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)

© ISO/IEC 2008

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2008 – All rights reserved

Not for Resale

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Conformance 1

3 Normative references 2

4 Terms and definitions 3

5 Environment 6
5.1 Employees in the targeted environment 6
5.2 Architecture 6
5.3 Token 6
5.4 Token management system 7
5.5 Command and control system 7
5.6 Command and control administration system 8
5.7 Infrastructure system 8

6 Process 8
6.1 General 8
6.2 Proofing 8
6.3 Registration 8
6.4 Issuance 9
6.5 Activation to a local access control system 9
6.6 Usage 9

7 Security Considerations 10

Annex A (normative) **Requirements List** 12
A.1 General 12
A.2 Relationship between RL and corresponding ICS *proformas* 12
A.3 Profile Specific Implementation Conformance Statement 13
A.4 Instruction for completing the ICS *proforma* 13
A.4.1 General structure of the ICS *proforma* 13
A.4.2 Additional Information 13
A.4.3 Exception Information 13
A.5 ICS *proforma* 14
A.6 Interchange Formats 15
A.6.1 Finger Image Data (ISO/IEC 19794-4:2005) 15
A.6.2 Finger Minutiae Data (ISO/IEC 19794-2:2005) 16
A.6.3 Finger Pattern Spectral Data (ISO/IEC 19794-3:2006) 19
A.6.4 Face Image Data (ISO/IEC19794-5:2005) 21
A.6.5 Iris Image Data (ISO/IEC 19794-6:2005) 24
A.6.6 Signature/Sign Time Series Data (ISO/IEC 19794-7:2007) 25
A.6.7 Finger Pattern Skeletal Data (ISO/IEC 19794-8:2006) 27
A.6.8 Vascular Image Data (ISO/IEC 19794-9:2007) 31
A.6.9 Hand Geometry Silhouette Data (ISO/IEC 19794-10:2007) 33
A.7 Technical Interface Standards 34
A.7.1 BioAPI (ISO/IEC 19784-1:2006) 34
A.7.2 CBEFF (ISO/IEC 19785-1:2006) 39

Annex B (informative) **Additional information** 41

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C (informative) **Security Considerations** **44**
C.1 Approaches **44**
C.2 Representative threat list **44**
Bibliography **46**

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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*

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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*

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

verification and employee authorization check may take place in part or in full on the token, in the biometric token terminal, in an access control device or other attached processing device, or in a command and control system or other networked central location. The preferred locations for these operations will be implementation dependent.

If the system decides that the biometrics successfully matched and the employee is authorized for the area, then access will be granted. This may involve opening a door, gate, or other entrance.

There are several possible reasons why the token would no longer be valid. These include, but are not limited to, the following.

— The Employee declares to the Airport Authority or to the Employers that the token is lost.

— The Employee declares to the Airport Authority or to the Employers that the token is stolen.

— The Employer declares to the Airport Authority that contractual link with an Employee is cancelled.

— The Airport Authority has decided to revoke a token.

Any of the above events will result in the decision to revoke the token. Such decision will be taken based on the mandatory unique ID number of the token and will be invoked automatically upon expiration of the token, expiration or cancellation of the relationship that exists between the Airport Authority and the Employer. The actual procedure for revoking a token, independent of the reason, should take careful consideration to protect the privacy of those involved. The specific procedures for revocation, and the privacy considerations associated with such action, are out of scope of this part of ISO/IEC 24713.

When a token is revoked, the privileges associated with that token are locked. Additionally, the unique ID number of the token shall also be locked and shall not be re-used in the future. Denied attempts to an access area with a revoked token should be monitored by the Airport Authority. The unique ID of the token should be used to establish statistics on denied attempts. The biometric sample captured during a denied attempt may be transmitted and stored for further investigation.

The Employee who declares lost or stolen his/her token, would request and be issued with a new token in accordance with the procedures of the Airport Authority.

The Airport Authority can replace a valid token by a new valid token at any time and for any reason. On request of Employers or the Airport Authority, the validity period of a token may be updated. In this case, the unique ID number of the token would be maintained. The biometric reference may be replaced when the validity period is updated. Biometric data is managed as described in the enrolment stage (see 6.2). The procedure for updating the validity period is out of scope of this part of ISO/IEC 24713.

The Airport Authority should establish a procedure in the case where a genuine Employee applies his/her valid token to request his/her privileges and the access privileges are not granted due to any failure (for example, due to False Rejection). The content of such a procedure is outside the scope of this part of ISO/IEC 24713.

The keys provisioned on the reader 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.

7 Security Considerations

This section describes general concepts of security applied for a Biometric authentication system, including approaches and profiles. See also annex D for a concrete example.

When an access control system for employees at an airport is deployed, then sensors and associated equipment should be certified in accordance with local regulations, taking into account environmental testing in the case of outdoor applications.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex D describes general concepts of security that could be applied for a Biometric authentication system, including approaches and profiles. Annex D is an example that is not inclusive but intended as a starting point for security considerations.

Liveness detection in a biometric system ensures that only fingerprints, facial images, irises, and other characteristics directly derived from the person requesting verification of such a characteristic are capable of generating valid biometric templates. For further information on liveness detection, see Annex C.

Performance of a Physical Access Control system for Employees at Airports is driven by security requirements. Performance evaluation shall be done in accordance with ISO/IEC 19795-1 and ISO/IEC 19795-2.

Typical performance parameters to be specified include:

FAR;

FRR;

FTE;

FTA.

The range of values for each parameter is managed by country legal authorities of Civil Aviation and local airports.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(normative)

Requirements List

A.1 General

Use of this part of ISO/IEC 24713 imposes requirements on the implementation that go beyond those of the base standards referred to by this part of ISO/IEC 24713. These result in modifications to the requirements expressed in the base standards. This annex specifies the modifications (the Requirements List - RL) that apply to the status of the items affected in each Implementation Conformance Statement (ICS) *proforma*, with consequently modified requirements on the answers to be provided.

The status notation used in this annex is that defined in ISO/IEC 9646-7. In summary, the meaning of the notations is as follows and in each case the base standard defines the content or behaviour of the implementation:

M Mandatory - the capability is required to be supported. In the case of values, the base standards define the content of the required element. In the case of functions, the base standard defines the required behaviour of the implementation.

N/A Not Applicable - in the given context, it is impossible to use the capability.

O Optional - the capability may be supported or not. If supported: in the case of values, the base standards define the content of the optional element; in the case of functions, the base standards define the required behaviour of the implementation.

O.i qualified optional - for mutually exclusive or selectable options from a set. "i" is an integer that identifies an unique group of related optional items and the logic of their selection, defined below the table.

X The use of this function is under the control of the application and may be subject to local agreement.

The Requirements List in this annex shall be used to restrict the permitted support answers in the corresponding ICS.

A.2 Relationship between RL and corresponding ICS *proformas*

In the context of the profile specification contained in this part of ISO/IEC 24713, ICS *proformas* of the base standards contain tables in 3 categories. The 3 categories are:

— those *proforma* tables where this profile does not restrict the permitted support answers;

— those *proforma* tables where this profile restricts the permitted support answers;

— those *proforma* tables that are not relevant to this profile.

The Requirements List consists of the tables falling into the second category, with an indication of the modified items in those tables.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.3 Profile Specific Implementation Conformance Statement

The supplier of a profile implementation that is claimed to conform to this part of ISO/IEC 24713 shall complete the Profile specific Implementation Conformance Statement (ICS) proforma contained in this annex for those items for which implementation and conformance is claimed. All others shall be ignored.

A completed Profile specific ICS *proforma* is the ICS for the implementation in question. The ICS is a statement of which capabilities and options of the profile have been implemented. The ICS can have a number of uses, including use:

— by the profile implementer, as a check list to reduce the risk of failure to conform to the standard through oversight;

— by the supplier and acquirer (or potential acquirer) of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard ICS *proforma*;

— by the user (or potential user) of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking cannot be guaranteed, failure to interwork can often be predicted from incompatible ICS);

— by a tester, as the basis for selecting appropriate test suites against which to assess the claim for conformance of the implementation.

A.4 Instruction for completing the ICS *proforma*

A.4.1 General structure of the ICS *proforma*

The ICS *proforma* is a fixed format questionnaire divided into formats each containing a group of individual items. Each item is identified by an item number, the name of the item (question to be answered), and the reference(s) to either the base standard, or a specific clause in a base standard, or specifying the item in the main body of this part of ISO/IEC 24713 (if no base standard is listed in the reference column).

