

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)



This is a preview of "ISO/IEC 24713-2:2008". [Click here to purchase the full version from the ANSI store.](#)

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

This is a preview of "ISO/IEC 24713-2:2008". Click here to purchase the full version from the ANSI store.

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 <i>proformas</i>	12
A.3 Profile Specific Implementation Conformance Statement	13
A.4 Instruction for completing the ICS <i>proforma</i>	13
A.4.1 General structure of the ICS <i>proforma</i>	13
A.4.2 Additional Information.....	13
A.4.3 Exception Information	13
A.5 ICS <i>proforma</i>	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/IEC 19794-5:2005)	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

This is a preview of "ISO/IEC 24713-2:2008". [Click here to purchase the full version from the ANSI store.](#)

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

This is a preview of "ISO/IEC 24713-2:2008". [Click here to purchase the full version from the ANSI store.](#)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

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

ISO/IEC 24713-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

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

- *Part 1: Overview of biometric systems and biometric profiles*
- *Part 2: Physical access control for employees at airports*
- *Part 3: Biometrics-based verification and identification of seafarers*

Introduction

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

Biometric data interchange format standards and biometric interface standards are both necessary to achieve full data interchange and interoperability for biometric recognition in an open systems environment. The ISO/IEC JTC 1/SC 37 biometric standards family includes a layered set of standards consisting of biometric data interchange formats and biometric interfaces, as well as biometric profiles that describe the use of these standards in specific application areas.

- The biometric data interchange format standards specify biometric data interchange records for different biometric modalities. Parties that agree in advance to exchange biometric data interchange records as specified in a subset of the ISO/IEC JTC 1/SC 37 biometric data interchange format standards should be able to perform biometric recognition with each other's data. Parties should also be able to perform biometric recognition even without advance agreement on the specific biometric data interchange format standards to be used, provided they have built their systems on the layered ISO/IEC JTC 1/SC 37 family of biometric standards.
- The biometric interface standards include ISO/IEC 19785, the Common Biometric Exchange Formats Framework (CBEFF) and ISO/IEC 19784, the Biometric Application Programming Interface (BioAPI). These standards support exchange of biometric data within a system or among systems. ISO/IEC 19785 specifies the basic structure of a standardized Biometric Information Record (BIR) which includes the biometric data interchange record with added metadata, such as when it was captured, its expiry date, whether it is encrypted, etc. ISO/IEC 19784 specifies an open system API that supports communications between software applications and underlying biometric technology services. BioAPI also specifies a CBEFF BIR format for the storage and transmission of BioAPI-produced data.

The biometric profile standards facilitate implementations of the base standards (e.g. the ISO/IEC JTC 1/SC 37 biometric data interchange format and biometric interface standards, and possibly non-biometric standards) for defined applications. These profile standards define the functions of an application (e.g. physical access control for employees at airports) and then specify use of options in the base standards to ensure biometric interoperability.

1) Open systems are built on standards-based, publicly defined data formats, interfaces, and protocols to facilitate data interchange and interoperability with other systems, which may include components of different design or manufacture. A closed system may also be built on publicly defined standards, and may include components of different design or manufacture, but inherently has no requirement for data interchange and interoperability with any other system.