

~~Date: 2024-09-09~~

ISO/IEC ~~DIS~~ FDIS 19785-4.2:2024(en)

ISO/IEC-JTC-1/SC-37/~~WG-2~~

Secretariat:-_ANSI

Date: 2025-03-12

Information technology — Common **biometric exchange formats framework** — 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

Partie 4: Spécifications de format de bloc de sécurité

~~COPYRIGHT PROTECTED DOCUMENT~~

FDIS stage

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 19785-4

<https://standards.iteh.ai/catalog/standards/iso/f5ef56b6-b0b1-419c-8a37-23f4bbe8c6dd/iso-iec-fdis-19785-4>

© ISO/IEC 2025

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 • ~~CP 401~~

CH-1214 Vernier, Geneva, ~~Switzerland~~

~~Tel.~~Phone: + 41 22 749 01 11

~~Fax~~ + 41 22 749 09 47

E-mail: copyright@iso.org

www.iso.org

Website: www.iso.org

Published in Switzerland

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 19785-4

<https://standards.iteh.ai/catalog/standards/iso/f5ef56b6-b0b1-419c-8a37-23f4bbe8c6dd/iso-iec-fdis-19785-4>

Contents—Page

Foreword	vi
Introduction	viii
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	4
5.7 Version identifier	4
5.8 Format specification and conformance statement	4
5.9 Encoding of abstract values	15
5.10 ASN.1 module for general-purpose security block format	15
6 ASN.1 Security block format: signature only	20
6.1 Security block format owner	20
6.2 Security block format owner identifier	20
6.3 Security block format name	20
6.4 Security block format identifier	20
6.5 ASN.1 object identifier for this security block format	20
6.6 Domain of use	21
6.7 Version identifier	21
6.8 Format specification and conformance statement	21
7 XML Security block format: general purpose	21
7.1 Security block format owner	21
7.2 Security block format owner identifier	21
7.3 Security block format name	22
7.4 Security block format identifier	22
7.5 ASN.1 object identifier for this security block format	22
7.6 Domain of use	22
7.7 Version identifier	22
7.8 Format specification and conformance statement	22
Bibliography	28
Foreword	v
Introduction	vii
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	4
5.6	Domain of use	4
5.7	Version identifier	4
5.8	Format specification and conformance statement	4
5.8.1	General	4
5.8.2	Encryption	6
5.8.3	Integrity	7
5.8.4	Encryption and integrity	11
5.9	Encoding of abstract values	12
5.10	ASN.1 module for general-purpose security block format	12
6	ASN.1 Security block format: signature only	14
6.1	Security block format owner	14
6.2	Security block format owner identifier	14
6.3	Security block format name	14
6.4	Security block format identifier	14
6.5	ASN.1 object identifier for this security block format	14
6.6	Domain of use	14
6.7	Version identifier	15
6.8	Format specification and conformance statement	15
7	XML Security block format: general purpose	15
7.1	Security block format owner	15
7.2	Security block format owner identifier	15
7.3	Security block format name	15
7.4	Security block format identifier	15
7.5	ASN.1 object identifier for this security block format	15
7.6	Domain of use	16
7.7	Version identifier	16
7.8	Format specification and conformance statement	16
7.8.1	General	16
7.8.2	Element <sbX>	16
7.8.3	Element <Version>	17
7.8.4	Element <EncryptionRelatedData>	17
7.8.5	Element <SignatureRelatedData>	17
7.8.6	Encryption and integrity	18
7.8.7	XML schema of the security block	18
	Bibliography	20

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~~ 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~~ the SB formats in ASN.1 ~~are~~ were specified in ~~Clauses 5~~ ~~Clauses 5~~ and ~~6~~. ~~The one in Clause 5 is designed to be as general as possible while another SB format specified in Clause 6 is designed to provide a basic security provision and supports integrity only. The 6;~~
- ~~the~~ the SB format for general purpose in XML ~~is~~ was newly added ~~in Clause 7~~ as Clause 7;
- ~~Formats~~ 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 ~~www.iso.org/members.html and www.iec.ch/national-committees~~.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 19785-4

<https://standards.iteh.ai/catalog/standards/iso/f5ef56b6-b0b1-419c-8a37-23f4bbe8c6dd/iso-iec-fdis-19785-4>

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.

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 2010

~~version~~previous edition of this document, have been removed ~~from the document~~ as they are considered deprecated and are not recommended for use in new implementations

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 19785-4

<https://standards.iteh.ai/catalog/standards/iso/f5ef56b6-b0b1-419c-8a37-23f4bbe8c6dd/iso-iec-fdis-19785-4>

Information technology — Common ~~biometric exchange formats framework~~ — 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