This is a preview - click here to buy the full publication

INTERNATIONAL STANDARD

ISO/IEC 24761

First edition
2009-05-15

Information technology — Security techniques — Authentication context for biometrics

Technologies de l'information — Techniques de sécurité — Contexte d'authentification biométrique

Withdrawn

Reference number
ISO/IEC 24761:2009(E)

© ISO/IEC 2009

This is a preview - click here to buy the full publication

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.

withdrawn

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009

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

© ISO/IEC 2009 – All rights reserved

This is a preview - click here to buy the full publication

Contents

Page

Withdrawn

© ISO/IEC 2009 – All rights reserved

This is a preview - click here to buy the full publication

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.

ISO/IEC 24761 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Withdrawn

© ISO/IEC 2009 – All rights reserved

This is a preview - click here to buy the full publication

Introduction

A biometric verification process executed at a remote site is exposed to many risks: falsified reference templates, forged raw data, unreliable biometric devices, etc. How can the validator check whether a biometric verification process carried out in a remote site is trustworthy? This International Standard gives a mechanism to cope with this problem.

In general, reliability of the result of a biometric verification process is dependent both on the security level of the process executed and on the functional performance level of the biometric devices used. If devices offering a better functional performance level are used, the result will be more reliable. If the devices are not secure or the process has been executed in an unsecure environment, then the result will not be reliable.

In the Internet environment, the validator of a biometric verification process usually does not directly know about the biometric devices used or about the process(es) executed at a remote site. Obtaining trusted information, such as the functional performance level of the biometric devices used, the security level of the remote system, and also knowing that the processes in the system were executed securely, the validator can make a better decision on how much trust can be placed on the result of the biometric verification.

This International Standard provides a solution to the above problem by sending information about the devices used and the processes executed at the remote site to the validator.

In general, the biometric enrolment process consists of the following subprocesses: data capture, intermediate signal processing, final signal processing (or feature extraction), and storage. (This is true in general, but there are many variants possible.)

In general, the biometric verification process consists of data capture, intermediate signal processing, final signal processing, retrieval from storage, comparison, and decision. (This is true in general, but there are many variants possible.)

Usually, subprocesses are executed in one or more biometric processing units (BPUs), each of which has its own uniform security level. Several subprocesses are involved in the biometric verification process, but the security of the retrieval subprocess from storage is also dependent on the subprocesses involved in the biometric enrolment process.

This International Standard is designed to be applied to this model of biometric verification processes, which is an extension of the biometric system model defined in ISO 19092, but is also applicable to other biometric verification process models.

This International Standard defines a data format for security data generated by BPUs, such as a sensor, smartcard, or comparison device, to provide certified information about the BPU to help the validator to determine the reliability of the result of the biometric verification process.

This International Standard is based on the Public Key Infrastructure (PKI) technology and PKIX (see ISO/IEC 9594-8 | ITU-T Recommendation X.509 and RFC 3852). This International Standard uses a digital signature as the base for trust and non-repudiation. This International Standard requires input and output information to be hashed, and subsequently digitally signed with other data such as a challenge from the validator, and the evaluation result of the BPU actions.

This International Standard recognizes that privacy requirements concerned with the storage of biometric elements have to respond to and comply with local laws and legislation on data privacy. ACBio ensures that the validator can validate the result of the biometric verification process without receiving private data, such as the biometric sample acquired from the claimant or the biometric reference template used for comparison.

Withdrawn

© ISO/IEC 2009 – All rights reserved

This is a preview - click here to buy the full publication

An ACBio instance is a report that is encoded using the XML Encoding Rules (XER) or the Basic Encoding Rules (BER) of ASN.1 [see ISO/IEC 8824 (All parts) | ITU-T Recommendations X.680-683 and ISO/IEC 8825-4 | ITU-T Recommendation X.693], commonly supported by cryptographic tool kit vendors. The syntax is algorithm independent and supports provision of data integrity and data origin authentication. The cryptographic algorithms specified by ISO/IEC JTC 1/SC 27 are recommended, though any algorithm appropriate for use by a given community may be used.

This International Standard uses BPU certificates, issued by a BPU certification organization (a trusted third party that issues certificates concerning the security of the BPU) and biometric reference template (BRT) certificates, issued by a BRT certification organization that issues certificates concerned with the production and retention of a biometric reference template in a database or on a smart-card.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning the ACBio instance given in Clauses 5, 6, 7, and 8.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Toshiba Corporation, Toshiba Solutions Corporation,
1-1, Shibaura 1-chome, Minato-ku,
Tokyo 105-8001, Japan

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

Withdrawn

© ISO/IEC 2009 – All rights reserved

This is a preview - click here to buy the full publication

Information technology — Security techniques — Authentication context for biometrics

1 Scope

This International Standard defines the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site. This International Standard allows any ACBio instance to accompany any data item that is involved in any biometric process related to verification and enrolment. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion.

This International Standard specifies the cryptographic syntax of an ACBio instance. The cryptographic syntax of an ACBio instance is based on an abstract Cryptographic Message Syntax (CMS) schema whose concrete values can be represented using either a compact binary encoding or a human-readable XML encoding.

This International Standard does not define protocols to be used between entities such as BPUs, claimant, and validator. Its concern is entirely with the content and encoding of the ACBio instances for the various processing activities.

Withdrawn

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 8824 (all parts) | ITU-T Recommendations X.680-683, *Information technology — Abstract Syntax Notation One (ASN.1)*

ISO/IEC 8825-4 | ITU-T Recommendation X.693, *Information technology — ASN.1 encoding rules: XML Encoding Rules (XER)*

ISO/IEC 9594-2 | ITU-T Recommendation X.501, *Information technology — Open Systems Interconnection — The Directory: Models*

ISO/IEC 9594-8 | ITU-T Recommendation X.509, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

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

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

RFC 3852, *Cryptographic Message Syntaxt (CMS), July 2004*

© ISO/IEC 2009 – All rights reserved