FINAL DRAFT
International Standard

ISO/IEC
FDIS
19785-4

Information technology — Common Biometric Exchange Formats Framework —

Part 4: Security block format specifications

Technologies de l'information — Cadre de formats d'échange biométriques communs —

Partie 4: Spécifications de format de bloc de sécurité

ISO/IEC JTC **1**/SC **37**

Secretariat: **ANSI**

Voting begins on:
2025-03-26

Voting terminates on:
2025-05-21

Reference number
ISO/IEC FDIS 19785-4:2025(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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

This second edition cancels and replaces the first edition (ISO/IEC 19785-4:2010), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 19785-4:2010/Cor. 1:2013.

The main changes are as follows:

— the SB formats in ASN.1 were specified in Clauses 5 and 6;

— the SB format for general purpose in XML was newly added as Clause 7;

— formats which were defined in ISO/IEC 19785-4:2010, but are now considered deprecated, have been listed in the Introduction.

A list of all parts in the ISO/IEC 19785 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

Biometric verification and identification are important techniques for the authentication and identification of an individual. It is essential for biometric data used in biometric verification and identification to come from a trusted source with no interference in transmission. This relates to the data's integrity. It can also be necessary to keep the data secret. This relates to the encryption of the data depending on security policy. This document provides for both the integrity and encryption of biometric data.

NOTE The term "security policy" in this context relates to security technology rather than contracts or law. Security policy is determined in and applied to an organization or system.

To ensure interoperability, the Common Biometric Exchange Formats Framework (CBEFF) was specified in ISO/IEC 19785-1 to associate metadata with one or more biometric data blocks (BDBs). In ISO/IEC 19785-1, the options for integrity and encryption and the concept of a security block (SB) to contain security information related to these options are defined, but the format and detailed content of SBs are not specified.

There are several sequential steps for specifying a security block, starting from a CBEFF patron format.

First, the patron format can determine that the abstract value of the CBEFF data element CBEFF_BDB_encryption_options is fixed as NO ENCRYPTION and that the CBEFF data element CBEFF_BIR_integrity_options is fixed as NO INTEGRITY. In this case, there is no need for an SB in the patron format.

If the patron format requires the inclusion of an SB in some circumstances, the SB format is specified in this document where the SB format is identified by the CBEFF data elements CBEFF_SB_format_owner and CBEFF_SB_format_type that can be included in the patron format.

Besides the SB formats defined in this document, there are many possible CBEFF SB formats that meet different needs. For example, ISO/IEC 24713-3 specifies the requirements for an SB format for the Seafarers' Identity Document according to the International Labour Organization. The SB format specified in Clause 5 is designed to be as general as possible. The SB format specified in Clause 6 is designed to provide a basic security provision and supports integrity only.

This document specifies three SB formats.

The first SB format specifies a general-purpose security block format with optional elements for encryption and integrity. This format uses RFC 5652 Cryptographic Message Syntax (CMS). Modifications have been made to `EnvelopedData`, `EncryptedData`, `SignedData`, and `AuthenticatedData` to meet the needs and requirements for expressing the security of biometric information in conformance with the CBEFF. The second SB format is a signature-only security block format, which is also defined using RFC 5652. The third is a general-purpose security block format in XML with optional elements for encryption and integrity.

The general-purpose security block format specified in this document also contains optional authentication context for biometrics (ACBio) instances, as specified in ISO/IEC 24761. ACBio instances also use the CMS scheme outlined in RFC 5652. Including ACBio instances helps determine the security levels of the systems producing the result of biometric verification. The optional use of ACBio instances is an important part of the provision of a telebiometric authentication infrastructure[8].

