

ISO/IEC 19785-4:2025-07 (E)

Information technology - Common Biometric Exchange Formats Framework - Part 4: Security block format specifications

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..... 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
- 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..... 14
 - 6.8 Format specification and conformance statement..... 14
- 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..... 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
- Bibliography..... 20