



**International  
Standard**

**ISO/IEC 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*

**Second edition  
2025-07**

[ISO/IEC 19785-4:2025](https://standards.iteh.ai/catalog/standards/iso/f5ef56b6-b0b1-419c-8a37-23f4bbe8c6dd/iso-iec-19785-4-2025)

<https://standards.iteh.ai/catalog/standards/iso/f5ef56b6-b0b1-419c-8a37-23f4bbe8c6dd/iso-iec-19785-4-2025>

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

ISO/IEC 19785-4:2025

<https://standards.iteh.ai/catalog/standards/iso/f5ef56b6-b0b1-419c-8a37-23f4bbe8c6dd/iso-iec-19785-4-2025>



**COPYRIGHT PROTECTED DOCUMENT**

© 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  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>iv</b>
<b>Introduction</b>	<b>v</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>2</b>
<b>4 Abbreviated terms</b>	<b>3</b>
<b>5 ASN.1 Security block format: general purpose</b>	<b>3</b>
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	6
5.8.3 Integrity	7
5.8.4 Encryption and integrity	11
5.9 Encoding of abstract values	11
5.10 ASN.1 module for general-purpose security block format	12
<b>6 ASN.1 Security block format: signature only</b>	<b>14</b>
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	14
6.8 Format specification and conformance statement	14
<b>7 XML Security block format: general purpose</b>	<b>15</b>
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	15
7.7 Version identifier	15
7.8 Format specification and conformance statement	16
7.8.1 General	16
7.8.2 Element <sbX>	16
7.8.3 Element <Version>	16
7.8.4 Element <EncryptionRelatedData>	17
7.8.5 Element <SignatureRelatedData>	17
7.8.6 Encryption and integrity	17
7.8.7 XML schema of the security block	18
<b>Bibliography</b>	<b>20</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.

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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://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](http://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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).