INTERNATIONAL STANDARD

ISO/IEC 24713-2

First edition
2008-06-01

Information technology — Biometric profiles for interoperability and data interchange —

Part 2: Physical access control for employees at airports

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

Partie 2: Contrôle d'accès physique pour les employés aux aéroports

Reference number
ISO/IEC 24713-2:2008(E)

COPYRIGHT PROTECTED DOCUMENT

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) 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national 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 24713-2 was prepared by Joint Technical Committee ISO/IEC 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: Biometrics-based verification and identification of seafarers*

Introduction

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.[1)] 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 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 ISO/IEC 19785, the Common Biometric Exchange Formats Framework (CBEFF) and ISO/IEC 19784, the Biometric Application Programming Interface (BioAPI). These standards support exchange of biometric data within a system or among systems. ISO/IEC 19785 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. ISO/IEC 19784 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 2: Physical access control for employees at airports

1 Scope

This part of ISO/IEC 24713 specifies the biometric profile including necessary parameters and interfaces between function modules (i.e. BioAPI based modules and an external interface) in support of token-based biometric identification and verification of employees, at local access points (i.e. doors or other controlled entrances) and across local boundaries within the defined area of control in an airport. The token is expected to contain one or more biometric references.

This part of ISO/IEC 24713 does not specify a complete Access Control System for deployment at access points within the secure area of an airport. It is assumed that such systems exist and that a biometric component that is the subject of this part of ISO/IEC 24713 is being added to an existing system. It therefore excludes such things as device features, and exception and incident reporting and handling. This information is contained in Annex C for information only.

This part of ISO/IEC 24713 includes recommended practices for enrolment, watch list checking, duplicate issuance prevention, and verification of the identity of employees at airports. It also describes architectures and business processes appropriate to the support of token-based identity management in the secure environment of an airport.

It is recommended that the confidentiality, integrity, and availability of biometric data be safeguarded in accordance with local, regional, or national policy considerations.

This part of ISO/IEC 24713 does not preclude users building applications based on this part of ISO/IEC 24713 from being able to meet such privacy/data protection requirements as may apply to their application. The specification of privacy/data protection requirements that may apply is outside the scope of this part of ISO/IEC 24713.

2 Conformance

A system conforms to this part of ISO/IEC 24713 if it correctly performs all the mandatory capabilities defined in the requirements list and supplies the profile specific Implementation Conformance Statement (ICS) in Annex A. Note that more capabilities may be required than in the base standards.

3 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 19784-1:2006, *Information technology — Biometric application programming interface — Part 1: BioAPI specification*

ISO/IEC 19785-1:2006, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-3:2007, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19794-2:2005, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

ISO/IEC 19794-3:2006, *Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data*

ISO/IEC 19794-4:2005, *Information technology — Biometric data interchange formats — Part 4: Finger image data*

ISO/IEC 19794-5:2005, *Information technology — Biometric data interchange formats — Part 5: Face image data*

ISO/IEC 19794-6:2005, *Information technology — Biometric data interchange formats — Part 6: Iris image data*

ISO/IEC 19794-7:2007, *Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data*

ISO/IEC 19794-8:2006, *Information technology — Biometric data interchange formats — Part 8: Finger pattern skeletal data*

ISO/IEC 19794-9:2007, *Information technology — Biometric data interchange formats — Part 9: Vascular image data*

ISO/IEC 19794-10:2007, *Information technology — Biometric data interchange formats — Part 10: Hand geometry silhouette data*

ISO/IEC 19795-1:2006, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

ISO/IEC 19795-2;2007, *Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation*

ISO/IEC 24713-1:2008, *Information technology — Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles*

4 Terms and definitions

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

4.1
application
program or piece of software designed to fulfil a particular purpose

4.2
base standard
standard that is part of a profile and from which options, subsets, and parameter values are selected if these choices are left open in the standard

4.3
biometric
pertaining to biometrics

4.4
biometrics
automated recognition of individuals based on their behavioural and biological characteristics

4.5
biometric characteristic
measurable, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of an enrolee

4.6
biometric feature
concise representation of information extracted from an acquired or intermediate biometric sample by applying a mathematical transformation

4.7
biometric profile
conforming subsets or combinations of base standards used to provide specific functions

NOTE Biometric profiles identify the use of particular options available in base standards, and provide a basis for the interchange of data between applications and interoperability of systems.

