INTERNATIONAL STANDARD

ISO/IEC 24713-1

First edition
2008-03-01

Information technology — Biometric profiles for interoperability and data interchange —

Part 1: Overview of biometric systems and biometric profiles

Technologies de l'information — Profils biométriques pour interopérabilité et échange de données —

Partie 1: Exposé général des systèmes biométriques et des profils biométriques

Reference number
ISO/IEC 24713-1:2008(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 24713-1 was prepared by Technical Committee ISO/TC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC 24713 consists of the following parts, under the general title *Information technology — Biometric profiles for interoperability and data interchange*:

— *Part 1: Overview of biometric systems and biometric profiles*

— *Part 2: Physical access control for employees at airports*

— *Part 3: Biometric based verification and identification of seafarers*

Introduction

This part of ISO/IEC 24713 is intended to form the overview part of the multipart standard on biometric profiles for interoperability and data interchange. It describes a schema for the use of a number of biometric standards. This part of ISO/IEC 24713 is not intended to replace or counter any other part of this International Standard, but rather to be used as a reference guide for the implementation of a generic biometric system or a profile-standardized system.

This part of ISO/IEC 24713 provides generic information and guidance to users about biometric systems and the use of the various base standards within biometric profiles to support interoperability and data interchange among biometrics applications and systems.

This part of ISO/IEC 24713 is one of a family of international standards being developed by ISO/IEC JTC 1/SC 37 that support interoperability and data interchange among biometrics applications and systems. This family of standards specifies requirements that solve the complexities of applying biometrics to a wide variety of personal recognition applications, whether such applications operate in an open systems [1)] environment or consist of a single, closed system.

Biometric data interchange format standards and biometric interface standards are both necessary to achieve full data interchange and interoperability for biometric recognition in an open systems environment. 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.

- The biometric data interchange format standards specify biometric data interchange records for different biometric modalities. Parties that agree in advance to exchange biometric data interchange records as specified in a subset of the ISO/IEC JTC 1/SC 37 biometric data interchange format standards should be able to perform biometric recognition with each other's data. Parties should also be able to perform biometric recognition even without advance agreement on the specific biometric data interchange format standards to be used, provided they have built their systems on the layered ISO/IEC JTC 1/SC 37 family of biometric standards.

- The biometric interface standards include the Common Biometric Exchange Formats Framework (CBEFF) and the Biometric Application Programming Interface (BioAPI). These standards support exchange of biometric data within a system or among systems. The CBEFF standard specifies the basic structure of a standardized Biometric Information Record (BIR) which includes the biometric data interchange record with added metadata, such as when it was captured, its expiry date, whether it is encrypted, etc. The BioAPI standard specifies an open system API that supports communications between software applications and underlying biometric technology services. BioAPI also specifies a CBEFF BIR format for the storage and transmission of BioAPI-produced data.

The biometric profile standards facilitate implementations of the base standards (e.g. the ISO/IEC JTC 1/SC 37 biometric data interchange format and biometric interface standards, and possibly non-biometric standards) for defined applications. These profile standards 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.

---

1) 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 may 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.

Information technology — Biometric profiles for interoperability and data interchange —

Part 1:
Overview of biometric systems and biometric profiles

1 Scope

This part of ISO/IEC 24713 identifies and defines the functional blocks and components of a generic biometric system, and the distinct characteristics of each component. It also defines a generic biometric reference architecture incorporating the relevant biometric-related base standards to support interoperability and data interchange.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19794-1:2006, *Information technology — Biometric data interchange formats — Part 1: Framework*

3 Terms and definitions

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

3.1
application programming interface
API
software based interface that can be used for communications and interfacing between an application and the biometric system.

NOTE 1 An API is computer code used by an application developer. Any biometric system that is compatible with the API can be added or interchanged by the application developer.

NOTE 2 APIs are often described by the degree to which they are high level or low level. High level means that the interface is proximate to the application and low-level means that the interface is proximate to the device.

3.2
application
hardware/software system implemented to satisfy a broad set of requirements.

NOTE In this context, an application incorporates a biometric system to satisfy a subset of requirements related to the verification or identification of an end-user's identity so that the end-user's identifier can be used to facilitate the end-user's interaction with the system.

EXAMPLE A biometrics-enabled time and attendance system has a 'broad' requirement to record an employee's starting and leaving times so the employee can be paid the correct amount of wages. The system uses biometrics to verify

the employee's "end-user's" claim that his identity is the one that the system has associated with the employee's id-number 'identifier' at the times when the employee interacts with the biometric device as he enters and leaves the work place.

3.3
base standard
fundamental standard with elements that contain options.

NOTE Base standards can be used in diverse applications, for each of which it may be useful to fix the optional elements in a standardized profile with the aim of achieving interoperability between instances of the specific application.

3.4
biometric
pertaining to the field of biometrics

NOTE "Biometric" is never used as a noun.