Answers to the questionnaire items are to be provided in the “Support” column, by simply marking an answer to indicate a restricted choice support

Refer to the tables below when completing this form to determine whether an item is mandatory or optional for the implementation type supplying.

A.4.2 Additional Information

Items of Additional information allow a supplier to provide further information intended to assist the interpretation of the ICS. It is not intended or expected that a large quantity will be supplied, and an ICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations.

References to items of Additional information may be entered next to any answer in the questionnaire, and may be included in items of Exception Information.

A.4.3 Exception Information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirements. No pre-printed answer will be found in the Support column for this. Instead, the supplier is required to write into the support column an x.<i> reference to an item of Exception Information, and to provide the appropriate rationale in the Exception item itself.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

An implementation for which an Exception item is required in this way does not conform to this part of ISO/IEC 24713. A possible reason for the situation described above is that a defect in the standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

A.5 ICS *proforma*

Supplier	
Contact point for queries about the ICS	
Implementation Name(s)and Version(s) (NOTE)	
Other information necessary for full Identification; e.g. name(s)and version(s)for machines and/or operating systems; system name(s)	
Have any exception items been required?	No [ ] Yes [ ] (The answer Yes means that the implementation does not conform to this part of ISO/IEC 24713)
Date of Statement	

NOTE The terms "Name" and "Version" should be interpreted appropriately to correspond with a supplier's terminology (e.g., Type, Series, Model).

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6 Interchange Formats

A.6.1 Finger Image Data (ISO/IEC 19794-4:2005)

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
1	Bit and Byte Ordering	6.1	M	M	[yes]		M	[yes]		M	[yes]
2	Scan Sequence	6.2	M	M	[yes]		M	[yes]		M	[yes]
3	Image Acquisition Requirements – (see Note 1)	7	O	M Image Level ≥30	[yes,N/A]		M Image Level ≥ 20	[yes,N/A]		M Image Level ≥ 20	[yes,N/A]
4	Pixel Aspect Ratio	7.2	M	M	[yes]		M	[yes]		M	[yes]
5	Pixel Depth	7.3	M	M	[yes]		M	[yes]		M	[yes]
6	Greyscale Data	7.4	M	M	[yes]		M	[yes]		M	[yes]
7	Dynamic Range	7.5	M	M	[yes]		M	[yes]		M	[yes]
8	Scan Resolution	7.6	M	M	[yes]		M	[yes]		M	[yes]
9	Image Resolution	7.7	M	M	[yes]		M	[yes]		M	[yes]
10	Finger Image Location	7.8	M	M	[yes]		M	[yes]		M	[yes]
11	Finger Image Record Format	8	M	M	[yes]		M	[yes]		M	[yes]
12	General Record Header	8.2	M	M	[yes]		M	[yes]		M	[yes]
13	Image Compression Algorithm (see Note 2)	8.2.14	O	M Algorithm = 2	[yes,N/A]		M Algorithm = any	[yes,N/A]		M Algorithm = any	[yes,N/A]
14	Finger Record header	8.3	M	M	[yes]		M	[yes]		M	[yes]

NOTE 1 Image Acquisition requirements (Image Level $\geqslant$ 30) is required for enrolment to obtain an image of at least 500 pixels. Whereas the lesser image level (Image Level $\geqslant$ 20) may be used and is acceptable for identification and verification, it is recommended that the greater image level be used for these functions.

NOTE 2 Image Compression Algorithm (2) is required for Image Level $\geqslant$ 30 and Image Compression Algorithm (any) may be used for all other image levels except Image Level $\geqslant$ 30

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6.2 Finger Minutiae Data (ISO/IEC 19794-2:2005)

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
1	Finger minutiae point location	6.3	M	M	[yes]		M	[yes]		M	[yes]
2	Coordinate location	6.3.1	M	M	[yes]		M	[yes]		M	[yes]
3	Minutia placement on ridge ending	6.3.2	M	M	[yes]		M	[yes]		M	[yes]
4	Minutia placement on ridge bifurcation	6.3.3	M	M	[yes]		M	[yes]		M	[yes]
5	Minutia placement on ridge skeleton	6.3.4	M	M	[yes]		M	[yes]		M	[yes]
6	Minutia placement on other minutia types	6.3.5	M	M	[yes]		M	[yes]		M	[yes]
7	Angle conventions	6.4.1	M	M	[yes]		M	[yes]		M	[yes]
8	Direction of a ridge ending	6.4.2	M	M	[yes]		M	[yes]		M	[yes]
9	Direction of a ridge bifurcation	6.4.3	M	M	[yes]		M	[yes]		M	[yes]
10	Direction of a ridge skeletal end point	6.4.4	M	M	[yes]		M	[yes]		M	[yes]
11	Core and delta placement and direction	6.5	M	M	[yes]		M	[yes]		M	[yes]
12	Minutia type matching	6.6	M	M	[yes]		M	[yes]		M	[yes]
13	Encoding of multibyte quantities	6.7	M	M	[yes]		M	[yes]		M	[yes]
14	Finger minutiae record organization	7.2	M	M	[yes]		M	[yes]		M	[yes]
11	Record header	7.3	M	M	[yes]		M	[yes]		M	[yes]
12	Format Identifier	7.3.1	M	M	[yes]		M	[yes]		M	[yes]

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
13	Version number	7.3.2	M	M	[yes]		M	[yes]		M	[yes]
14	Length of record	7.3.3	M	M	[yes]		M	[yes]		M	[yes]
15	Capture Equipment certification	7.3.4	M	M	[yes]		M	[yes]		M	[yes]
16	Capture Equipment ID	7.3.5	M	M	[yes]		M	[yes]		M	[yes]
17	Size of scanned image in X direction	7.3.6	M	M	[yes]		M	[yes]		M	[yes]
18	Size of scanned image in Y direction	7.3.7	M	M	[yes]		M	[yes]		M	[yes]
19	X (horizontal) resolution	7.3.8	M	M	[yes]		M	[yes]		M	[yes]
20	Y (horizontal) resolution	7.3.9	M	M	[yes]		M	[yes]		M	[yes]
21	Number of finger views	7.3.10	M	M	[yes]		M	[yes]		M	[yes]
22	Reserved byte	7.3.11	M	M	[yes]		M	[yes]		M	[yes]
23	Single finger record format	7.4	M	M	[yes]		M	[yes]		M	[yes]
24	Finger header	7.4.1	M	M	[yes]		M	[yes]		M	[yes]
25	Finger minutia data	7.4.2	M	M	[yes]		M	[yes]		M	[yes]
26	Extended data	7.5	O	O	[yes,no]		O	[yes,no]		O	[yes,no]
27	Common extended data fields	7.5.1	O	O	[yes,no]		O	[yes,no]		O	[yes,no]
28	Ridge count data format	7.5.2	O	O.1	[yes,no]		O.1	[yes,no]		O.1	[yes,no]
29	Core and delta data format	7.5.3	O	O.2	[yes,no]		O.2	[yes,no]		O.2	[yes,no]
30	Zonal quality data	7.5.4	O	O.2	[yes,no]		O.2	[yes,no]		O.2	[yes,no]
31	Minutiae record format summary	7.6	M	M	[yes]		M	[yes]		M	[yes]

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement								
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
32	Finger minutia card format	8	O	M	[yes]		M	[yes]		M	[yes]
33	CBEFF Format owner and format types	9	M	M	[yes]		M	[yes}		M	[yes]

NOTE 1 Options denoted “O.1” are related to the optional ridge count information, and should appear or be used together.

NOTE 2 Options denoted “O.2” are related to the optional core and delta information, and should appear or be used together.

Additional requirements for the use of this format are identified below to apply to implementations claiming conformance with this part of ISO/IEC 24713:

1. Extended Data shall not be used to specify a proprietary Minutiae format in order to bypass the mandatory functions of this part of ISO/IEC 24713.

2. Minutiae that represent endings of a friction ridge shall be encoded as “ridge ending”, and minutiae that represent divisions of a friction ridge into two ridges shall be encoded as “bifurcation”. The “Other” minutiae type shall be used for minutiae whose type is either ridge ending or bifurcation, but where the encoding application is unsure of the type.

