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 ... iv

Introduction ... v

1 Scope ... 1

2 Normative references ... 1

3 Terms and definitions ... 1

4 Abbreviated terms ... 6

5 General biometric system ... 6
5.1 Conceptual diagram of general biometric system ... 6
5.2 Conceptual components of a general biometric system ... 7
5.2.1 Data capture subsystem ... 7
5.2.2 Transmission subsystem (not portrayed in diagram) ... 7
5.2.3 Signal processing subsystem ... 7
5.2.4 Data storage subsystem ... 7
5.2.5 Matching subsystem ... 7
5.2.6 5.2.6 Decision subsystem ... 7
5.2.7 5.2.7 Administration subsystem (not portrayed in diagram) ... 8
5.2.8 Interface (not portrayed in diagram) ... 8
5.3 Functions of general biometric system ... 8
5.3.1 Enrolment ... 8
5.3.2 Verification ... 9
5.3.3 Identification ... 9

6 Relationship between the biometric system and the application ... 10
6.1 General ... 10
6.2 The ID life-cycle ... 10
6.2.1 Proofing ... 11
6.2.2 Registration ... 11
6.2.3 Issuance ... 11
6.2.4 Usage ... 11
6.3 Subject versus end-user ... 11
6.3.1 6.3.1 Access control example ... 12
6.3.2 Travel document example ... 12
6.4 Biometric decision versus authorization ... 13

7 Interfaces between the biometric system and the application ... 14
7.1 Application programming interface (API) ... 14
7.2 Protocol interface ... 15
7.3 Hardware based electronic input/output interface ... 15

8 Developing biometric profiles utilising biometrics base standards ... 15
8.1 Relationships of biometric base standards and their use in biometric profiles ... 15
8.2 Classes ... 16
8.2.1 Application class ... 16
8.2.2 Data class ... 16
8.2.3 Interface class ... 17
8.3 Using biometric base standards to develop biometric profiles ... 17

Bibliography ... 18

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

4 Abbreviated terms

For the purposes of this document, the following abbreviations apply.

BID Biometric Interchange Data
ID Identification

5 General biometric system

5.1 Conceptual diagram of general biometric system

Given the variety of applications and technologies, it might seem difficult to draw any generalizations about biometric systems. All such systems, however, have many elements in common. Biometric samples are acquired from a subject by a sensor. The sensor output is sent to a processor which extracts the distinctive but repeatable measures of the sample (the "features"), discarding all other components. The resulting features can be stored in the database as a "template", or compared to a specific template, many templates or all templates already in the database to determine if there is a match. A decision regarding the identity claim is made based upon the similarity between the sample features and those of the template or templates compared.

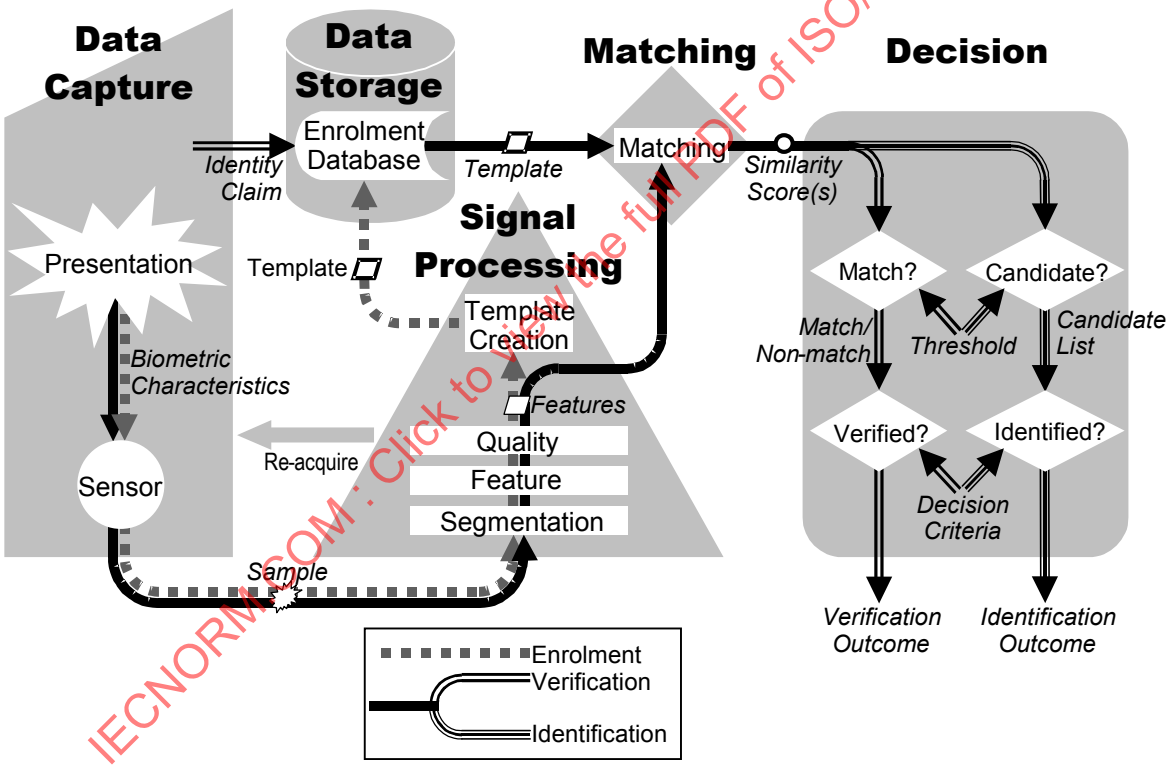

Figure 1 — Components of general biometric system

Figure 1 illustrates the information flow within a general biometric system, showing a general biometric system consisting of data capture, signal processing, storage, matching and decision subsystems. This diagram illustrates both enrolment, and the operation of verification and identification systems. The following sub-clauses describe each of these subsystems in more detail. It should be noted that, in any real biometric system, these conceptual components may not exist or may not directly correspond to the physical components.

5.2 Conceptual components of a general biometric system

5.2.1 Data capture subsystem

The data capture subsystem collects an image or signal of a subject's *biometric characteristics* that they have *presented* to the *biometric sensor*, and outputs this image/signal as a *biometric sample*.

5.2.2 Transmission subsystem (not portrayed in diagram)

The transmission subsystem (not always present or visibly present in a biometric system) will transmit *samples, features,* and/or *templates* between different subsystems. *Samples, features* or *templates* may be transmitted using standard biometric data interchange formats. The biometric *sample* may be compressed and/or encrypted before transmission, and expanded and/or decrypted before use. A biometric *sample* may be altered in transmission due to noise in the transmission channel as well as losses in the compression/expansion process. It is advisable that cryptographic techniques be used to protect the authenticity, integrity, and confidentiality of stored and transmitted biometric data.

5.2.3 Signal processing subsystem

The signal processing subsystem extracts the distinguishing *features* from a biometric *sample*. This may involve locating the signal of the subject's *biometric characteristics* within the received *sample* (a process known as *segmentation*), *feature extraction*, and *quality control* to ensure that the extracted features are likely to be distinguishing and repeatable. Should *quality control* reject the received *sample/s*, control may return to the data capture subsystem to collect a further *sample/s*.

In the case of enrolment, the signal processing subsystem creates a *template* from the extracted biometric *features*. Often the enrolment process requires *features* from several presentations of the individual's *biometric characteristics*. Sometimes the *template* comprises just the *features*.

5.2.4 Data storage subsystem

Templates are stored within an *enrolment database* held in the data storage subsystem. Each *template* is associated with details of the enrolled subject. It should be noted that prior to being stored in the *enrolment database*, *templates* may be re-formatted into a biometric data interchange format. *Templates* may be stored within a biometric capture device, on a portable medium such as a smart card, locally such as on a personal computer or local server, or in a central database.

5.2.5 Matching subsystem

In the matching subsystem, the *features* are compared against one or more *templates* and *similarity scores* are passed to the decision subsystem. The *similarity scores* indicate the degree of fit between the *features* and *template/s* compared. In some cases, the *features* may take the same form as the stored *template*. For verification, a single specific claim of subject enrolment would lead to a single *similarity score*. For identification, many or all *templates* may be compared with the *features*, and output a *similarity score* for each comparison.