3.5
biometrics
automated recognition of individuals based on their behavioural and biological characteristics

3.6
biometric data
information extracted from the biometric sample used to build a template or to compare against a previously created template

3.7
biometric functions
procedures or activities of **enrolment** (3.19), **verification** (3.40) and/or **identification** (3.25) within a biometric system

3.8
biometric interchange data
BID
biometric data formatted according to one or more of the data interchange standards as defined by ISO 19794

3.9
biometric profile
conforming subsets or combinations of base standards used to effect specific biometric functions

NOTE Biometric profiles define specific values or conditions from the range of options described in the relevant base standards, with the aim of supporting the interchange of data between applications and the interoperability of systems.

3.10
biometric sample
raw data representing a biometric characteristic of an end-user as captured by a biometric system

3.11
biometric system
(mainly) automated system capable of

1) capturing a biometric sample from an end-user or as provided by a forensic technology,

2) extracting biometric data from that sample, or alternatively, deriving biometric features from the biometric data in a form suitable for comparison with one or more reference templates,

3) comparing the biometric features with those contained in one or more reference templates ,

4) determining the level of similarity by a score or other metric, or alternatively, ranking in accordance with the level of similarity as determined by a score or other metric,

5) returning a result to the application indicating whether the identification and/or verification has been successful or not, and

6) storing and managing biometric data and related system information

NOTE The set of biometric systems can be divided in two classes as follows:

Single-biometric system: biometric system that uses a single biometric modality, algorithm or sensor.

Multi-biometric system: biometric system that uses multiple biometric modalities and/or sensors and/or algorithms.

3.12
biometric system components
those parts or elements of the system that perform specific tasks that are required by the system in order for it to function.

EXAMPLE Examples of biometric system components are capture, process and compare.

3.13
biometric template
biometric data derived from a biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison

3.14
capture
method of taking a biometric sample from an end-user

3.15
comparison
process of evaluating the similarities between a template and a reference template

3.16
database
structured set of data held in a computer

3.17
decision
result of the comparison between the match score and the threshold

NOTE The decision can be acceptance or rejection.

3.18
end-user
person who interacts with a biometric system to enroll or have his/her identity checked

3.19
enrolment
process of collecting biometric sample(s) from an end-user and the subsequent preparation and storage of biometric reference template(s) and, if necessary, associated data in connection with the end-user's identity

3.20
extraction
process of converting a captured biometric sample into biometric data

3.21
false acceptance
when a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity

3.22
false rejection
when a biometric system fails to identify an end-user or fails to verify the legitimate claimed identity of an end-user

3.23
identifier
unique data string used as a key in the biometric system to associate a person's biometric with a person's identity attributes

3.24
identity
common-sense notion of personal identity

NOTE Attributes that could be used in defining an identity include a person's name, aspects of their personality or physical appearance, previous history of transactions between the application and the end-user, nationality, educational achievements, employer, security clearances, financial and credit history. In a biometric system, identity is typically established when the person is registered in the system through the use of so-called "breeder documents" such as birth certificate, passport, etc.

3.25
identification
〈biometric system function〉 biometric system function that performs a one-to-many search to obtain a candidate list

EXAMPLE BioAPI_IdentifyMatch

NOTE An identification function may be used to verify a claim of enrolment in an enrolment database without a specified biometric reference identifier.

3.26
match
matching

process of comparing biometric data derived from biometric samples against a previously stored template(s) and scoring the level of similarity

3.27
multiple biometric
biometric system that includes more than one biometric technology

3.28
negative identification
biometric system function that performs a one-to-many search of submitted biometric data derived from a biometric sample against all or some of the templates in a database of end-users in order to confirm that the assertion that an end-user has not yet been enrolled into (that part) of a database

3.29
population
set of end-users for the application

3.30
positive Identification
biometric system function that performs a one-to-many search of submitted biometric data derived from a biometric sample against all or some of the templates in a database of end-users, and outputs the template corresponding to the identity of the correctly authenticated end-user

3.31
record
template and other information about the end-user (e.g. access permissions)

3.32
registration
process of making a person's **identity** (3.24) known to a biometric system, associating a unique **identifier** (3.23) with that identity, and collecting and recording the person's relevant attributes into the system

3.33
score
numerical value, result of a comparison, indicating the degree of similarity or correlation between a biometric sample and a reference template

3.34
standard
document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context - Note - Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits

3.35
subject
end-user whose biometric data is intended to be enrolled or compared

3.36
token
physical device that contains information specific to the end-user or bearer

3.37
threshold
boundary value of the score used by the comparison application to decide automatically if one reference template, compared to the template submitted to the system, is accepted or rejected

NOTE If the score of the comparison is above the threshold, the reference template is accepted in the candidates list; if not, it is rejected. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

3.38
user
individual responsible for managing and/or implementing and/or administering the biometric system, as distinct from the end-user whose biometric sample is captured

3.39
validation
process of demonstrating that the system under consideration meets in all respects the specification of that system

3.40
verification
biometric system function that performs a one-to-one comparison of a submitted sample against a specified stored template, and returns the matching score or matching decision

3.41
biometric Features
distinctive and repeatable measures of the biometric sample which can be stored as a template in a database or compared with a specific template