3. If ridge counts are used, they shall be derived in the following manner. If 4-neighbor ridge counts are used, the quadrants shall be bounded by the angles 45, 135, 225, and 315 degrees. If 8-neighbor ridge counts are used, the octants shall be 45 degrees wide, forming a theoretical circle centred on the location of the minutia.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6.3 Finger Pattern Spectral Data (ISO/IEC 19794-3:2006)

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
1	Format Identifier	8.1.1	M	M	[yes]		M	[yes]		M	[yes]
2	Version Number	8.1.2	M	M	[yes]		M	[yes]		M	[yes]
3	Length of Record	8.1.3	M	M	[yes]		M	[yes]		M	[yes]
5	Number of single finger Records	8.1.4	M	M	[yes]		M	[yes]		M	[yes]
6	x (horizontal) resolution	8.1.5	M	M	[yes]		M	[yes]		M	[yes]
7	y (vertical) resolution	8.1.6	M	M	[yes]		M	[yes]		M	[yes]
8	Number of Cells in x-direction	8.1.7	M	M	[yes]		M	[yes]		M	[yes]
9	Number of Cells in y-direction	8.1.8	M	M	[yes]		M	[yes]		M	[yes]
10	Number of Pixels in Cells in x-direction	8.1.9	M	M	[yes]		M	[yes]		M	[yes]
11	Number of Pixels in Cells in y-direction	8.1.10	M	M	[yes]		M	[yes]		M	[yes]
12	Cellular x-offset	8.1.11	M	M	[yes]		M	[yes]		M	[yes]
13	Cellular y-offset	8.1.12	M	M	[yes]		M	[yes]		M	[yes]
14	Spectral component selection method	8.1.13	M	M	[yes]		M	[yes]		M	[yes]
15	Type of window	8.1.14	M	M	[yes]		M	[yes]		M	[yes]
16	Standard deviation	8.1.15	M	M	[yes]		M	[yes]		M	[yes]
17	Number of frequencies	8.1.16	M	M	[yes]		M	[yes]		M	[yes]
18	Frequencies	8.1.17	M	M	[yes]		M	[yes]		M	[yes]
19	Number of orientations	8.1.18	M	M	[yes]		M	[yes]		M	[yes]
20	Number of spectral components to be retained	8.1.19	M	M	[yes]		M	[yes]		M	[yes]
21	Bit-depth of propagation Angle	8.1.20	M	M	[yes]		M	[yes]		M	[yes]
22	Bit-depth of Wavelength	8.1.21	M	M	[yes]		M	[yes]		M	[yes]
23	Bit-depth of phase	8.1.22	M	M	[yes]		M	[yes]		M	[yes]
24	Bit-depth of magnitude	8.1.23	M	M	[yes]		M	[yes]		M	[yes]

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
25	Bit-depth of quality score	8.1.24	M	M	[yes]		M	[yes]		M	[yes]
26	Cell quality group granularity	8.1.25	M	M	[yes]		M	[yes]		M	[yes]
27	Reserved Bytes	8.1.26	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
28	Single finger record	8.2	M	M	[yes]		M	[yes]		M	[yes]
29	Header	8.2.1	M	M	[yes]		M	[yes]		M	[yes]
30	Finger pattern spectral data block	8.2.2	M	M	[yes]		M	[yes]		M	[yes]
31	Extended data block	8.2.3	M	M	[yes]		M	[yes]		M	[yes]
32	Finger pattern spectral data card format	9	M	M	[yes]		M	[yes]		M	[yes]

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6.4 Face Image Data (ISO/IEC19794-5:2005)

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	Question/ Feature	Base Ref.	Base Standard Status	Profile Status enrolment	ICS Support		Profile Status identification	ICS Support		Profile Status verification	ICS Support
1	Byte Ordering	5.2.1	M	M	[yes]		M	[yes]		M	[yes]
2	CBEFF Header	5.3	M	M	[yes]		M	[yes]		M	[yes]
3	Format Identifier	5.4.1	M	M	[yes]		M	[yes]		M	[yes]
4	Version Number	5.4.2	M	M	[yes]		M	[yes]		M	[yes]
5	Record Length	5.4.3	M	M	[yes]		M	[yes]		M	[yes]
6	Number of Facial Images	5.4.4	M	M	[yes]		M	[yes]		M	[yes]
7	Facial record data Length	5.5.1	M	M	[yes]		M	[yes]		M	[yes]
8	Number of Feature Points	5.5.2	M	M	[yes]		M	[yes]		M	[yes]
9	Gender	5.5.3	M	M	[yes]		M	[yes]		M	[yes]
10	Eye Colour	5.5.4	M	M	[yes]		M	[yes]		M	[yes]
11	Hair Colour	5.5.5	M	M	[yes]		M	[yes]		M	[yes]
12	Feature Mask	5.5.6	M	M	[yes]		M	[yes]		M	[yes]
13	Expression	5.5.7	M	M	[yes]		M	[yes]		M	[yes]
14	Pose Angle Yaw	5.5.8.1	M	M	[yes]		M	[yes]		M	[yes]
15	Pose Angle Pitch	5.5.8.2	M	M	[yes]		M	[yes]		M	[yes]
16	Pose Angle Roll	5.5.8.3	M	M	[yes]		M	[yes]		M	[yes]
17	Pose Angle Uncertainty	5.5.9	M	M	[yes]		M	[yes]		M	[yes]
18	Feature Point Type	5.6.1	M	M	[yes]		M	[yes]		M	[yes]
19	Feature Point Code	5.6.2	M	M	[yes]		M	[yes]		M	[yes]
20	MPEG4 feature points	5.6.3	M	M	[yes]		M	[yes]		M	[yes]
21	Eye and nostril centre feature points	5.6.4	M	M	[yes]		M	[yes]		M	[yes]
22	Facial Image Type	5.7.1	M	M	[yes]		M	[yes]		M	[yes]
23	Image Data Type	5.7.2	M	M	[yes]		M	[yes]		M	[yes]
24	Width	5.7.3	M	M	[yes]		M	[yes]		M	[yes]
25	Height	5.7.4	M	M	[yes]		M	[yes]		M	[yes]
26	Image Colour Space	5.7.5	M	M	[yes]		M	[yes]		M	[yes]
27	Source type	5.7.6	M	M	[yes]		M	[yes]		M	[yes]
28	Device type	5.7.7	M	M	[yes]		M	[yes]		M	[yes]
29	Quality	5.7.8	M	M	[yes]		M	[yes]		M	[yes]
30	Image Data Structure	5.8.1	M	M	[yes]		M	[yes]		M	[yes]

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	Question/ Feature	Base Ref.	Base Standard Status	Profile Status enrolment	ICS Support		Profile Status identification	ICS Support		Profile Status verification	ICS Support
31	Inheritance requirements for basic face image type	6.1	M	M	[yes|		M	[yes|		M	[yes|
32	Data encoding requirements	6.2	M	M	[yes|		M	[yes|		M	[yes|
33	Data compression requirements	6.3	M	M	[yes|		M	[yes|		M	[yes|
34	Format requirements for Basic Face Image	6.4	M	M	[yes|		M	[yes|		M	[yes|
35	Facial header	6.4.1	M	M	[yes|		M	[yes|		M	[yes|
36	Facial Information	6.4.2	M	M	[yes|		M	[yes|		M	[yes|
37	Image information	6.4.3	M	M	[yes|		M	[yes|		M	[yes|
38	Pose	7.2.2	M.1 M.2	M.1,M.2	[yes|		N/A	[n/a]		N/A	[n/a]
39	Expression	7.2.3	O.1,O.2	M.1,M.2	[yes|		N/A	[n/a]		N/A	[n/a]
40	Assistance in Positioning the Face	7.2.4	M.1 M.2	M	[yes|		N/A	[n/a]		N/A	[n/a]
41	Shoulders	7.2.5	M.1 M.2	M.1,M.2	[yes|		N/A	[n/a]		N/A	[n/a]
42	Backgrounds	7.2.6	O.1,O.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
43	Subject and Scene Lighting	7.2.7	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
44	Shadows over the Face	7.2.8	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
45	Shadows in Eye Sockets	7.2.9	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
46	Hot Spots	7.2.10	O.1,O.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
47	Eye Glasses	7.2.11	O.1,O.2	M.1,M.2	[yes|		N/A	[n/a]		N/A	[n/a]
48	Eye Patches	7.2.12	O.1,O.2	M.1,M.2	[yes|		N/A	[n/a]		N/A	[n/a]
49	No Over or Under Exposure	7.3.2	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
50	Focus and Depth of Field	7.3.3	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
51	Unnatural Colour	7.3.4	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
52	Colour or Greyscale Enhancement	7.3.5	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
53	Radial Distortion of the Camera Lens	7.3.6	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
54	Pixel Aspect Ratio	7.4.1.1	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
55	Origin at Upper Left	7.4.1.2	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
56	Greyscale Density	7.4.2.1	O.1,O.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
57	Colour Saturation	7.4.2.2	O.1,O.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
58	Colour Space	7.4.2.3	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|
59	Video Interlacing	7.4.3	M.1 M.2	M.1,M.2	[yes|		M.1,M.2	[yes|		M.1,M.2	[yes|