The PER-encoded general-purpose security block format, the XER-encoded general-purpose security block format, the DER-encoded signature-only security block format, the PER-encoded signature-only security block format, and the XER-encoded signature-only security block format, which were specified in the previous edition of this document, have been removed as they are considered deprecated and are not recommended for use in new implementations

Information technology — Common Biometric Exchange Formats Framework —

Part 4:
Security block format specifications

1 Scope

This document specifies security block (SB) formats (see ISO/IEC 19785-1) registered in accordance with ISO/IEC 19785-2 as formats defined by the Common Biometric Exchange Formats Framework (CBEFF) biometric organization ISO/IEC JTC 1/SC 37. This document also specifies registered SB format identifiers.

NOTE The SB format identifier is recorded in the standard biometric header (SBH) of a patron format (or defined by that patron format as the only available SB format).

The general-purpose SB format specifies whether the biometric data block (BDB) is encrypted or the SBH and BDB have integrity applied (or both). The general-purpose SB format can include ACBio instances (see ISO/IEC 24761). This SB provides all necessary security parameters, including those used for encryption or integrity.

This document does not restrict the algorithms and parameters used for encryption or integrity, but it provides for the recording of such algorithms and parameter values.

This document does not cover profiling to determine what algorithms and parameter ranges can be used by the generator of an SB for a particular application area, and hence what algorithms and parameter ranges have to be supported by the user of an SB.

The second SB format is more limited but simpler. In particular, it cannot contain ACBio instances and does not support encryption of the BDB.

The general-purpose SB format in XML provides for specification of whether the BDB is encrypted or the SBH and BDB have integrity applied (or both).

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 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*

ISO/IEC 24761, *Information technology — Security techniques — Authentication context for biometrics*

RFC 5652, *Cryptographic Message Syntax (CMS), September 2009*

RFC 6268, *Additional New ASN.1 Modules for Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX), July 2011*

XML Encryption Syntax and Processing Version 1.1, April 2013

XML Signature Syntax and Processing Version 2.0, July 2015

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19785-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
ACBio instance
report generated by a BPU compliant to ISO/IEC 24761 to show the validity of the execution result of one or more subprocesses executed in the BPU

[SOURCE: ISO/IEC 24761:2019, 3.1, modified — "this document" has been replaced with "ISO/IEC 24761".]

3.2
BioAPI Unit
abstraction of a hardware or software resource that is directly managed by a biometric service provider (BSP) or BioAPI function provider (BFP)

Note 1 to entry: BioAPI Units are categorized and include sensor units, archive units, matching algorithm units and processing algorithm units.

Note 2 to entry: The term "matching" is replaced with "comparison" in the current biometric vocabulary defined in ISO/IEC 2382-37.

[SOURCE: ISO/IEC 19784-1:2018, 4.7, modified — Note 2 to entry has been added.]

3.3
biometric processing unit
BPU
trusted implementation of a collection of biometric subprocesses implemented in a single physical unit

Note 1 to entry: A BPU commonly comprises biometric subprocesses that are sequential in the process flow for a biometric verification.

Note 2 to entry: Application/service requirements typically require BPU subprocesses to meet a uniform level of security assurance. In ACBio, assurance is achieved through a BPU evaluation process that is authenticated by means of an X.509 certificate embedded in an ACBio instance.

[SOURCE: ISO/IEC 24761:2019, 3.3]

3.4
message authentication code
MAC
string of bits which is the output of a MAC algorithm

Note 1 to entry: A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2).

[SOURCE: ISO/IEC 9797-1:2011, 3.9]

4 Abbreviated terms

ACBio	authentication context for biometrics
BDB	biometric data block
BER	Basic Encoding Rules
BIR	biometric information record
CBEFF	Common Biometric Exchange Formats Framework
CRL	certificate revocation list
SB	security block
SBH	standard biometric header
XML	eXtensible Markup Language

5 ASN.1 Security block format: general purpose

5.1 Security block format owner

ISO/IEC JTC 1/SC 37.

5.2 Security block format owner identifier

257 (0101Hex). This identifier has been assigned to ISO/IEC JTC 1/SC 37 as a CBEFF biometric organization in accordance with ISO/IEC 19785-2.

5.3 Security block format name

ISO/IEC JTC 1/SC 37 CBEFF general-purpose security block format

5.4 Security block format identifier

7 (0007 Hex). This has been registered in accordance with ISO/IEC 19785-2 when BER encodings are applied (see ISO/IEC 8825-1).

5.5 ASN.1 object identifier for this security block format

```
{iso(1) registration-authority(1) cbeff(19785) organizations(0) jtc-sc37 (257) sb-formats(3)
general-purpose-ber(7)}
```

or, in XML value notation,

```
1.1.19785.0.257.3.7
```

5.6 Domain of use

The general-purpose security block is designed for applications that require either integrity or encryption or both. It is also designed for optional inclusion of ACBio instances.

5.7 Version identifier

This SB format specification has a version identifier of (major 1, minor 0).

5.8 Format specification and conformance statement

5.8.1 General

5.8.1.1 In this document, a CBEFF SB is defined as the ASN.1 type **CBEFFSecurityBlock** which is a sequence of the ASN.1 type **CBEFFSecurityBlockElement**.

```
CBEFFSecurityBlock ::= SEQUENCE OF CBEFFSecurityBlockElement

CBEFFSecurityBlockElement ::= CHOICE {
        elementCBEFFSB ContentInfoCBEFFSB,
        subBlockForACBio SubBlockForACBio,
        accumulatedACBioInstances ACBioInstances
         }
```

5.8.1.2 There are three alternatives for the type **CBEFFSecurityBlockElement**. These are **ContentInfoCBEFFSB**, **SubBlockForACBio**, or **ACBioInstances**. **CBEFFSecurityBlockElement** carries information about the integrity of the concatenation of the SBH and the BDB or the encryption of the BDB. **SubBlockForACBio** and **ACBioInstances** carry information on the ACBio which is specified in ISO/IEC 24761.

5.8.1.3 The type **ContentInfoCBEFFSB** is defined as:

```
ContentInfoCBEFFSB ::= SEQUENCE {
        contentType CONTENT-TYPE.&id({ContentTypeCBEFF}),
        content [0] EXPLICIT CONTENT-TYPE.&Type
            ({ContentTypeCBEFF}{@contentType})
        }
```

NOTE This type replaces the type **ContentInfo** in RFC 6268. The first component of this type can take only four object identifiers, namely **id-envelopeRelatedData**, **id-encryptionRelatedData**, **id-signatureRelatedData**, or **id-authenticationRelatedData**. The type **ContentInfo** in RFC 6268 can take other object identifiers.

This type can occur twice at most in the **CBEFFSecurityBlock** sequence, once to support integrity and once to support encryption.

The type **ContentInfoCBEFFSB** is composed of two components, **contentType** and **content**. The first component **contentType** is an object identifier, which indicates the type of content in the second component **content**. The value of **contentType** takes one of the following four object identifiers: **id-envelopeRelatedData**, **id-encryptionRelatedData**, **id-signatureRelatedData**, or **id-authenticationRelatedData**. This is done by the following definition of **ContentTypeCBEFF** and that of the four **CONTENT-TYPE**s. Here, type **CONTENT-TYPE** associates an object identifier with an ASN.1 type.

```
ContentTypeCBEFF CONTENT-TYPE ::= { envelopeRelatedData | encryptionRelatedData |
                    signatureRelatedData | authenticationRelatedData}
envelopeRelatedData CONTENT-TYPE ::= {
        EnvelopeRelatedData
        IDENTIFIED BY id-envelopeRelatedData
}

encryptionRelatedData CONTENT-TYPE ::= {
        EncryptionRelatedData
        IDENTIFIED BY id-encryptionRelatedData
}

signatureRelatedData CONTENT-TYPE ::= {
        SignatureRelatedData
        IDENTIFIED BY id-signatureRelatedData
}

authenticationRelatedData CONTENT-TYPE ::= {
        AuthenticationRelatedData
        IDENTIFIED BY id-authenticationRelatedData
}
```

These four object identifier names are defined as follows: