enhancement, i.e. improving the quality and clarity of the captured biometric sample;

— segmentation, i.e. locating the signal of the subject's biometric characteristics within the captured biometric sample;

— biometric feature extraction, i.e. deriving the subject's repeatable and distinctive measures from the captured biometric sample; and

— quality control, i.e. assessing the suitability of samples, features, references, etc., possibly affecting other processes, such as:

  — returning control to the data capture subsystem to collect further samples or

  — modifying parameters for segmentation, biometric feature extraction, comparison.

In the case of enrolment, the signal processing subsystem creates a biometric reference. Sometimes the enrolment process requires features from several presentations of the individual's biometric characteristics. Sometimes the reference comprises just the features, in which case the reference may be called a biometric template. Sometimes the reference comprises just the sample, in which case biometric feature extraction from the reference occurs immediately before comparison.

In the case of verification and identification, the signal processing subsystem creates a biometric probe. Sequencing and iteration of the above-mentioned processes are determined by the specifics of each system.

6.2.4 Data storage subsystem

References are stored within an enrolment database held in the data storage subsystem. Each reference may be associated with some details of the enrolled subject or the enrolment process. Prior to being stored in the enrolment database, references may be reformatted into a biometric data interchange format. References may be stored within a biometric capture device, on a portable medium such as an integrated-circuit card, on a personal computer or local server, or in a central database.

6.2.5 Comparison subsystem

In the comparison subsystem, the features extracted from probes are compared against one or more references and comparison scores are passed to the decision subsystem. The comparison scores indicate the similarities or dissimilarities between the probes and references compared. For verification, a single specific claim of subject enrolment would lead to a single comparison score. For identification, many or all references may be compared with the probe, and a comparison score may be produced for each comparison.

6.2.6 Decision subsystem

The decision subsystem uses the comparison scores generated from one or more comparison attempts to provide the decision outcome for a verification or identification transaction.

In the case of verification, the probe is considered to match a compared reference when (assuming that higher scores correspond to greater similarity) the comparison score exceeds a specified threshold. A biometric claim can then be verified on the basis of the decision policy, which may allow or require multiple attempts.

In the case of identification, an enrolee is a potential candidate when (assuming that higher scores correspond to greater similarity) the comparison score exceeds a specified threshold, and/or when the comparison score is among the highest ranked values generated during comparisons across the entire database. The decision policy may allow or require multiple attempts before making an identification decision.

NOTE Conceptually, it is possible to treat multi-biometric systems in the same manner as unibiometric systems, by treating the combined captured biometric samples/references/scores as if they were a single sample/reference/score and allowing the decision subsystem to operate score fusion or decision fusion as and if appropriate. See also ISO/IEC TR 24722[9].

6.2.7 Administration subsystem

The administration subsystem (not shown in Figure 2) governs the overall policy, implementation, configuration and usage of the biometric system, in accordance with the relevant legal, jurisdictional and societal constraints and requirements. Illustrative examples include:

— interacting with the biometric capture subject including providing guidance feedback to the subject during and/or after data capture and requesting additional information from the subject;

— storing and formatting of interchanged biometric data;

— providing final arbitration on output from decision and/or scores;

— setting threshold values for decision;

— setting biometric capture parameters;

— controlling the operational environment and non-biometric data storage;

— providing appropriate safeguards for subject privacy and data security; and

— interacting with the application that utilizes the biometric system.

6.2.8 Interface

The biometric system may or may not interface to an external application or system via a web services interface, an application programming interface, a hardware interface or a protocol interface (not shown in Figure 2).

6.3 Functions of general biometric system

6.3.1 Enrolment

In enrolment, a transaction by a biometric capture subject is processed by the system in order to generate and store a biometric reference for that individual.

Enrolment typically involves:

— capturing one or more biometric samples;

— sample restoration or enhancement;

— segmentation;

— biometric feature extraction;

— quality checks (which may reject the sample/features as being unsuitable for creating a reference, and require capture of further samples);

— (where system policy requires it) comparison against the stored biometric references to ensure that the subject is not already enrolled;