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
60	Horizontally centred face	8.3.2	M.1	M.1	[yes|		N/A	[n/a]		N/A	[n/a]
61	Vertical position of the face	8.3.3	M.1	M.1	[yes|		N/A	[n/a]		N/A	[n/a]
62	Width of Head	8.3.4	M.1	M.1	[yes|		N/A	[n/a]		N/A	[n/a]
63	Length of Head	8.3.5	M.1	M.1	[yes|		N/A	[n/a]		N/A	[n/a]
64	Full Frontal image resolution	8.4.1	M.1	M.1	[yes|		N/A	[n/a]		N/A	[n/a]
65	Token Image Eye Positions	9.2.2	O	N/A	[n/a]		N/A	[n/a]		O.2	[yes, no]
66	Token Image Geometric Format	9.2.3	O	N/A	[n/a]		N/A	[n/a]		O.2	[yes, no]
67	Minimum Width Token Image	9.2.4	O	N/A	[n/a]		N/A	[n/a]		O.2	[yes, no]
68	Token Image Padding	9.2.5	O	N/A	[n/a]		N/A	[n/a]		O.2	[yes, no]
69	Inheritance requirements	9.3.1	M	M	[yes]		M	[yes]		M	[yes]
70	Image information	9.3.2	M	M	[yes]		M	[yes]		M	[yes]

NOTE 1 Options denoted “O.1” are related to the frontal image type, and should appear or be used together.

NOTE 2 Options denoted “O.2” are related to the token image type, and should appear or be used together.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6.5 Iris Image Data (ISO/IEC 19794-6:2005)

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
1	Iris image format - general	6.1	M	M	[yes]		M	[yes]		M	[yes]
2	Image compression	6.2	M	M	[yes]		M	[yes]		M	[yes]
3	Iris image pre-processing	6.3	M	M	[yes]		M	[yes]		M	[yes]
4	Iris image data record	6.4	M	M	[yes]		M	[yes]		M	[yes]
5	Iris header structures	6.5	M	M	[yes]		M	[yes]		M	[yes]
6	Image quality	A.1	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
7	Greyscale density	A.2	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
8	Illumination	A.3	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
9	Contrast	A.4	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
10	Visible iris	A.5	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
11	Pixel aspect ratio	A.6	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
12	Image scale	A.7	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
13	Optical distortion	A.8	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
14	Noise	A.9	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
15	Image orientation	A.10	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
16	Presentation	A.11	O	O	[yes, no]		O	[yes, no]		O	[yes, no]

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6.6 Signature/Sign Time Series Data (ISO/IEC 19794-7:2007)

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
1	Pen position channels	6.2	M	M	[yes]		M	[yes]		M	[yes]
2	Pen velocity channels	6.3	O	O	[yes]		O	[yes]		O	[yes]
3	Pen acceleration channels	6.4	O	O	[yes]		O	[yes]		O	[yes]
4	Time channel	6.5	O	O	[yes]		O	[yes]		O	[yes]
5	Time difference channel	6.6	O	O	[yes]		O	[yes]		O	[yes]
6	Pen tip force channel	6.7	O	O	[yes]		O	[yes]		O	[yes]
7	Tip switch state channel	6.8	O	O	[yes]		O	[yes]		O	[yes]
8	Pen orientation channel	6.9	O	O	[yes]		O	[yes]		O	[yes]
9	Record Format Identifier	7.3.2	M	M/na.1	[yes]		M/na.1	[yes]		M/na.1	[yes]
10	Standard Version Number	7.3.3	M	M/na.1	[yes]		M/na.1	[yes]		M/na.1	[yes]
11	Channel descriptions	7.3.4	M	M/na.1	[yes]		M/na.1	[yes]		M/na.1	[yes]
12	Reserved Octet	7.3.5	M	M/na.1	[yes]		M/na.1	[yes]		M/na.1	[yes]
13	Record body	7.4	M	M/na.1	[yes]		M/na.1	[yes]		M/na.1	[yes]
14	Sequence of sample points	7.4.2	M	M/na.1	[yes]		M/na.1	[yes]		M/na.1	[yes]
15	Extended data	7.4.3	M	M/na.1	[yes]		M/na.1	[yes]		M/na.1	[yes]
16	Reserved byte	6.4.7	M	M/na.1	[yes]		M/na.1	[yes]		M/na.1	[yes]
17	Compact format	8	O	O/M.1	[yes]		O/M.1	[yes]		O/M.1	[yes]
18	Matching algorithm parameters template	8.2	O	O/M.1	[yes, no]		O/M.1	[yes, no]		O/M.1	[yes, no]
19	Embedment in a CBEFF data structure	8.3	O	O/M.1	[yes, no]		O/M.1	[yes, no]		O/M.1	[yes, no]

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
20	BDB body	8.4	O	O/M.1	[yes, no]		O/M.1	[yes, no]		O/M.1	[yes, no]
21	Sequence of sample points	8.4.2	O	O/M.1	[yes, no]		O/M.1	[yes, no]		O/M.1	[yes, no]
22	`Extended data	8.4.3	O	O	[yes]		O	[yes]		O	[yes]

NOTE 1 Entries marked M/na.1 are mandatory if the biometric reference is not stored on a token and are not applicable if the biometric reference is stored on a token.

NOTE 2 Entries marked O/M.1 are optional if the biometric reference is not stored on a token and are mandatory if the biometric reference is stored on a token.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6.7 Finger Pattern Skeletal Data (ISO/IEC 19794-8:2006)

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
1	Minutiae type	6.1.1	M	M	[yes]		M	[yes]		M	[yes]
2	Finger minutiae point location	6.1.2	M	M	[yes]		M	[yes]		M	[yes]
3	Coordinate location	6.1.2	M	M	[yes]		M	[yes]		M	[yes]
4	Angle convention	6.1.3	M	M	[yes]		M	[yes]		M	[yes]
5	Direction code	6.2.1	M	M	[yes]		M	[yes]		M	[yes]
6	General skeleton line encoding rules	6.2.2	M	M	[yes]		M	[yes]		M	[yes]
7	Constructing direction elements	6.2.3	M	M	[yes]		M	[yes]		M	[yes]
8	Finger pattern record organization	7.2	M	M	[yes]		M	[yes]		M	[yes]
9	Record header	7.3	M	M	[yes]		M	[yes]		M	[yes]
10	Format identifier	7.3.1	M	M	[yes]		M	[yes]		M	[yes]
11	Version number	7.3.2	M	M	[yes]		M	[yes]		M	[yes]
12	Length of record	7.3.3	M	M	[yes]		M	[yes]		M	[yes]
13	Capture device ID	7.3.4	M	M	[yes]		M	[yes]		M	[yes]
14	Number of finger pattern in record	7.3.5	M	M	[yes]		M	[yes]		M	[yes]
15	Resolution of scaled image	7.3.6	M	M	[yes]		M	[yes]		M	[yes]
16	Bit-depth of coordinates	7.3.7	M	M	[yes]		M	[yes]		M	[yes]
17	Bit-depth of start and stop directions	7.3.8	M	M	[yes]		M	[yes]		M	[yes]
18	Bit-depth of direction in direction code	7.3.9	M	M	[yes]		M	[yes]		M	[yes]