5.2.6 Decision subsystem

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

In the case of verification, the *features* are considered to match a compared *template* when the *similarity score* exceeds a specified *threshold*. A claim about the subject's enrolment can then be verified on the basis of the *decision policy*, which may allow or require multiple attempts.

In the case of identification, the end-user identifier or *template* is a potential *candidate* for the subject when the *similarity score* exceeds a specified *threshold*, and/or when the *similarity score* is among the highest k values generated for a specified value k. 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 uni-biometric systems, by treating the combined biometric *samples/templates/scores* as if they were a single *sample/template/score* and allowing the decision subsystem to operate score fusion or decision fusion as and if appropriate.

5.2.7 Administration subsystem

The administration subsystem (which is not portrayed in Figure 1) governs the overall policy, implementation and usage of the biometric system, in accordance with the relevant legal, jurisdictional and societal constraints and requirements. Illustrative examples include:

- providing feedback to the subject during and/or after data capture;
- requesting additional information from the subject;
- storage and format of the biometric *templates* and/or biometric interchange data;
- provide final arbitration on output from decision and/or scores;
- set *threshold* values;
- set biometric system acquisition settings;
- control the operational environment and non-biometric data storage;
- provide appropriate safeguards for end-user privacy;
- interact with the application that utilizes the biometric system.

5.2.8 Interface (not portrayed in diagram)

The biometric system may or may not interface to an external application or system via an Application Programming Interface, Hardware Interface or a Protocol Interface.

5.3 Functions of general biometric system

5.3.1 Enrolment

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

Enrolment typically involves:

- sample acquisition,
- egmentation and feature extraction,
- quality checks, (which may reject the sample/features as being unsuitable for creating a template, and require acquisition of further samples),
- template creation (which may require features from multiple samples), possible conversion into a biometric data interchange format and storage,
- test verification or identification attempts to ensure that the resulting enrolment is usable, and
- should the initial enrolment be deemed unsatisfactory, repeat enrolment attempts may be allowed (dependent on the enrolment policy).

5.3.2 Verification

In verification, a transaction by a subject is processed by the system in order to verify a positive specific claim about the subject's enrolment (e.g. "I am enrolled as subject X"). Verification will either accept or reject the claim. The verification decision outcome is considered to be erroneous if either a false claim is accepted (false accept) or a true claim is rejected (false reject). Note that some biometric systems will allow a single end-user to enroll more than one instance of a biometric characteristic (for example, an iris system may allow end-users to enroll both iris images, while a fingerprint system may have end-users enroll two or more fingers as backup, in case one finger gets damaged)

Verification typically involves:

- sample acquisition,
- segmentation and feature extraction,
- quality checks, (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples),
- comparison of the sample features against the template for the claimed identity producing a similarity score,
- judgement on whether the sample features match the template based on whether the similarity score exceeds a threshold, and
- a verification decision based on the match result of one or more attempts as dictated by the decision policy.

EXAMPLE In a verification system allowing up to three attempts to be matched to an enrolled template, a false rejection will result with any combination of failures-to-acquire and false non-matches over three attempts. A false acceptance will result if a sample is acquired and falsely matched to the enrolled template for the claimed identity on any of three attempts.

5.3.3 Identification

In identification, a transaction by a subject is processed by the system in order to find an identifier of the subject's enrolment. Identification provides a candidate list of identifiers that may be empty or contain only one identifier. Identification is considered correct when the subject is enrolled, and an identifier for their enrolment is in the candidate list. The identification is considered to be erroneous if either an enrolled subject's identifier is not in the resulting candidate list (false-negative identification error), or if a transaction by a non-enrolled subject produces a non-empty candidate list (false-positive identification error).

Identification typically involves:

- sample acquisition,
- segmentation and feature extraction,
- quality checks, (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples),
- comparison against some or all templates in the enrolment database, producing a similarity score for each comparison,
- judgement on whether each matched template is a potential candidate identifier for the user, based on whether the similarity score exceeds a threshold and/or is among the highest k scores returned, producing a candidate list,
- an identification decision based on the candidate lists from one or more attempts, as dictated by the decision policy.

6 Relationship between the biometric system and the application

6.1 General

An application that incorporates a biometric system (besides other things) must be able to manage identities. This can be described on an abstract level by the ID Life Cycle. The ID Life cycle describes the interaction of

- individuals,
- credentials,
- privileges, and resources.

The general use case is that an individual wishes to receive and use some (logical or physical) credential granting them access to privileges and/or resources. A credential is “something that entitles one to confidence, credit, or authority”.

Credentials can include:

- documents,
- cards,
- personal identification numbers (PINs),
- passwords.

The privilege may be an authorization, e.g. accessing certain data.

A simple access control example is that an employee applies for an access control card granting him the right to access certain areas. In a passport scenario, a citizen may apply for a new passport or visa permitting him to cross the border to a country he wishes to visit.

The role that biometric systems play within a general Application or Security System is to provide evidence (through a Biometric Decision) that a subject either is who they claim to be (Verification or Positive Identification); or to establish that they are not part of a pre-existing group (Negative Identification or Watchlist Identification).

6.2 The ID life-cycle

In general the ID life cycle for a verification system consists of four different phases in identity management. In specific applications, some of the phases may occur in conjunction with other phases of the life cycle. But generally speaking, any of these phases may occur (physical or logical) separate from each other.

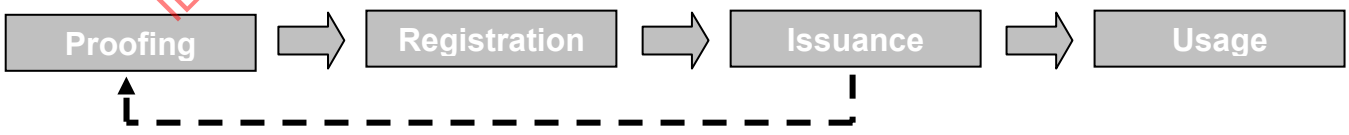

Figure 2 — The ID life cycle

Applications typically iterate through the cycle when managing identities throughout their lifetime.

6.2.1 Proofing

Proofing is the process of verifying that a physical identity is valid, i.e. that a person is who he or she claims to be.

EXAMPLE Checking breeder documents (e.g. birth certificate, passport) for validation. Biometrics may be used for background checks and to verify the person against breeder documents etc. (see below).

6.2.2 Registration

Registration is the process of creating an electronic identity in the application domain representing the physical identity (and binding information to it). Typically, a unique identifier representing the physical identity is established during this process. Furthermore, biometric data samples are captured in the enrolment stage of this registration process.

EXAMPLE Capturing and storing personal data before issuing a new drivers license.

The biometric subsystem is usually used by an authority (legal, professional, etc.) that decides to establish a strong relation between a biometric sample and a set of information relevant to that authority. This strong relation is initially established at the enrolment level, where biometric data is added to the already proofed identity. The authority has the capability to establish the strong relation through the use of any security mechanism, like the encryption of records relating to end-users.

6.2.3 Issuance

Issuance is the process of granting privileges to an identity and giving him or her a credential to access the privileges.

EXAMPLE 1 Authorising a person physical access rights in combination with an access control card,

EXAMPLE 2 Issuing a passport to the person enabling him to cross borders,

EXAMPLE 3 Issuing a password to a person to access confidential data.

In the issuance process biometrics may be involved, e.g. for checking if the person wanting to pick up the credential is the “right“ person, i.e. matches the biometrics stored on an ID document.

6.2.4 Usage

After having granted rights, the physical identity uses the credential in the application domain to access his/her privileges, e.g. a certain authorization.

EXAMPLE 1 Physical access to a restricted area by using a biometric enabled token.

EXAMPLE 2 Crossing a border by using a biometric enabled machine-readable travel document.

