AS ISO/IEC 19785.4:2025
ISO/IEC 19785-4:2025

Australian STANDARD®

STANDARDS Australia

Information technology — Common Biometric Exchange Formats Framework

Part 4: Security block format specifications



AS ISO/IEC 19785.4:2025

This Australian Standard® was prepared by IT-032, Biometrics and Identification. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 13 August 2025.

This Standard was published on 29 August 2025.

The following are represented on Committee IT-032:

Department of Defence (Australian Government)
Department of Foreign Affairs and Trade (DFAT)
Department of Home Affairs — Digital and Technology Policy Division
Photo Marketing Association
SITA

This Standard was issued for comment as DR AS ISO/IEC 19785.4:2025

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals and new products by visiting:

www.standards.org.au

ISBN: 978 1 76175 343 5

AS ISO/IEC 19785.4:2025

ISO/IEC 19785-4:2025

Australian Standard®

Information technology — Common Biometric Exchange Formats Framework

Part 4: Security block format specifications

First published as AS ISO/IEC 19785.4:2025.

© ISO/IEC 2025 — All rights reserved
© Standards Australia Limited 2025

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

How to read this Standard

This page explains the meaning of the language and structure of this Standard.

Refer to Standards Australia's Standardisation Guide 006 for more details about drafting rules.

Australian and Australian/New Zealand Standards are voluntary unless they are referenced in legislation or called up in contracts.

Requirements

To conform to a Standard, all requirements in the Standard need to be met.

A requirement is any statement in the Standard which uses the word "shall".

Recommendations, permissions and possibilities

The following words are commonly used in Standards, but statements using them do not have to be followed to conform to the Standard:

(a) "should" means that something is recommended.

(b) "may" means that something is permitted.

(c) "can" means that something is possible.

Structure of Standards

A Standard always has the following parts:

(i) The Preface states who developed the Standard, what the Standard is aiming to do, and how it relates to other documents.

(ii) The Scope states what the Standard is about, what it covers and what it does not cover.

(iii) The Normative references clause lists other documents that are referenced in the Standard as part of requirements.

(iv) The Terms and definitions clause defines important terms to help with understanding the Standard.

A Standard may also include other parts, such as the following:

(1) A normative appendix sets additional requirements that need to be conformed to.

(2) An informative appendix provides additional information or guidance. They usually do not contain requirements. If an informative appendix does contain requirements, the Standard will explain when those requirements apply.

(3) A Bibliography lists documents referenced in the Standard but not as part of requirements.

Many Standards include notes. Notes provide recommendations and/or guidance only. They never contain requirements.

Preface

This Standard was prepared by the Standards Australia Committee IT-032, Biometrics and Identification.

The objective of this document is to specify security block (SB) formats (refer to AS ISO/IEC 19785.1:2023) registered in accordance with AS ISO/IEC 19785.2:2023 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.

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).

This document is identical to, and has been reproduced from, ISO/IEC 19785-4:2025, *Information technology — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications*.

As this document has been reproduced from an international document, a comma is to be read as a full point when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

© Standards Australia Limited 2025

Contents

Page

Preface ..... **v**
Foreword ..... **vii**
Introduction ..... **viii**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Abbreviated terms **2**
5 ASN.1 Security block format: general purpose **3**
5.1 Security block format owner 3
5.2 Security block format owner identifier 3
5.3 Security block format name 3
5.4 Security block format identifier 3
5.5 ASN.1 object identifier for this security block format 3
5.6 Domain of use 3
5.7 Version identifier 3
5.8 Format specification and conformance statement 3
5.8.1 General 3
5.8.2 Encryption 5
5.8.3 Integrity 7
5.8.4 Encryption and integrity 10
5.9 Encoding of abstract values 11
5.10 ASN.1 module for general-purpose security block format 11
6 ASN.1 Security block format: signature only **13**
6.1 Security block format owner 13
6.2 Security block format owner identifier 13
6.3 Security block format name 13
6.4 Security block format identifier 13
6.5 ASN.1 object identifier for this security block format 13
6.6 Domain of use 13
6.7 Version identifier 13
6.8 Format specification and conformance statement 13
7 XML Security block format: general purpose **14**
7.1 Security block format owner 14
7.2 Security block format owner identifier 14
7.3 Security block format name 14
7.4 Security block format identifier 14
7.5 ASN.1 object identifier for this security block format 14
7.6 Domain of use 14
7.7 Version identifier 14
7.8 Format specification and conformance statement 15
7.8.1 General 15
7.8.2 Element <sbX> 15
7.8.3 Element <Version> 15
7.8.4 Element <EncryptionRelatedData> 16
7.8.5 Element <SignatureRelatedData> 16
7.8.6 Encryption and integrity 16
7.8.7 XML schema of the security block 17
Bibliography **18**

© Standards Australia Limited 2025

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 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.

© Standards Australia Limited 2025

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

© Standards Australia Limited 2025