4.8
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to an individual and used for comparison

4.9
biometric sample
raw data representing a biometric characteristic of an end-user as captured by a biometric system (for example, the image of a fingerprint)

4.10
biometric system
automated system capable of:

— capturing a biometric sample from an end-user;

— extracting biometric data from that sample;

— comparing the biometric data with that contained in one or more reference templates;

— deciding how well they match, and indicating whether or not an identification or verification of identity has been achieved

4.11
biometric template
data that represents the biometric measurement of an enrolee

NOTE Used by a biometric system for comparison against submitted biometric samples.

4.12
capture
method of taking a biometric sample from an end-user

4.13
comparison
process of comparing a biometric sample with a previously stored reference template or templates

cf. **identification** and **verification**

4.14
claimant
person submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity

4.15
database
structured set of data held in a computer

4.16
end-user
person (employee) who interacts with a biometric system to enrol or have his/her identity checked

4.17
enrolee
person who has a biometric reference template on file

4.18
enrolment
process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity

4.19
extraction
process of converting a captured biometric sample into biometric data

4.20
false acceptance
⟨biometric system⟩ incorrect identification of an individual or incorrect verification of an impostor against a claimed identity

4.21
false acceptance rate
FAR
proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed

NOTE The false acceptance rate is estimated as the proportion of recorded zero-effort impostor transactions that were incorrectly accepted (or weighted proportion, in case the number of recorded zero-effort impostor transactions is different for individual crew members).

4.22
false rejection
when a biometric system fails to identify an enrolee or fails to verify the legitimate claimed identity of an enrolee

4.23
false rejection rate
FRR
proportion of verification transactions with truthful claims of identity that are incorrectly denied

NOTE The false rejection rate is estimated as the proportion of recorded genuine transactions that were incorrectly denied (or weighted proportion, in case the number of recorded genuine transactions is different for individual test crew members).

4.24
identifier
unique data string used as a key in the biometric system to associate a person's biometric with a person's identity attributes

4.25
identification
identify
biometric system function that performs a one-to-many search of a submitted sample against all or part of the enrolled database, and outputs a candidate list of zero, one or more identifiers for the stored templates found to be similar to the submitted sample

4.26
match
matching
process of comparing (a) biometric sample(s) against (a) previously stored template(s) and scoring the level of similarity

4.27
multiple biometric
biometric system that includes more than one biometric modality

4.28
population
set of end-users for the application

4.29
record
template and other information about the end-user

EXAMPLE Access permissions.

4.30
registration
process of making a person's identity known to a biometric system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system

4.31
token
physical device that contains information specific to the bearer (end-user) or issuer (user)

4.32
transaction
an attempt by an end-user to validate a claim of identity or non-identity by consecutively submitting one or more samples, as allowed by the system decision policy

4.33
verification
verify
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

5 Environment

5.1 Employees in the targeted environment

The physical Access Control deployment requests that groups of employees shall be identified. Employees are sets of people involved in airport activities with common characteristics.

Employees are targeted by this part of ISO/IEC 24713. Characteristics are:

— individuals that access different restricted areas covered by the airport authorities;

— individuals that have access to the restricted areas only under condition of professional objectives;

— individuals subject to labour regulation.

For example, employees are receptionists, refuelling staff, maintenance staff, carrier, temporal road workers.

Employers maintain contractual links with employees. The contractual links are either employment contract or commercial contract. Employers are responsible for requesting physical access control for employees to the airport authorities. Employers shall be in charge of collecting all information requested by the airport authorities, except biometric information.

For example, employers are the airport company, any sub-contractor companies, or airport authorities.

Airport authority is the unique legal authority in charge of granting access rights to restricted areas. This shall include enrolment activities. The airport authority is solely responsible for proofing (see ISO/IEC 24713-1, 6.2.1). Registration and issuance (see ISO/IEC 24713-1, 6.2) could be either directly managed by airport authority or only supervised by airport authority.

Privacy authority is an authority, strictly independent from airport authority, employers and also any employees lobbying association. Privacy authority is responsible for the supervision of biometric data protection in respect of the applicable laws or regulation. It should be noted that in some configurations, privacy officers are employees with a dedicated mission from the privacy authority.