With respect to biometrics, within the usage process the information integrity established during the enrolment process can be checked, and the strong relationship between the end-user and the information can be confirmed, depending on the level of confidence of the authority that enrolled.

6.3 Subject versus end-user

In this section, two aspects of a subject’s Identity are highlighted; an Identifier (referring to a logical identity) by which they are known to an application; and the proofing process, which provides additional evidence that they are the person associated with the identifier.

6.3.1 Access control example

As an example, the various steps comprising the registration of a new end-user within an application should be considered, e.g. an employee access control system:

Proofing:
An administrator of the application will establish the unique identity of the subject by using non-biometric and biometric means. Proofing is typically achieved through the use of so-called “breeder documents” such as birth certificates, passports etc. This step may also include a search over a biometric database to establish the uniqueness of the individual’s claim according to the range of that database. This is accomplished through the use of Negative Identification. This may include a background check with a law enforcement agency or a database search of all end-users enrolled in the system up to that point

Registration:
If the Subject is identified as unique, the access control system will establish the individual as a new end-user of the system, and assign a unique Identifier by which they are known to the system. An example of an Identifier would be an Access Control ID number. As part of the registration process the Subject will be instructed to enroll their biometric and the biometric system will create a Biometric Interchange Data Record that is associated with the end-user via this Identifier. The BID Record will be bound to the Identifier, either by physically storing them in related locations in the BID Storage or Application database, or by binding them together using encryption or through a digital signature mechanism, to create an end-user Record. The registration of the Subject as a new end-user of the system is now complete.

6.3.2 Travel document example

A second example shows the steps that may occur in the process of a citizen applying for a new travel document, e.g. a biometric enabled passport.

Proofing:
In this specific example the process of proofing will extend beyond that used in the access control example (ref. section 6.3.1), often requiring evidence of a social footprint through reference to other databases, and possibly some form of attestation by an accepted authority. Furthermore, in the case of a renewal, positive biometric verification may be used to check the person’s identity.

Registration:
If the Subject is identified as unique, the administrator establishes the individual as a valid end-user and assigns a unique Identifier by which they are known to the system. An example of an Identifier would be a passport number. As part of the registration process the Subject will be instructed to enroll or re-enroll their biometric, and the biometric system will create a Biometric Interchange Data Record that is associated with the end-user via this Identifier. The BID Record will be bound to the Identifier, either by physically storing them in related locations in the BID Storage or Application database, or by binding them together using encryption (see figure 2 above) or through a digital signature mechanism, to create or update an end-user Record. The registration process is now complete. For the issuance process, the administrator may hand out a unique transaction number that enables the Subject to pick up the passport after production. This may or may not be identical to the Identifier that they are known by within the application.

Issuance:

After notification, and if a transaction number has been delivered as part of the Registration process, the subject can use this to pick up the new travel document. Biometrics may be used to verify that the person trying to pick up the passport is the person whose biometrics are stored on the passport.

In both examples, the registration results in a binding of the biometric with an ID number. It is the ID number (identifier), i.e. a logical identity, that is recognized by the application and not a physical identity.

6.4 Biometric decision versus authorization

The following section further clarifies the differences between a decision (verification or identification) of the biometric system and the privileges (authorizations) of the application. Whether an individual is required to either be verified or identified by a biometric system, the application manages the decision and the privileges (authorization).

The Decision is the output of the biometric system, based upon a comparison between the biometric data of the Subject derived form the biometric sample, and either a template, in the case of verification, or a set of templates in the case of identification.

Note: the result type depends on the application and may be: a go / no go, a score, a list, etc.

The privileges (authorization) are the result of the process based on the decision and the information associated with the biometric data obtained during the registration process. At this stage, the integrity of the information, the confidence level in the authority that manages the information, the rights and privileges associated, etc. are essential to provide a valid authorization.

It is instructive to consider what happens in the usage process, i.e. when an individual wishes to gain access (example 6.3.1) or to cross a border (example 6.3.2), respectively.

