

---

---

**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*

**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.

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2010

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword .....	iv
Introduction.....	v
<b>1</b> <b>Scope</b> .....	<b>1</b>
<b>2</b> <b>Normative references</b> .....	<b>1</b>
<b>3</b> <b>Terms and definitions</b> .....	<b>2</b>
<b>3.1</b> <b>Terms defined in ISO/IEC 19785-1</b> .....	<b>2</b>
<b>3.2</b> <b>Terms defined in ISO/IEC 19784-1</b> .....	<b>2</b>
<b>3.3</b> <b>Terms defined in ISO/IEC 24761</b> .....	<b>2</b>
<b>3.4</b> <b>Terms defined in ISO/IEC 9798-6</b> .....	<b>2</b>
<b>4</b> <b>Abbreviated terms</b> .....	<b>2</b>
<b>4.1</b> <b>Abbreviated terms defined in ISO/IEC 19785-1</b> .....	<b>2</b>
<b>4.2</b> <b>Abbreviated terms defined in ISO/IEC 24761</b> .....	<b>2</b>
<b>4.3</b> <b>Abbreviated terms defined in ISO/IEC 9798-6</b> .....	<b>2</b>
<b>4.4</b> <b>Abbreviated terms defined in RFC 3852</b> .....	<b>3</b>
<b>5</b> <b>Security block format: general purpose</b> .....	<b>3</b>
<b>5.1</b> <b>Security block format owner</b> .....	<b>3</b>
<b>5.2</b> <b>Security block format owner identifier</b> .....	<b>3</b>
<b>5.3</b> <b>Security block format name</b> .....	<b>3</b>
<b>5.4</b> <b>Security block format identifier</b> .....	<b>3</b>
<b>5.5</b> <b>ASN.1 object identifier for this security block format</b> .....	<b>3</b>
<b>5.6</b> <b>Domain of use</b> .....	<b>4</b>
<b>5.7</b> <b>Version identifier</b> .....	<b>4</b>
<b>5.8</b> <b>Format specification and conformance statement</b> .....	<b>4</b>
<b>5.9</b> <b>Encoding of abstract values</b> .....	<b>10</b>
<b>6</b> <b>Security block format: signature only</b> .....	<b>11</b>
<b>6.1</b> <b>Security block format owner</b> .....	<b>11</b>
<b>6.2</b> <b>Security block format owner identifier</b> .....	<b>11</b>
<b>6.3</b> <b>Security block format name</b> .....	<b>11</b>
<b>6.4</b> <b>Security block format identifier</b> .....	<b>11</b>
<b>6.5</b> <b>ASN.1 object identifier for this security block format</b> .....	<b>11</b>
<b>6.6</b> <b>Domain of use</b> .....	<b>12</b>
<b>6.7</b> <b>Version identifier</b> .....	<b>12</b>
<b>6.8</b> <b>Format specification and conformance statement</b> .....	<b>12</b>
<b>Annex A</b> (normative) <b>ASN.1 module for security block format</b> .....	<b>13</b>
<b>Annex B</b> (informative) <b>Difference from types defined in RFC 5911</b> .....	<b>15</b>
<b>Bibliography</b> .....	<b>18</b>

## 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].

# 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