NOTE Privacy/data protection requirements are outside the scope of this part of ISO/IEC 24713. However, in some jurisdictions a privacy authority may be put in place, dependent on local laws and regulations.

5.2 Architecture

The architecture of this specific employee profile can be broken down into four subsystems. The first is the token, which is the physical component, used by the individual worker to gain physical access to secure areas of the place of employment. The specification of the token is outside the scope of this part of ISO/IEC 24713. The second is a Token Management System (TMS) to manage the inventory, distribution, and revocation of the token. The third is the Command and Control System, which is the central database and security umbrella for the employee system. The fourth is the Command and Control Administration System, which is used for the administration of the operations. The infrastructure system to support the application binds the four elements above.

NOTE There may be other architectures with a different structure of subsystems, i.e. one where the token contains the biometric reference data and/or performs the verification (see ISO/IEC 7816-11).

5.3 Token

The token is the physical component that, in the possession of the Employee, shall provide authorized physical access within the airport restricted area. The token may also support multiple memory technologies including integrated circuit chip (ICC) memory, magnetic stripe, optical stripe and barcodes, as well as processing capabilities as provided within an ICC microprocessor. The token shall contain a unique token ID number. The biometric reference is typically stored in the token.

Depending on the command and control system design, the token is an element of security containing a biometric. Appropriate security evaluation of the token shall be considered. Security requirements for the token are out of the scope of this part of ISO/IEC 24713.

5.4 Token management system

The Token Management System is a system that handles the shipping, storage, printing, personalization, loading, processing, and revoking of the token. Processing within the Token Management System may include the following functions:

Applet loading

Manage requests

Handle volume printing

Track inventory

Test tokens

Biometric quality

Exception handling

Handle returns

Produce images

Handle encryption

Photograph capture that works with digital video capture device

Digital camera compatibility

Database maintenance including photograph storage

Magnetic stripe encoding

Barcode printing

Built-in token design capability

Token locking/unlocking

PKI encoding

Biometric encoding and storage

Open application program interface (API) for applet development

Smart-chip encoding

NOTE This list is not exhaustive, and some entries on this list are outside the scope of this part of ISO/IEC 24713.

5.5 Command and control system

The command and control system is the central database and security umbrella for the employee system. As a minimum, the central database shall contain the list of the valid and revoked token id numbers. It may also have several components including directory services, central communication, token information, and other information as deemed necessary by security requirements (as determined by the specific application). The biometric data may be stored in the central database, and linked to the token ID. The command and control system should also support claimed identity checks and other background check material. The command and control system shall provide the “watch list” function for tokens and should provide this function for individuals. The final component of the command and control system shall be a passive/active secure messaging system.

5.6 Command and control administration system

The command and control administration system monitors data integrity issues, actively monitors for attempted attacks on the system, enables or disables administrative control of the system and policy management, i.e., control over authentication policies, based on alert level. Further, this part of the system includes an override control in case of a terrorist or other attack.

5.7 Infrastructure system

The infrastructure incorporates biometric token terminals, wiring, door controls, wire status sensors, and access control products and services. Those elements of the system that are software oriented (i.e. can be changed in the field) should incorporate digital security technology to protect against system compromise.

6 Process

6.1 General

Clause 6 of ISO/IEC 24713-1 describes in detail the relationship between the biometric system and the application. The application defined by this part of ISO/IEC 24713 is access control for employees at airports. The process described below is the instantiation of the reference architecture. See also annex C for additional information. Indeed, as mentioned in the scope of this part of ISO/IEC 24713, this clause addresses business process for the support of token-based identity management.

An airport contains public areas, airport offices and restricted areas. Restricted area access is restricted to employees only. Restricted areas are delimited by security mechanisms, such as walls, gates, barriers, etc. Entry Gates to the access area shall be equipped with access control mechanisms, including biometric facilities for employees. Each area requires a level of privileges. For example, if a restricted area A is included in the restricted area B, then the privilege of A is higher than the privilege of B. If restricted area A and B have no “relation”, then privilege A and B have no access dependencies.

6.2 Proofing

When an employee applies or re-applies for a token, the process begins at a proofing and issuance station. Here, the worker will first produce a request for a token from his/her employer using the employer’s procedures. Claimed identity verification is then completed through a review of the documentation presented by the employee (photograph identity card, birth certificate, link to community, link to employer, etc).

This process is the first stage of the ID life-cycle (see ISO/IEC 24713-1). This process concerns only Employees (see description in clause 5.0). Physical identity can be claimed by documents. Documents are provided either by the Employee or by the Employer. Only the Airport Authority has the privilege to process the identity verification. The Privacy authority should be involved in this stage. As indicated in Part 1, biometrics may be used for background check.

NOTE The Employee may have a token, issued previously. This is due to managing identities throughout their lifetime.

6.3 Registration

Once claimed identity is proven, the biometric reference(s) and personal information is collected to initiate the background check process. As indicated in ISO/IEC 24713-1, biometrics may be used to perform a background check. Other screening measures, if required by the local facility, would also be administered at this time.

The data required by the token system is then entered into the enrolment record along with a digital photograph and biometric reference template. The biometric reference(s) will be selected from the list of reference technologies deemed suitable for identification (one-to-many) and verification (one-to-one) and specified in annex A. In the event of a lost token, see 6.5. The enrolment team should be trained to operate the biometric system efficiently to collect the biometric samples from the employees. The enrolment area and token storage area shall be secure area(s), with access control managed only by the airport authority.

The biometric sample may be encrypted and signed by the application (see A.7.2, item 2). The keys that are used to encrypt the biometric sample should be managed within the context of a suitable key management system, and a suitable certificate management system and private key management system should be used for effective biometric authentication.

In addition to a background check process, the system may provide a duplication check function to examine the biometric templates against previously enrolled biometric templates using biometric identification (1:N) to reduce the threat of alias identities in the system.

6.4 Issuance

The issuance stage, as described in ISO/IEC 24713-1, is the process of granting privilege and giving a credential. This stage is the next stage after registration (enrolment). If the previous stages are successfully completed, the enrolment information and a request are sent to a printing and personalization centre, where the token is prepared and printed, and the final personalization is completed. The token is then locked electronically and shipped to the appropriate enrolment and issuance centre. Notifications are then made to both the central administration and the individual, informing them that the token is ready for issuance.

The individual then returns to the Airport Authority, where the token is electronically unlocked; the biometric reference(s) is verified (1:1 check) to ensure the token is being issued to the same individual who applied; the data is validated; and the token is issued and the central administration is notified. The token issuance shall have a validity period. The validity period shall be determined by the Airport Authority.

6.5 Activation to a local access control system

Activation of the token takes place at each facility, where the individual requires access. Any transmission of the biometric shall be protected with encrypted and signed templates. When the individual arrives at the facility or the appropriate enrolment and issuance station, the employee presents the token and the reason for requesting access.

The worker's identity and background clearance status, if appropriate, are verified by the use of the biometric reference. This process is a validation as well as a security check. The access privilege decision is then made and the appropriate access to the facility is granted. The access privilege given to an individual is determined by the facility based on the established local security plan and the information verified by the token. If the local access control system is compatible with the token, the token is ready for use throughout the facility. If the systems are incompatible, the employee shall restart at the proofing stage to obtain a compatible token. Upon granting access to an employee, the facility notifies the central administration of the access privilege assigned and the individual’s record is updated.

6.6 Usage

An employee uses the issued token to gain access to one or more restricted areas within a local airport. The token must have been activated for the local airport and the employee granted authorization to enter the restricted area. The sequence of events during usage will be implementation dependent. A sample usage scenario is now presented (noting that this is one of a number of alternative ways of implementing the system):

At the access point to a restricted area, the employee presents the token to a biometric token terminal, for authentication. The employee identifier or token identifier is read from the token. The reference biometric(s) is read from the token or the central database. The system should ensure the validity and integrity of the data read from the token, through use of security techniques such as digital signatures, certificates or other cryptographic techniques and/or encryption. The employee is requested to present one or more biometric samples to a biometric capture device. Through these actions the employee is making a claim that they are a valid authorized user of the restricted area at that specific point in time.

The biometric reference(s) are compared against the biometric(s) submitted by the claimant. An authorization check is performed to confirm that the employee is allowed to access the restricted area and under the current conditions (e.g. time of day, employee work schedule, threat level, movement history). The biometric

