INTERNATIONAL STANDARD

ISO/IEC 24761

Second edition
2019-10

Information technology — Security techniques — Authentication context for biometrics

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

Reference number
ISO/IEC 24761:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 24761:2009), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 24761:2009/Cor.1:2013. The main changes compared to the previous edition are as follows:

- extension of data types which reflects the progress in biometric technology for protection of biometric data such as renewable biometrics and others,
- introduction of a new biometric capability model which makes the validation of ACBio instances simpler, and
- changes to the ASN.1 module as a result of the above changes.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

A biometric verification process executed at a remote site is exposed to many risks, for example, falsified reference, forged captured biometric data, and unreliable biometric products, etc. How can the validator check whether a biometric verification process, carried out in a remote site, is trustworthy? This document gives a mechanism to cope with this problem.

In general, the reliability of the result of a biometric verification process is dependent both on the security of the process executed and on the functional performance of the biometric products used. If products offering a better functional performance are used, the result will be more reliable. If the products are not secure or the process has been executed in an insecure 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 products used or about the process(es) executed at a remote site. Authentication Context for Biometrics (ACBio) provides a solution to the above problem and mitigates security risks of biometric authentication, by sending information about the products used and the processes executed at the remote site to the validator if the biometric processing has resulted successfully.

ACBio defines data formats for evidence data generated by biometric processing units (BPUs), such as a sensor, smartcard or comparison device, which are carried in data structures called ACBio instances. ACBio specifies a trust and assurance mechanism based on digital signature technology to provide assured information about the BPU and its execution of the biometric enrolment and verification processes where the assured information about the BPU is provided as BPU report issued by the vendor of the BPU. This is based on the Public Key Infrastructure (PKI) technology and PKIX (see ISO/IEC 9594-8 and RFC 3852). An ACBio instance carries information about the biometric processing units (BPUs), biometric reference and biometric verification results that together characterise a biometric verification transaction. Assurance of the information in an ACBio instance is provided by digital certificates associated with the relevant elements of the information. These certificates are issued by trusted certification authorities in registration processes which gather evidence about the BPUs and their verification performance capabilities, and the biometric reference and the binding to a known subject. The certificates serve two purposes. Firstly, to provide assurance of the identity of the source of the biometric transaction (the BPUs) and the biometric reference, and secondly to provide assurance for the biometric verification result contained in the transaction. With all the ACBio instances sent to the validator, it can check the integrity of the data transmitted between BPUs. The real-time information of presentation attack detection is not provided with this document. The BPU report may, however, contain the assurance information of the PAD mechanism. ACBio recognizes that privacy requirements concerned with the storage of biometric data must 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 used for comparison.

An ACBio instance is a report that is encoded using the Basic Encoding Rules (BER) of ASN.1 [see ISO/IEC 8824 (all parts)], commonly supported by cryptographic tool kit vendors. The syntax is algorithm independent and supports provision of data integrity and data origin authentication. In regard to cryptographic algorithms, those specified by ISO/IEC JTC 1/SC 27 are recommended, though any algorithm appropriate for use by a given community may be used.

This document reflects the progress in biometric technology for protection of biometric data such as renewable biometrics specified in ISO/IEC 24745 and others by extending the variation of biometric data types transmitted between biometric subprocesses, and in addition establishes a new biometric capability model which makes the validation of ACBio instance(s) simpler. This has resulted in some changes to the ASN.1 module which will give rise to inter-operational incompatibilities between systems implementing different versions of the ASN.1 modules.

Information technology — Security techniques — Authentication context for biometrics

1 Scope

This document 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 enrolment and verification process executed at a remote site. This document allows any ACBio instance to accompany any biometric processes related to enrolment and verification. The specification of ACBio is applicable not only to single modal biometric enrolment and verification but also to multimodal fusion. The real-time information of presentation attack detection is not provided in this document. Only the assurance information of presentation attack detection (PAD) mechanism can be contained in the BPU report.

Biometric identification is out of the scope of this document.

This document specifies the cryptographic syntax of an ACBio instance. The cryptographic syntax of an ACBio instance is defined in this document applying a data structure specified in Cryptographic Message Syntax (CMS) schema whose concrete values can be represented using a compact binary encoding. This document 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.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

ISO/IEC 9594-2, *Information Technology — Open Systems Interconnection — The Directory: Models*

ISO/IEC 9594-8, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

ISO/IEC 24745, *Information technology — Security techniques — Biometric information protection*