INTERNATIONAL STANDARD

ISO/IEC 19785-4

First edition
2010-08-15

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 2010

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 19785-4:2010
https://standards.iteh.ai/catalog/standards/sist/60c59192-95eb-4720-ba5e-
93db7c123413/iso-iec-19785-4-2010

COPYRIGHT PROTECTED DOCUMENT

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 19785-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC 19785 consists of the following parts, under the general title *Information technology — Common Biometric Exchange Formats Framework*:

— *Part 1: Data element specification*

— *Part 2: Procedures for the operation of the Biometric Registration Authority*

— *Part 3: Patron format specifications*

— *Part 4: Security block format specifications*

Introduction

Biometric verification and identification are important techniques for the authentication and/or identification of an individual. Biometric data used in biometric verification and identification has to be from a trusted source with no interference in transmission (integrity). It might or might not be necessary for it to be kept secret (encryption) depending on security policy. This part of ISO/IEC 19785 provides for both integrity and encryption of the biometric data.

To ensure interoperability, the Common Biometric Exchange Formats Framework (CBEFF) was specified in ISO/IEC 19785-1 to associate meta-data 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 security blocks (SB formats) are not specified.

There are several steps in the chain, 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 a security block to be required in that patron format.

If the patron format requires the inclusion of a security block in some circumstances, it can fix it as one of the security blocks defined in this part of ISO/IEC 19785 (or as some other security block), or can include the CBEFF data elements CBEFF_SB_format_owner and CBEFF_SB_format_type to identify one of these or some other security block format.

Besides the security block formats defined in this part of ISO/IEC 19785, there will be many possible CBEFF security block formats meeting different needs. For example, a security block format is specified for the ILO seafarers profile in ISO/IEC 24713-3. The security block format specified in Clause 5 is designed to be as general as possible. The security block format specified in Clause 6 is designed to provide a basic security provision and supports integrity only.

This part of ISO/IEC 19785 specifies two security block formats.

The first security block specifies a general-purpose security block format with optional elements for encryption, and for integrity, using RFC 3852 Cryptographic Message Syntax (CMS), with certain modifications to **EnvelopedData**, **EncryptedData**, **SignedData**, and **AuthenticatedData**, to meet the needs and requirements in expressing the security of biometric information in conformance with CBEFF. The second is named signature-only security block format, which is also defined using RFC 3852.

The general-purpose security block format specified in this part of ISO/IEC 19785 also contains optional Authentication Context for Biometrics (ACBio) instances specified in ISO/IEC 24761. ACBio also uses the RFC 3852 Cryptographic Message Syntax scheme. The inclusion of ACBio instances enables the security levels of the systems producing the authenticated biometric to be determined. The optional use of ACBio instances is an important part of the provision of a telebiometric authentication infrastructure (TAI) [3].

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Information technology — Common Biometric Exchange Formats Framework —

Part 4:
Security block format specifications

1 Scope

This part of ISO/IEC 19785 specifies security block formats (see ISO/IEC 19785-1) registered in accordance with ISO/IEC 19785-2 as formats defined by the CBEFF biometric organization ISO/IEC JTC 1/SC 37, and specifies their registered security block format identifiers.

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

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

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

It is a matter for profiling to determine, for a particular application area, what algorithms and parameter ranges can be used by the generator of a security block, and hence what algorithms and parameter ranges have to be supported by the user of a security block. This is out of the scope of this part of ISO/IEC 19785.

The second security block is more limited, but simpler (and in particular cannot contain ACBio instances, and does not support encryption of the BDB).

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 Rec. X.680–683, *Information technology — Abstract Syntax Notation One (ASN.1)*

ISO/IEC 8825 (all parts) | ITU-T Rec. X.690–693, *Information technology — ASN.1 encoding rules*

ISO/IEC 9798-6, *Information technology — Security techniques — Entity authentication — Part 6: Mechanisms using manual data transfer*

ISO/IEC 19784-1, *Information technology — Biometric application programming interface — Part 1: BioAPI specification*

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

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

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

RFC 5911, *New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S-MIME*, June 2010

3 Terms and definitions

3.1 Terms defined in ISO/IEC 19785-1

For the purposes of this document, the following terms defined in ISO/IEC 19785-1 apply:

biometric, biometrics, biometric data block (BDB), biometric information record (BIR), CBEFF biometric organization, security block (SB), security block format, security block format identifier, security block format owner, standard biometric header (SBH).

3.2 Terms defined in ISO/IEC 19784-1

For the purposes of this document, the following term defined in ISO/IEC 19784-1 applies:

BioAPI Unit.

3.3 Terms defined in ISO/IEC 24761

For the purposes of this document, the following terms defined in ISO/IEC 24761 apply:

ACBio instance, authentication context for biometrics (ACBio), biometric processing unit (BPU).