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
19	Step size of direction code	7.3.10	M	M	[yes]		M	[yes]		M	[yes]
20	Relative perpendicular step size	7.3.11	M	M	[yes]		M	[yes]		M	[yes]
21	Number of directions on 180°	7.3.12	M	M	[yes]		M	[yes]		M	[yes]
22	Finger view header	7.4.1	M	M	[yes]		M	[yes]		M	[yes]
23	View number	7.4.2	M	M	[yes]		M	[yes]		M	[yes]
24	Finger position	7.4.3	M	M	[yes]		M	[yes]		M	[yes]
25	Impression type	7.4.4	M	M	[yes]		M	[yes]		M	[yes]
26	Finger quality	7.4.5	M	M	[yes]		M	[yes]		M	[yes]
27	Image size in X	7.4.6	M	M	[yes]		M	[yes]		M	[yes]
28	Image size in Y	7.4.7	M	M	[yes]		M	[yes]		M	[yes]
29	Length of skeletal data	7.4.8	M	M	[yes]		M	[yes]		M	[yes]
30	Finger pattern skeletal data	7.4.9	M	M	[yes]		M	[yes]		M	[yes]
31	Extended data	7.5	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
32	Common extended data fields	7.5.1	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
33	Extended data block length	7.5.1.1	M	M	[yes]		M	[yes]		M	[yes]
34	Type identification code	7.5.1.2	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
35	Length of data	7.5.1.3	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
36	Data area	7.5.1.4	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
37	Ridge count data format	7.5.2	O	O.1	[yes, no]		O.1	[yes, no]		O.1	[yes, no]
38	Ridge count extraction method	7.5.2.1	O	O.1	[yes, no]		O.1	[yes, no]		O.1	[yes, no]
39	Ridge count data	7.5.2.2	O	O.1	[yes, no]		O.1	[yes, no]		O.1	[yes, no]

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	Question/ Feature	Base Ref.	Base Standard Status	Profile Status enrolment	ICS Support		Profile Status identification	ICS Support		Profile Status verification	ICS Support
40	Core and delta format	7.5.3	O	O.2	[yes, no]		O.2	[yes, no]		O.2	[yes, no]
41	Number of cores	7.5.3.1	O	O.2	[yes, no]		O.2	[yes, no]		O.2	[yes, no]
42	Core information type	7.5.3.2	O	O.2	[yes, no]		O.2	[yes, no]		O.2	[yes, no]
43	Core position	7.5.3.3	O	O.2	[yes, no]		O.2	[yes, no]		O.2	[yes, no]
44	Core angle	7.5.3.4	O	O.2	[yes, no]		O.2	[yes, no]		O.2	[yes, no]
45	Number of deltas	7.5.3.5	O	O.2	[yes, no]		O.2	[yes, no]		O.2	[yes, no]
46	Delta information type	7.5.3.6	O	O.2	[yes, no]		O.2	[yes, no]		O.2	[yes, no]
47	Delta position	7.5.3.7	O	O.2	[yes, no]		O.2	[yes, no]		O.2	[yes, no]
48	Delta angles	7.5.3.8	O	O.2	[yes, no]		O.2	[yes, no]		O.2	[yes, no]
49	Zonal quality data	7.5.4	O	O.3	[yes, no]		O.3	[yes, no]		O.3	[yes, no]
50	Cell width and height	7.5.4.1	O	O.3	[yes, no]		O.3	[yes, no]		O.3	[yes, no]
51	Cell quality information depth	7.5.4.2	O	O.3	[yes, no]		O.3	[yes, no]		O.3	[yes, no]
52	Cell quality data	7.5.4.3	O	O.3	[yes, no]		O.3	[yes, no]		O.3	[yes, no]
53	Pore position data	7.5.5	O	O.4	[yes, no]		O.4	[yes, no]		O.4	[yes, no]
54	Pore position resolution	7.5.5.1	O	O.4	[yes, no]		O.4	[yes, no]		O.4	[yes, no]
55	Pore distance information depth	7.5.5.2	O	O.4	[yes, no]		O.4	[yes, no]		O.4	[yes, no]
56	Pore position description	7.5.5.3	O	O.4	[yes, no]		O.4	[yes, no]		O.4	[yes, no]
57	Skeleton structural data	7.5.6	O	O.5	[yes, no]		O.5	[yes, no]		O.5	[yes, no]
58	Normal size finger pattern skeletal format	8.1	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
59	Compact size finger pattern skeletal format	8.2	O	O	[yes, no]		O	[yes, no]		O	[yes, no]

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
60	Skeleton image size in X and Y	8.3.1	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
61	X or Y coordinate extension for compact card format	8.4	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
62	Usage of additional features for the card format	8.5	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
63	Comparison parameters and card capabilities	8.6	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
64	CBEFF format owner and format types	9	M	M	[yes, no]		M	[yes, no]		M	[yes, no]

NOTE 1 Options denoted “O.1” are related to the optional ridge count information, and should appear or be used together.

NOTE 2 Options denoted “O.2” are related to the optional core and delta information, and should appear or be used together.

NOTE 3 Options denoted “O.3” are related to the optional pore position information, and should appear or be used together.

NOTE 4 Options denoted “O.4” are related to the optional cell quality information, and should appear or be used together.

NOTE 5 Options denoted “O.5” are related to the optional skeleton structural information, and should appear or be used together.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6.8 Vascular Image Data (ISO/IEC 19794-9:2007)

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
1	Byte and bit ordering	6.1	M	M	[yes]		M	[yes]		M	[yes]
2	Scan sequence	6.2	M	M	[yes]		M	[yes]		M	[yes]
3	Spatial resolution	7.1	M	M	[yes]		M	[yes]		M	[yes]
4	Gray scale depth	7.2	M	M	[yes]		M	[yes]		M	[yes]
5	Illumination	7.3	M	M	[yes]		M	[yes]		M	[yes]
6	Pixel aspect ration	7.4	M	M	[yes]		M	[yes]		M	[yes]
7	Normalization of projection	7.5	M	M	[yes]		M	[yes]		M	[yes]
8	Image storage format	7.6	M	M	[yes]		M	[yes]		M	[yes]
9	Imaging area	7.7	M	M	[yes]		M	[yes]		M	[yes]
10	Standard pose	7.8	M	M	[yes]		M	[yes]		M	[yes]
11	Object coordinate system	7.9	M	M	[yes]		M	[yes]		M	[yes]
12	Vascular image data block	8.1	M	M	[yes]		M	[yes]		M	[yes]
13	Vascular image record header	8.2	M	M	[yes]		M	[yes]		M	[yes]
14	Vascular image header	8.3	M	M	[yes]		M	[yes]		M	[yes]
15	Image type	8.3.1	M	M	[yes]		M	[yes]		M	[yes]
16	Vascular image record length	8.3.2	M	M	[yes]		M	[yes]		M	[yes]
17	Image width and height	8.3.3	M	M	[yes]		M	[yes]		M	[yes]
18	Gray scale depth	8.3.4	M	M	[yes]		M	[yes]		M	[yes]
19	Image position and property bit field	8.3.5	M	M	[yes]		M	[yes]		M	[yes]

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
20	Rotation angle	8.3.6	O	O	[yes,no]		O	[yes,no]		O	[yes,no]
21	Image format	8.3.7	M	M	[yes]		M	[yes]		M	[yes]
22	Illumination type	8.3.8	O	O	[yes,no]		O	[yes,no]		O	[yes,no]
23	Image background	8.3.9	O	O	[yes,no]		O	[yes,no]		O	[yes,no]
24	Horizontal scan resolution	8.3.10	O	O	[yes,no]		O	[yes,no]		O	[yes,no]
25	Vertical scan resolution	8.3.11	O	O	[yes,no]		O	[yes,no]		O	[yes,no]
26	Pixel aspect ratio	8.3.12	O	O	[yes,no]		O	[yes,no]		O	[yes,no]

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6.9 Hand Geometry Silhouette Data (ISO/IEC 19794-10:2007)

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
1	Format identifier	7.1.1	M	M	[yes]		M	[yes]		M	[yes]
2	Version number	7.1.2	M	M	[yes]		M	[yes]		M	[yes]
3	Record length	7.1.3	M	M	[yes]		M	[yes]		M	[yes]
4	Number of HGVRs	7.1.4	M	M	[yes]		M	[yes]		M	[yes]
5	Reserved	7.1.5	M	M	[yes]		M	[yes]		M	[yes]
6	Length of HGVR	7.2.1	M	M	[yes]		M	[yes]		M	[yes]
7	HGVR index	7.2.2	M	M	[yes]		M	[yes]		M	[yes]
8	Hand Identifier	7.2.3	M	M	[yes]		M	[yes]		M	[yes]
9	Hand Integrity	7.2.4									
10	Data Resolution	7.2.5	M	M	[yes]		M	[yes]		M	[yes]
11	Distortion	7.2.6	M	M	[yes]		M	[yes]		M	[yes]
12	Silhouette Quality	7.2.7	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
13	Camera X Position	7.2.8	M	M	[yes]		M	[yes]		M	[yes]
14	Camera Y Position	7.2.9	M	M	[yes]		M	[yes]		M	[yes]
15	Camera Z Position	7.2.10	M	M	[yes]		M	[yes]		M	[yes]
16	Target X Position	7.2.11	M	M	[yes]		M	[yes]		M	[yes]
17	Target Y Position	7.2.12	M	M	[yes]		M	[yes]		M	[yes]
18	Target Z Position	7.2.13	M	M	[yes]		M	[yes]		M	[yes]
19	X position of silhouette starting point	7.2.14	M	M	[yes]		M	[yes]		M	[yes]
20	Y position of silhouette starting point	7.2.15	M	M	[yes]		M	[yes]		M	[yes]
21	Data Compression	7.2.16	M	M	[yes]		M	[yes]		M	[yes]
22	Hand Scanning Technology	7.2.17	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
23	Extended Data Length	7.2.18	M	M	[yes]		M	[yes]		M	[yes]
24	Reserved	7.2.19	M	M	[yes]		M	[yes]		M	[yes]
25	Silhouette Data	7.2.20	M	M	[yes]		M	[yes]		M	[yes]
26	Extended Data	7.2.21	O	O	[yes, no]		O	[yes, no]		O	[yes, no]

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.7 Technical Interface Standards

A.7.1 BioAPI (ISO/IEC 19784-1:2006)

NOTE This table specifies the conformity requirements placed on BSPs that are to be deployed under this profile. This implies that some functions are designated as mandatory in the BSP in case the application uses that function. Conformity requirements placed on applications are limited to those specified in Annex A.1 of BioAPI, which requires only that the applications calls to the BSP conform to the BioAPI specification. No requirements to use specific calls are placed on applications by BioAPI.

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
1	BioAPI Registry	10.2, 10.1.2	M	M	[yes]		M	[yes]		M	[yes]
2	BioSPI_ BSPLoad	9.3.1.1	M	M	[yes]		M	[yes]		M	[yes]
3	BioSPI_ BSP Unload	9.3.1.2	M	M	[yes]		M	[yes]		M	[yes]
4	BioSPI_ BSP Attach	9.3.1.3	M	M	[yes]		M	[yes]		M	[yes]
5	BioSPI_ BSP Detach	9.3.1.4	M	M	[yes]		M	[yes]		M	[yes]
6	BioSPI_ Query units	9.3.1.5	M	M	[yes]		M	[yes]		M	[yes]
7	BioSPI_ Query BFPs	9.3.1.6	O	M	[yes]		M	[yes]		M	[yes]
8	BioSPI_ Control unit	9.3.1.7	O	M	[yes]		M	[yes]		M	[yes]
6	BioSPI_ Free BIR Handle	9.3.2.1	M	M	[yes]		M	[yes]		M	[yes]
7	BioSPI_ Get BIR From Handle	9.3.2.2	M	M	[yes]		M	[yes]		M	[yes]
8	BioSPI_ Get Header from Handle	9.3.2.3	M	M	[yes]		M	[yes]		M	[yes]
9	BioSPI_ Enable Events	9.3.3.1	M	M	[yes, no]		M	[yes, no]		M	[yes, no]
10	BioSPI Set GUI Callbacks	9.3.3.2	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
11	BioSPI_ Capture	9.3.4.1	C	M	[yes]		M	[yes]		M	[yes]
11a	Return of raw/audit data	9.3.4.1	O	M	[yes]		O	[yes, no]		O	[yes, no]
11b	Return of quality in the captured BIR header	9.3.4.1	O	M	[yes]		O	[yes, no]		O	[yes, no]

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
11c	BIR signing (by BSP)	9.3.4.1	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
11d	BIR encryption (by BSP)	9.3.4.1	O	X (see note e)	[no]		X (see note e)	[no]		X (see note e)	[no]
11e	Detection of Source Presence	9.3.4.1	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
11f	Support of application control of the GUI	9.3.4.1	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
12	BioSPI_ Create Template	9.3.4.2	C	M	[yes]		N/A	[n/a]		N/A	[n/a]
12a	Accept input of stored template to return update/ adapted template	9.3.4.2	O	O	[yes, no]		N/A	[n/a]		N/A	[n/a]
12b	Acceptance of payload	9.3.4.2	O	O	[yes, no]		N/A	[n/a]		N/A	[n/a]
12c	Return of quality in the processed BIR header	9.3.4.2	O	M	[yes]		N/A	[n/a]		N/A	[n/a]
12d	BIR signing (by BSP)	9.3.4.2	O	O	[yes, no]		N/A	[yes, no]		N/A	[yes, no]
12e	BIR encryption (by BSP)	9.3.4.2	O	X (see note e)	[no]		N/A	[n/a]		N/A	[n/a]
13	BioSPI_ Process	9.3.4.3	C	N/A	[yes, no]		O	[yes, no]		O	[yes, no]
13a	Return of quality in the processed BIR header	9.3.4.3	O	N/A	[yes, no]		O	[yes, no]		O	[yes, no]
13b	BIR signing (by BSP)	9.3.4.3	O	N/A	[yes, no]		O	[yes, no]		O	[yes, no]
13c	BIR encryption (by BSP)	9.3.4.3	O	N/A	[no]		X (see note e)	[no]		X (see note e)	[no]
14	BioSPI_ process with aux BIR	9.3.4.4	O	N/A	[yes,no]		O	[yes,no]		O	[yes,no]
15	BioSPI_ Verify Match	9.3.4.5	C	N/A	[n/a]		N/A	[n/a]		M	[yes]
15a	Model/ template adaptation	9.3.4.5	O	N/A	[n/a]		N/A	[n/a]		O	[yes, no]

Copyright International Organization for Standardization © ISO/IEC 2008 All rights reserved
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
15b-	Return of coarse scores	9.3.4.5	See note d	N/A	[n/a]		N/A	[n/a]		O	[yes, no]
15c	Return of payload	9.3.4.5	O	N/A	[n/a]		N/A	[n/a]		O	[yes, no]
16	BioSPI_ Identify Match	9.3.4.6	C	N/A	[n/a]		M	[yes]		N/A	[n/a]
16a	Return of coarse scores	9.3.4.6	See note d	N/A	[n/a]		O	[yes, no]		N/A	[n/a]
16b	Support of binning	9.3.4.6	O	N/A	[n/a]		O	[yes, no]		N/A	[n/a]
17	BioSPI_ Enrol	9.3.4.7	M	M	[yes]		N/A	[n/a]		N/A	[n/a]
17a	Template update	9.3.4.7	O	O	[yes, no]		N/A	[n/a]		N/A	[n/a]
17b	Acceptance of payload	9.3.4.7	O	O	[yes, no]		N/A	[n/a]		N/A	[n/a]
17c	Return of raw/audit data	9.3.4.7	O	M	[yes]		N/A	[n/a]		N/A	[n/a]
17d	Return of quality in the enrolment BIR header	9.3.4.7	O	M	[yes]		N/A	[n/a]		N/A	[n/a]
17e	Support of application control of the GUI	9.3.4.7	O	O	[yes, no]		N/A	[n/a]		N/A	[n/a]
17f	BIR signing (by BSP)	9.3.4.7	O	O	[yes, no]		N/A	[n/a]		N/A	[n/a]
17g	BIR encryption (by BSP)	9.3.4.7	O	X (see note e)	[no]		N/A	[n/a]		N/A	[n/a]
18	BioSPI_ Verify	9.3.4.8	M	N/A	[n/a]		N/A	[n/a]		M	[yes]
18a	Model/ template adaptation	9.3.4.8	O	N/A	[n/a]		N/A	[n/a]		O	[yes, no]
18b	Return of coarse scores	9.3.4.8	See note d	N/A	[n/a]		N/A	[n/a]		O	[yes, no]
18c	Return of payload	9.3.4.8	O	N/A	[n/a]		N/A	[n/a]		O	[yes, no]
18d	Return of raw/audit data	9.3.4.8	O	N/A	[n/a]		N/A	[n/a]		O	[yes, no]
18e	Support of application control of the GUI	9.3.4.8	O	N/A	[n/a]		N/A	[n/a]		O	[yes, no]

