



Information technology — Common Biometric Exchange Formats Framework —

Part 4: Security block format specifications

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Cadre de formats d'échange biométriques communs —

Partie 4: Spécifications de format de bloc de sécurité

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 19785-4:2010 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

1. Add the following description at the end of 5.4:

7 (0007 Hex). This has been registered in accordance with ISO/IEC 19785-2 when BER encodings (See ISO/IEC 8825-1) are applied.

2. Add the following subclause after 5.5.3:

5.5.4 The case of BER encodings

{iso registration-authority cbeff(19785) organizations(0) jtc-sc37 (257) sb-formats(3)
general-purpose(0) ber-encoding(7)}

or, in XML value notation,

1.1.19785.0.257.3.0.7

3. Replace the definition of type `SubBlockForACBio` in 5.8.1.4 with:

```
SubBlockForACBio ::= SEQUENCE {
    bpuIOIndex INTEGER,
    acbioInstance [0] EXPLICIT ACBioInstance
}
```

4. Replace the definition of type `EnvelopeRelatedData` in 5.8.2.1.2 with:

```
EnvelopeRelatedData ::= SEQUENCE {
    version CBEFFSBVersion DEFAULT v1,
    originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
    recipientInfos RecipientInfos,
    encryptedContentRelatedInfo EncryptedContentRelatedInfo
}
```

5. Replace the definition of type `CBEFFSBVersion` in a) in 5.8.2.1.2 with:

```
CBEFFSBVersion ::= INTEGER { v1(1) } ( v1, ... )
```

6. Replace d) in 5.8.2.1.2 with:

d) The field `encryptedContentRelatedInfo` of type `EncryptedContentRelatedInfo` consists of two fields as follows:

```
EncryptedContentRelatedInfo ::= SEQUENCE {
    contentType IdentifierEncryptedContent,
    contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier
}
```

where the field `contentType` identifies the content type of the encrypted content with type `IdentifierEncryptedContent` and the field `contentEncryptionAlgorithm` identifies the content-encryption algorithm with any associated parameters, used to encrypt the biometric data. The same content-encryption algorithm and content-encryption key are used for all recipients.

`IdentifierEncryptedContent` is defined as follows:

```
IdentifierEncryptedContent OBJECT IDENTIFIER ::= { id-cbeffbDB }
```

7. Replace the definition of type `EncryptionRelatedData` in 5.8.2.2.1 with:

```
EncryptionRelatedData ::= SEQUENCE {
    version CBEFFSBVersion DEFAULT v1,
    encryptedContentRelatedInfo EncryptedContentRelatedInfo
}
```

8. Replace the definition of type `SignatureRelatedData` in 5.8.3.1.2 with:

```
SignatureRelatedData ::= SEQUENCE {
```