The Biometric Decision can use either Positive Identification or Verification. In the case where the BID Record has been bound to the Identifier though encryption, the following steps are undertaken:

A Subject establishes a claim to the Application that they are a valid end-user of the system. In the access control scenario, this can be achieved, for example, by entering the username associated with the end-user, or by presenting a token to the system from which a pointer to the end-user Record, or the end-user Record itself, is extracted. In the travel document scenario, the passport may hold a token or a chip, that stores the end-user Record itself and is read by the passport reader it is presented to.

- The Application ensures that the end-user Record of the claimed end-user is available to the biometric system (either by transmitting it to the biometric system, or by selecting it within the biometric system), where it will be unbound to produce the BID Record and Identifier that were bound during end-user registration. Note that as part of this step, either the Application or the biometric system (or both) may verify the authenticity of the end-user record, by, for example, checking a digital signature.

- The Subject is requested to demonstrate that they are the person associated with the identifier by providing a sample of their biometric to the biometric capture device. Following the usual steps for verification (See clause 5.3.2), the biometric system will produce a decision about whether or not the subject is indeed associated with the identifier.

- If the biometric decision is positive, this implies that the Subject is associated with the BID, which is bound to the identifier in the end-user record, thus implying the subject is associated with the identifier in the end-user Record. This identifier is then relayed to the application (see figure 3 below) where the end-user is authorized, according to their application rights. In the access control scenario, access to the system would be granted, and in the travel document scenario, the subject would be permitted to cross the border.

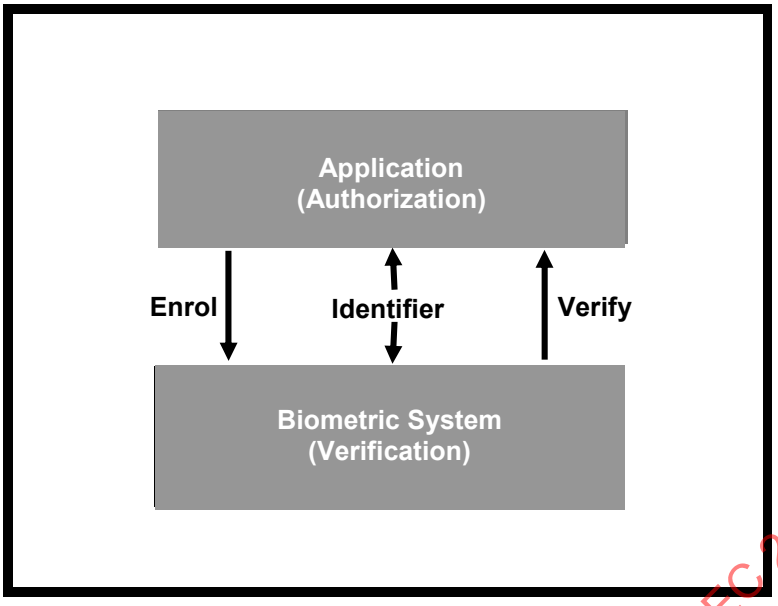

Figure 3 — The interaction of the identifier between end-user verification and application authorization

This separation between the Verification of the Subject (a decision of the biometric system) and the privileges of the end-user, e.g. an authorization, within the application is key for successful integration of biometric systems into general applications. It provides an explicit segregation between the decision process in the biometric system and the rights and privileges that the end-user is assigned by the application. This is especially important when considering issues such as the revocation of an end-user's rights and privileges, and the fact that any individual may appear as multiple end-users to an application (for example, as a normal end-user *and* as an administrator). The use of encryption or a similar binding mechanism also mitigates potential of data compromise.

7 Interfaces between the biometric system and the application

The purpose of this section is to define possible interfaces that may exist between the Biometric System and the Application.

The following possible interfaces may exist:

— Application programming Interface

— Protocol Interface

— Hardware based Electronic Input/Output interface

7.1 Application programming interface (API)

As is commonly defined within Information Technology Standards, an API is a software based interface that can be used for communications and interfacing between the application and the biometric system. This form of interface may, but need not, occur on the same physical processing computer. This is the most common form of interface and is supported by the BioAPI Specification. The API is a low-level interface that usually provides extensive functionality between the Application and the Biometric System.