3.4 Terms defined in ISO/IEC 9798-6

For the purposes of this document, the following term defined in ISO/IEC 9798-6 applies:

message authentication code.

4 Abbreviated terms

4.1 Abbreviated terms defined in ISO/IEC 19785-1

For the purposes of this document, the following abbreviated terms in ISO/IEC 19785-1 apply:

BDB, BIR, CBEFF, SB, SBH.

4.2 Abbreviated terms defined in ISO/IEC 24761

For the purposes of this document, the following abbreviated terms in ISO/IEC 24761 apply:

ACBio, BPU.

4.3 Abbreviated terms defined in ISO/IEC 9798-6

For the purposes of this document, the following abbreviated term in ISO/IEC 9798-6 applies:

MAC.

4.4　Abbreviated terms defined in RFC 3852

For the purposes of this document, the following abbreviated term in RFC 3852 applies:

CRL.

5　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 in accordance with ISO/IEC 19785-2 to ISO/IEC JTC 1/SC 37 as a CBEFF biometric organization.

5.3　Security block format name

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

5.4　Security block format identifier

`1 (0001 Hex).` This has been registered in accordance with ISO/IEC 19785-2 when DER encodings (see ISO/IEC 8825-1) are applied.

`2 (0002 Hex).` This has been registered in accordance with ISO/IEC 19785-2 when canonical PER encodings (see ISO/IEC 8825-2) are applied.

`3 (0003 Hex).` This has been registered in accordance with ISO/IEC 19785-2 when canonical XER encodings (see ISO/IEC 8825-3) are applied.

5.5　ASN.1 object identifier for this security block format

5.5.1　The case of DER encodings

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

or, in XML value notation,

```
1.1.19785.0.257.3.0.1
```

5.5.2　The case of canonical PER encodings

```
{iso registration-authority cbeff(19785) organizations(0) jtc-sc37 (257) sb-formats(3)
general-purpose(0) per-encoding(2)}
```

or, in XML value notation,

```
1.1.19785.0.257.3.0.2
```

5.5.3   The case of canonical XER encodings

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

or, in XML value notation,

```
1.1.19785.0.257.3.0.3
```

5.6   Domain of use

The general-purpose security block is designed for applications that require integrity and/or encryption, and optionally inclusion of ACBio instances.

5.7   Version identifier

This security block format specification has a version identifier of (major 0, minor 0).

5.8   Format specification and conformance statement

5.8.1   General

5.8.1.1   In this part of ISO/IEC 19785, a CBEFF security block is defined as the ASN.1 (see ISO/IEC 8824) 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 encryption of the BDB. The latter two carry information on 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 5911. The first component of this type can take only four object identifiers, namely `id-envelopeRelatedData`, `id-encryptionRelatedData`, `id-signatureRelatedData`, or `id-authenticationRelatedData`, while that of the type `ContentInfo` in RFC 5911 can take other object identifiers.

This type can occur two times 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
}
```

The above listed four object identifier names are defined as follows:

```
id-envelopeRelatedData OBJECT IDENTIFIER ::= {
      iso(1) standard(0) cbeff(19785) contentType(1) envelopeRelatedData(1)
}

id-encryptionRelatedData OBJECT IDENTIFIER ::= {
      iso(1) standard(0) cbeff(19785) contentType(1) encryptionRelatedData(2)
}

id-signatureRelatedData OBJECT IDENTIFIER ::= {
      iso(1) standard(0) cbeff(19785) contentType(1) signatureRelatedData(3)
}

id-authenticationRelatedData OBJECT IDENTIFIER ::= {
      iso(1) standard(0) cbeff(19785) contentType(1) authenticationRelatedData(4)
}
```

`id-envelopeRelatedData` or `id-encryptionRelatedData` shall be taken in the field `contentType` of type `ContentInfoCBEFFSB` if the data element CBEFF_BDB_encryption_options (see ISO/IEC 19785-1) is present and contains the encoding for ENCRYPTION.

`id-signatureRelatedData` or `id-authenticationRelatedData` shall be taken in the field `contentType` of type `ContentInfoCBEFFSB` if the data element CBEFF_BIR_integrity_options (see ISO/IEC 19785-1) is present and contains the encoding for INTEGRITY.

5.8.1.4 The second alternative `subBlockForACBio` of type `SubBlockForACBio` shall be used if a BPU of a BioAPI unit generates and outputs an ACBio instance. This data shall be exchanged to the successive BPU of BioAPI unit. The type `SubBlockForACBio` is defined as follows:

```
SubBlockForACBio ::= SEQUENCE {
      bpuIOIndex INTEGER,
      acbioInstance ACBioInstance
}
```

The first component `bpuIOIndex` is the BPU IO index for the output from a BPU and is transferred to the next BPU as the BPU IO index for the input to the second BPU. The second component is the ACBio instance generated by the first BPU. For details, see ISO/IEC 24761.