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
18f	BIR signing (by BSP)	9.3.4.8	O	N/A	[n/a]		N/A	[n/a]		O	[yes, no]
18g	BIR encryption (by BSP)	9.3.4.8	O	N/A	[n/a]		N/A	[n/a]		X (see note e)	[no]
19	BioSPI_ Identify	9.3.4.9	C	N/A	[n/a]		M	[yes]		N/A	[n/a]
19a	Return of coarse scores	9.3.4.9	See note d	N/A	[n/a]		O	[yes, no]		N/A	[n/a]
19b	Support of binning	9.3.4.9	O	N/A	[n/a]		O	[yes, no]		N/A	[n/a]
19c	Return of raw/audit data	9.3.4.9	O	N/A	[n/a]		O	[yes, no]		N/A	[n/a]
19d	Support of application control of the GUI	9.3.4.9	O	N/A	[n/a]		O	[yes, no]		N/A	[n/a]
19e	BIR signing (by BSP)	9.3.4.9	O	N/A	[n/a]		O	[yes, no]		N/A	[n/a]
19f	BIR encryption (by BSP)	9.3.4.9	O	N/A	[n/a]		X (see note e)	[no]		N/A	[n/a]
20	BioSPI_ Import	9.3.4.10	O	M	[yes]		N/A	[n/a]		N/A	[n/a]
21	BioSPI_ db Open	9.3.5.1	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
22	BioSPI_ db Close	9.3.5.2	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
23	BioSPI_ db Create	9.3.5.3	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
24	BioSPI_ db Delete	9.3.5.4	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
25	BioSPI_ db Set Marker	9.3.5.5	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
26	BioSPI_ db Free Marker	9.3.5.6	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
27	BioSPI_ db Store BIR	9.3.5.7	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
28	BioSPI_ db Get BIR	9.3.5.8	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
29	BioSPI_ db Get Next BIR	9.3.5.9	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
30	BioSPI_ db Delete BIR	9.3.5.10	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
31	BioSPI_ Set Power Mode	9.3.6.1	O	O	[yes, no]		O	[yes, no]		O	[yes, no]

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement								
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
32	BioSPI_ Set Indicator Status	9.3.6.2	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
33	BioSPI_ Get Power Mode	9.3.6.3	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
34	BioSPI_ Calibrate Sensor	9.3.6.4	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
35	BioSPI_ Cancel	9.3.7.1	M	M	[yes, no]		M	[yes, no]		M	[yes, no]
36	BioSPI_ Free	9.3.7.2	M	M	[yes, no]		M	[yes, no]		M	[yes, no]

NOTES

a) BioAPI requirements apply to the biometric technology as implemented in a BioAPI compliant Biometric Service Provider (BSP) module.

b) DB functions only apply for 1) self contained devices, 2) BSP controlled databases, 2a) smart card (store on card), 2b) 1:N search/match engines.

c) See Annex A.4.6.2 of the BioAPI Specification for a description of optional capabilities.

d) Return of scores is mandatory; however, the BSP has the option of returning continuous or stepwise/incremental (coarse) scores. This is described but not specified by the BioAPI.

e) Encryption of BIRs by BSPs is prohibited under this profile to insure interoperability of data between BSPs of different vendors. Encryption by the application is optional.

f) 13b/14c/18d – During capture for enrolment purposes, it is important to receive quality information in order to make decisions regarding recapture (i.e., by comparing it to an enrolment quality threshold). Quality is not critical for the BIRs collected for immediate matching, thus they are left as optional.

g) Quality is left optional in 15a because it is the output of the BioAPI_Process function, which is not used in enrolment operations (BioAPI_CreateTemplate is used for enrolments). [Could be changed to N/A if desired.]

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.7.2 CBEFF (ISO/IEC 19785-1:2006)

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
1	Standard Biometric Header	6.2.1	M	M	[yes]		M	[yes]		M	[yes]
2	SBH Security Options	6.2.1.1	M	M	[yes]		M	[yes]		M	[yes]
3	Integrity Options	6.2.1.2	M	M	[yes]		M	[yes]		M	[yes]
4	CBEFF Header Version	6.2.1.3	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
5	Patron Header Version	6.2.1.4	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
6	Biometric Type	6.2.1.5	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
7	Biometric Data Type	6.2.1.7	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
8	Biometric Subtype	6.2.1.6	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
9	Biometric Purpose	6.2.1.8	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
10	Biometric Data Quality	6.2.1.9	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
11	Biometric Creation Date	6.2.1.10	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
12	Validity Period	6.2.1.11	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
13	Index	6.2.1.13	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
14	Challenge/ Response	6.2.1.14	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
15	Payload	6.2.1.15	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
16	Subheader/ Basic Structure Count	6.2.1.16	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
17	Creator	6.2.1.12	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
18	BDB Format Owner	6.2.1.17.1	M	M	[yes]		M	[yes]		M	[yes]
19	BDB Format Type	6.2.1.17.2	M	M	[yes]		M	[yes]		M	[yes]
20	Product Identifier (PID)	6.2.1.18	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
21	Biometric Data.	6.2.2	M	M	[yes]		M	[yes]		M	[yes]

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Base Standard Requirements List				Profile Requirements List and Implementation Conformance Statement							
Item	**Question/ Feature**	**Base Ref.**	**Base Standard Status**	**Profile Status enrolment**	**ICS Support**		**Profile Status identification**	**ICS Support**		**Profile Status verification**	**ICS Support**
22	Security block	6.2.3	O	O	[yes, no]		O	[yes, no]		O	[yes, no]
23	Data elements	6.2.5	M	M	[yes]		M	[yes]		M	[yes]

The usage of the TLV-encoded patron format for use with smartcards or other tokens is mandatory (see ISO/IEC 19785-3, clause 11).

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(informative)

Additional information

This Annex contains additional information that may be of use to Airport Administrators when deploying Biometric based Access Control systems. This information is provided for guidance only and does not establish new or additional requirements on systems claiming conformance with this part of ISO/IEC 24713. Reference is also made to Annex B where additional information of interest may be found.

Fault Tolerant Design

As part of its fault tolerant design, the access controllers should have some stand-alone capabilities, such as storage to handle situations when there is no network or when the network has been denied. Whenever the network is available, it should save its auditing and transaction recording (webcam image of each person or vehicle passing) onto its main server securely. The total system should provide an efficient means to index and search for incidents that are historical and to highlight attacks or abnormalities as soon as possible. It should support the capability to correlate disparate event records, like images and logs, and integrate the entire transaction as one coherent interpretation and also to flag out abnormalities, while doing so. With respect to Zone or Area access, the ability to visualise physical areas and to map the ongoing activities would be highly valued. There should be software for flexible reporting.

Liveness Detection in Biometric Systems

Introduction

Liveness detection in a biometric system ensures that only real fingerprints, facial images, irises, and other characteristics are capable of generating valid biometric templates. Many people think that biometric systems are able to detect liveness in biometric samples. Recent tests done by the media and institutions however, show that with little effort many leading biometric technologies are susceptible to attacks in which fake fingerprints, static facial images, and static iris images can be used successfully as biometric samples. These fake samples are processed by the biometric system to generate templates and to verify enroled individuals. Methods of attack include fake fingerprints from gelatine, superimposing iris images atop contact lenses in human eyes, or even breathing on a fingerprint sensor showing the latent fingerprint of the last person who used the system. The most alarming however, is that some biometric systems have generated valid templates when a non living human part was presented. This is of course not acceptable and systems allowing this practice should not be used, or better, should be forbidden. Since biometrics is increasingly accepted as a solution for a wide range of public and private sector applications such as civil identification, network security, border control, and point of sale authentication, the question of liveness detection in leading biometric technologies must be addressed. If biometric systems can be fooled so easy, they can hardly be seen as the new security solutions.

Principle of Liveness Detection

Biometric systems are comprised of acquisition elements and processing elements. Acquisition elements record, image, or otherwise capture raw data: fingerprints, facial images, photographs, etc. Processing elements scan this raw data for distinctive or identifiable characteristics and process this information into a biometric template. Liveness detection can take place at the acquisition stage, in such a way that non-live data is not acquired, or at the processing stage, such that non-live data is not processed. The question is how liveness can be detected; e.g. what is the difference between a living or dead/fake finger? In theory, liveness detection is based on the determination that one or more qualities of a biometric sample are consistent with the qualities associated with live biometric samples. The biometric system should be designed and built in this way. More effort should be put in the capturing and processing part of the biometric system to detect liveness and only process this data. It may be necessary to implement additional liveness detection sensors and processing.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Spoofing a biometric system

As already indicated in the introduction, there are several ways of spoofing a biometric system.

1. Taking a biometric characteristic by force, e.g. cutting a finger.
2. Forcing a person to present a biometric characteristic.
3. Obtain a biometric sample without co-operation of the person, taking a fingerprint from an object touched by the person, or taking a photograph.
4. Making a copy of a biometric characteristic with co-operation of the person.
5. Insert the fake biometric in electronic form (Image) just after the acquisition stage.
6. Insert the fake biometric in electronic form (template) just after the processing stage.

Each way of spoofing has to be detected in a different way but can all be categorized under liveness detection, apart from item 2. This form of spoofing can of course not be found by using liveness detection. For Items 5 and 6 this will be dependent of the nature of the inserted signal.

Liveness detection in practice

Enrolment

The enrolment process is in almost all cases a supervised process where procedures and checks should be put in place to make it difficult to present a fake biometric. Specific measures for automatic liveness detection in the biometric equipment will normally not be necessary.

Verification

The verification process requires in addition to the presentation of a biometric characteristic also a PIN number to be keyed in, or in the case of this part of ISO/IEC 24713 a token.

Spoofing

This system requires thus a valid token and a valid biometric. In non supervised systems and especially for remote unmanned locations liveness detection will be important.

Identification

In this case, only a good copied fake biometric is needed to gain access. It will be clear that an unsupervised entrance using biometrics based on Identification forms the highest risk in a security system using biometrics. Developing effective liveness detection in biometric equipment will improve the situation, but one has to accept that any liveness detection method can and will eventually be defeated. A security problem cannot be solved by only using biometrics, but when biometrics are well implemented into a total security concept and one takes into account that even biometric ID may be spoofed, an acceptable security solution can be provided.

Biometric Access Control System with Smart Card

The Biometric Access Control System with Smart Card is a general architecture that describes the system which secures an access point by using biometric authentication with smart card. **Conformance to** (Use of) this architecture should imply the use of secure communication by means of cryptographic protection for data transmission of sensitive information such as the biometric template, end-user's information and control code to the smart card. It is also necessary to have schemes that can counter illegitimate attacks such as hill climb attack. Firmware upgrade should be possible and should be deemed necessary to update the system/security for fixing any loophole that is discovered after the release of the hardware to the end-user. The firmware upgrade should be done through a secure channel to avoid uploading malicious code that could override the

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

system. For contactless smart card system, the designer should incorporate EMI shielding to reduce the problems of electromagnetic eavesdropping and interference during the process of authentication. Audit trails for transactions should be securely date-time stamped for security auditing purpose.

For system using off-card biometric matching as the means of authentication, the smart card system should use security management scheme to protect information exchange to unauthorized terminal. For applications that require high security such as immigration, measures to counter fake biometrics attack such as liveness detection should be supported and the appropriate alerts should be triggered to the authority. The biometric matching result should be a session digitally signed by the smart card controller or system with on-card matching which has stronger security nature.

The User Interface (UI) should be intuitive for a new end-user to use. It should provide easy to understand guidance for an end-user to present biometric modal to the system to perform acquisition without assistance from the administrator. The UI should give sufficient feedback to let the end-user be informed of the status of authentication and give assistance to the end-user if any problem occurred such as system failure and acquisition problem.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C
(informative)

Security Considerations

NOTE The following items comprise general security considerations and as such are neither complete nor specific to a given system implementation. Therefore, they should be considered as a starting point for the development of a system specific security profile.

C.1 Approaches

As the purpose of a biometric access control system is security improvement, it is necessary to consider the security requirements as well as the functional and interoperability requirements. These include those unique to biometric systems as well as those of a general IT system.

When examining security requirements, it is important to analyze the value of the assets to be protected and the potential threats to those assets. After security risks are identified, appropriate countermeasures can be applied after fully considering cost vs. effect.

Moreover, it is noted that the strength of both the IT security function and the operation management are to be considered since the overall system security strength is dependent upon the strength of the weakest part. Therefore, it is important to pay attention to both the presence and consistency of countermeasures, and to consider the technical and operational elements cooperatively.

C.2 Representative threat list

Threats related to IT functions

Threat	Description
Impersonation through tampering or counterfeiting	Threats where an attacker uses his/her own biometric template instead of a legitimate biometric template by tampering with, counterfeiting, or replacing a biometric template in an attempt to impersonate a legitimate user.
Impersonation through alternation of thresholds	Threats where an attacker tampers with authentication parameters such as thresholds and making the identity verification function to come up with a false judgment, in an attempt to impersonate a legitimate user.
Leakage of biometric template	Threat to which staff's biometric information leaks by illegal reading about biometric template from token device.
Leakage of staff information	Threat to which staff's information leaks by illegal reading from biometric authentication system.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Threats related to operations

Threat	Description
Information security infrastructure	It is desirable for an organization that operates a biometric authentication system to introduce information security, and establish a management framework to govern its operation conditions.
Security in job definition and resourcing	The security responsibility of the staff shall be defined in order to reduce the risk of human error, theft, illegal acts, or misuse of facilities.
Staff training	Staff that will use the biometric authentication system shall be trained in order to ensure their awareness towards the threats and considerations of information security and to minimize any security risks that may occur.
Physical and environmental security	To prevent unauthorized access, damage, and interruption to working facilities and work information
Operational procedures and responsibilities	In order to ensure accurate and secure operation of biometric authentication systems, management and operation responsibilities and procedures for all information processing facilities should be established.
Responding to security incidents and malfunctions	In order to minimize the damage from security incidents and malfunctions. Staff members should be enforced to report occurrence of events and accidents that may effect security as well as report vulnerabilities of the system.
Impersonation with artifacts	Threats where an attacker will use a physical artificial item towards a capture device in an attempt to impersonate a legitimate user.
Impersonation through piggyback attacks	Threats where impersonation is achieved by piggyback attacks in which a legitimate user performs authentication and a third party enters the room by going in with the legitimate user.
Registration of impersonated staff	Threats where a staff that is permitted to enter the room where assets are kept, is impersonated to create an authentication token.
Impersonation by taking advantage of alternative procedures	Threats where an attacker causes a false rejection or failure to acquire (FTA) on purpose, in order to use a vulnerable alternative method thereby achieving impersonation.
Impersonation attributed to authentication accuracy	Threats where vulnerabilities are exploited in an attempt impersonate a legitimate user.
Information leakage by the recording medium's incomplete management	Threat to which information leaks by incomplete management of medium that records information on biometric authentication system.
Information leakage by network setting mistake	Threat to which information leaks by generating illegal access by setting's of network becoming improper by operation mistake etc.
Information leakage because of administrator's injustice	Threat to which information leaks because of system administrator's injustice.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] ISO/IEC 7816 (all parts), *Identification cards — Integrated circuit cards*

[2] ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

[3] ISO/IEC 9646-7:1995/Cor.1:1997, *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation Conformance Statements — Technical Corrigendum 1*

[4] ISO/IEC 9796:1991, *Information technology — Security techniques — Digital signature scheme giving message recovery*

[5] ISO/IEC 11770 (all parts), *Information technology — Security techniques — Key management*

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

[7] ISO/IEC 18031:2005, *Information technology — Security techniques — Random bit generation*

[8] ISO/IEC 18032:2005, *Information technology — Security techniques — Prime number generation*

[9] ISO/IEC 18033 (all parts), *Information technology — Security techniques — Encryption algorithms*

[10] ISO 19092, *Financial services — Biometrics — Security framework*

[11] NIST IR 6887, *Government Smart Card Interoperability Specification (GSC-IS)*

[12] ITU-T X.509, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 46 pages

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale