



DPC: 24/30490408 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 21 June 2024

Origin: International

Latest date for receipt of comments: 14 August 2024

Project No. 2024/00984

Responsible committee: IST/44/-/2 Biometric technical interfaces

Interested committees:

Title: Draft BS EN ISO/IEC 19785-4 BS EN ISO/IEC 19785-4 Information technology - Common Biometric Exchange Formats Framework. Part 4: Security block format specifications.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 14 August 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 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

ICS: ISO ics

ISO/IEC JTC 1/SC 37

Secretariat: **ANSI**

Voting begins on:
2024-06-21

Voting terminates on:
2024-09-13

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 19785-4:2024(en)

Full document details: 24/30490408 DC

 **Documents**
Document Sharing Hub
© ISO/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Abbreviated terms	3
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	4
5.8 Format specification and conformance statement	4
5.8.1 General	4
5.8.2 Encryption	5
5.8.3 Integrity	7
5.8.4 Encryption and integrity	10
5.9 Encoding of abstract values	10
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	14
7.8.1 General	14
7.8.2 Element <sbX>	15
7.8.3 Element <Version>	15
7.8.4 Element <EncryptionRelatedData>	15
7.8.5 Element <SignatureRelatedData>	16
7.8.6 Encryption and integrity	16
7.8.7 XML schema of the security block	16
Bibliography	18

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 19785-4:2010/Cor. 1:2013.

The main changes are as follows:

- [Clauses 5](#) and [6](#) have been technically revised.
- [Clause 7](#) has been added.
- 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 defined in the first edition (ISO/IEC 19785-4:2010), are deprecated and are not recommended for use in new implementations.

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. Biometric data used in biometric verification and identification must be 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 (Security policy is a term in the security technology and has nothing to do with contracts or law. It is a policy determined in and applied to an organization or system). This document provides for both the integrity and encryption of biometric data.

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, 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 authenticated biometric. The optional use of ACBio instances is an important part of the provision of a telebiometric authentication infrastructure^[8].

