INTERNATIONAL STANDARD

ISO/IEC 24745

First edition
2011-06-15

Information technology — Security techniques — Biometric information protection

Technologies de l'information — Techniques de sécurité — Protection des informations biométriques

Reference number
ISO/IEC 24745:2011(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) 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 and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 24745 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

As the Internet becomes a more pervasive part of daily life, various services are being provided via the Internet, such as Internet banking, remote healthcare, etc. In order to provide these services in a secure manner, the need for authentication mechanisms between subjects and the service being provided becomes even more critical. Some of the authentication mechanisms already developed include token based schemes, personal identification and transaction numbers (PIN/TAN), digital signature schemes based on public key cryptosystems, and authentication schemes using biometric techniques.

Biometrics – the automated recognition of individuals based on their behavioural and physiological characteristics – has come of age, and includes recognition technologies based on fingerprint image, voice patterns, iris image, facial image, and the like. The cost of biometric techniques has been decreasing while their reliability has been increasing, and both are now acceptable and viable for use as an authentication mechanism.

Biometric authentication introduces a potential discrepancy between privacy and authentication assurance. On the one hand, biometric characteristics are ideally an unchanging property associated with and distinct to an individual. This binding of the credential to the person provides strong assurance of authentication. On the other hand, this strong binding also underlies the privacy concerns surrounding the use of biometrics, such as unlawful processing of biometric data, and poses challenges to the security of biometric systems to prevent the compromise of biometric references. The usual solution to the compromise of an authentication credential – to change the password or issue a new token – is not generally available for biometric authentication because biometric characteristics, being either intrinsic physiological properties or behavioural traits of individuals, are difficult or impossible to change. At most another finger or eye could be enrolled, but the choices are usually limited. Therefore, appropriate countermeasures to safeguard the security of a biometric system and the privacy of data subjects are essential.

Biometric systems usually bind a biometric reference with other personally identifiable information (PII) for authenticating individuals. In this case, the binding is needed to assure the security of the data record containing biometric information. The increasing linkage of biometric references with other PII and the sharing of biometric information across legal jurisdictions make it extremely difficult for organizations to assure the protection of biometric information and to achieve compliance with various privacy regulations.

Information technology — Security techniques — Biometric information protection

1 Scope

This International Standard provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, this International Standard provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information.

This International Standard specifies the following:

- analysis of the threats to and countermeasures inherent in a biometric and biometric system application models;
- security requirements for securely binding between a biometric reference and an identity reference;
- biometric system application models with different scenarios for the storage and comparison of biometric references; and
- guidance on the protection of an individual's privacy during the processing of biometric information.

This International Standard does not include general management issues related to physical security, environmental security and key management for cryptographic techniques.

2 Terms and definitions

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

2.1
authentication
process of establishing an understood level of confidence that a specific entity or claimed identity is genuine

NOTE 1 Authentication includes the process of ascertaining an understood level of confidence of the truth of a claimed identity before the entity can be registered and recognized in a domain.

NOTE 2 Although this definition is generic, its use within this International Standard is limited to the biometric authentication of human subjects.

[ISO 19092:2008]

2.2
auxiliary data
AD
subject-dependent data that is part of a renewable biometric reference and may be required to reconstruct pseudonymous identifiers during verification, or for verification in general

NOTE 1 If auxiliary data is part of a renewable biometric reference, it is not necessarily stored in the same place as the corresponding pseudonymous identifiers.