INTERNATIONAL STANDARD

ISO/IEC 18033-2

First edition
2006-05-01

AMENDMENT 1
2017-11

Information technology — Security techniques — Encryption algorithms —

Part 2:
Asymmetric ciphers

AMENDMENT 1: FACE

Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement —

Partie 2: Chiffres asymétriques

AMENDEMENT 1: FACE

Reference number
ISO/IEC 18033-2:2006/Amd.1:2017(E)

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A list of all parts in the ISO/IEC 18033 series can be found on the ISO website.

Information technology — Security techniques — Encryption algorithms —

Part 2: Asymmetric ciphers

AMENDMENT 1: FACE

Introduction

Replace the Introduction with the following:

Introduction

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights. The holders of these patent rights have assured the ISO and IEC that they are willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from

— IBM Corporation. Address: North Castle Drive, Armonk, NY 10504 USA,

— NTT Corporation. Address: 9-11 Midori-Cho 3-chome, Musashino-shi, Tokyo 180-8585, Japan, and

— Hitachi, Ltd. Address: 6-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8220, Japan.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and/or IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up-to-date information concerning patents.

Scope, NOTE

Replace:

— ECIES-HC; PSEC-HC; ACE-HC: generic hybrid ciphers based on ElGamal encryption;

with the following:

— ECIES-HC; PSEC-HC; ACE-HC; FACE-HC: generic hybrid ciphers based on ElGamal encryption;

8.1.2

Replace:

— *ECIES-KEM* (described in Clause 10.2),

— *PSEC-KEM* (described in Clause 10.3),

— *ACE-KEM* (described in Clause 10.4), and

— *RSA-KEM* (described in Clause 11.5).

with the following:

— *ECIES-KEM* (described in 10.2),

— *PSEC-KEM* (described in 10.3),

— *ACE-KEM* (described in 10.4),

— *FACE-KEM* (described in 10.5), and

— *RSA-KEM* (described in 11.5).

8.1.2

Replace NOTE 1 with the following:

NOTE 1 As a matter of convention, the corresponding generic hybrid ciphers built from these key encapsulation mechanisms via the generic hybrid construction in 8.3 should be called (respectively) *ECIES-HC*, *PSEC-HC*, *ACE-HC*, *RSA-HC*, and *FACE-HC*.

Clause 10

Add the following after "*ACE-KEM* is described in Clause 10.4":

— *FACE-KEM* is described in 10.5.

Clause 10

Add the following after 10.4.4:

10.5 *FACE-KEM*

The key encapsulation mechanism *FACE-KEM* is described in 10.5.

NOTE *FACE-KEM* is based on a series of research papers (see References [43] to [46]).

10.5.1 System parameters

FACE-KEM is a family of key encapsulation mechanisms, parameterized by the following system parameters:

— Γ: a concrete group

$$\Gamma = \left(\mathcal{H}, \mathcal{G}, \mathbf{g}, \mu, \nu, \mathcal{E}, \mathcal{D}, \mathcal{E}', \mathcal{D}'\right);$$

— *KDF*: a key derivation function, as described in 6.2;

— *Hash*: a cryptographic hash function, as described in 6.1;

— *CofactorMode*: one of two values: 0 or 1.

— *KeyLen*: a positive integer.

— *TagLen*: a positive integer.

Any combination of allowable system parameters (in 6.1.1, 6.2.1, 10.1.1) is allowed, except for the following restrictions:

— $Hash.len$ shall be less than $\log_{256}\mu$.

— If $\nu = 1$, then *CofactorMode* shall be 0.

— If $\nu > 1$, then *CofactorMode* may be 1 provided $\gcd(\mu, \nu) = 1$.

NOTE The value of *CofactorMode* is used only by the decryption algorithm.

10.5.2 Key generation

The key generation algorithm *FACE-KEM.KeyGen* takes no input, and runs as follows.

a) Generate numbers a_1, a_2 uniformly at random from the range $[0..\mu)$.

b) Compute the group elements

$$\mathbf{g}_1 = a_1 \cdot \mathbf{g},\ \mathbf{g}_2 = a_2 \cdot \mathbf{g}.$$

c) Generate numbers x_1, x_2, y_1, y_2 uniformly at random from the range $[0..\mu)$.

d) Compute the group elements

$$\mathbf{c} = x_1 \cdot \mathbf{g}_1 + x_2 \cdot \mathbf{g}_2,\ \mathbf{d} = y_1 \cdot \mathbf{g}_1 + y_2 \cdot \mathbf{g}_2.$$

e) Output the public key $\mathbf{g}_1, \mathbf{g}_2, \mathbf{c}, \mathbf{d}$.

f) Output the private key $x_1, x_2, y_1, y_2 \in [0..\mu)$.

10.5.3 Encryption

The encryption algorithm *FACE-KEM.Encrypt* takes as input a public key, consisting of

$$\mathbf{g}_1, \mathbf{g}_2, \mathbf{c}, \mathbf{d} \in \mathcal{G},$$

together with an encryption option fmt that specifies the format to be used for encoding group elements. It runs as follows.

a) Generate a number r uniformly at random from the range $[0..\mu)$.

b) Compute group elements

$$\boldsymbol{u}_1 = r \cdot \mathbf{g}_1,\ \boldsymbol{u}_2 = r \cdot \mathbf{g}_2.$$

c) Compute the octet strings

$$EU_1 = \mathcal{E}(\boldsymbol{u}_1, fmt),\ EU_2 = \mathcal{E}(\boldsymbol{u}_2, fmt).$$

d) Compute the integer

$$\alpha = OS2IP\left(Hash.eval\left(EU_1 \| EU_2\right)\right).$$

e) Compute the integer

$$r' = \alpha r \bmod \mu.$$

f) Compute the group element

$$\mathbf{v} = r \cdot \mathbf{c} + r' \cdot \mathbf{d}.$$

g) Set $EV = \mathcal{E}(\mathbf{v}, fmt)$.

h) Set $Len = KeyLen + TagLen$.

i) Set $W = KDF(EV, Len)$.

j) Parse W as $W = \langle W_1, \ldots, W_{Len} \rangle$ of Len octets.

k) Set $K = \langle W_1, \ldots, W_{KeyLen} \rangle$ of $KeyLen$ octets.

l) Set $T = \langle W_{KeyLen+1}, \ldots, W_{Len} \rangle$ of $TagLen$ octets.

m) Set $C_0 = EU_1 \| EU_2 \| T$.

n) Output the ciphertext C_0 and the secret key K.

10.5.4 Decryption

The decryption algorithm *FACE-KEM.Decrypt* takes as input a private key, consisting of

$$x_1, x_2, y_1, y_2 \in [0..\mu),$$

and ciphertext C_0. It runs as follows.

a) Parse C_0 as $C_0 = EU_1 \| EU_2 \| T$, where EU_1, EU_2 are octet strings such that for some (uniquely determined) group elements $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathcal{H}$, $\boldsymbol{u}_1 = \mathcal{D}(EU_1)$, $\boldsymbol{u}_2 = \mathcal{D}(EU_2)$. This step **fails** if C_0 cannot be so parsed. Check that $\{EU_1, EU_2\}$ is a consistent set of valid encodings; if not, then **fail**.

b) If CofactorMode $= 0$ and $\nu > 1$: test if $\boldsymbol{u}_1 \in \mathcal{G}$ and $\boldsymbol{u}_2 \in \mathcal{G}$; if either $\boldsymbol{u}_1 \notin \mathcal{G}$ or $\boldsymbol{u}_2 \notin \mathcal{G}$, then **fail**.

c) If CofactorMode $= 0$, set

$$\hat{\boldsymbol{u}}_1 = \boldsymbol{u}_1,\ \hat{\boldsymbol{u}}_2 = \boldsymbol{u}_2;$$

$$\hat{x}_1 = x_1,\ \hat{x}_2 = x_2,\ \hat{y}_1 = y_1,\ \hat{y}_2 = y_2.$$

d) If *CofactorMode* $= 1$, set:

$$\hat{\boldsymbol{u}}_1 = \nu \cdot \boldsymbol{u}_1,\ \hat{\boldsymbol{u}}_2 = \nu \cdot \boldsymbol{u}_2;$$

$$\hat{x}_1 = \nu^{-1} x_1 \bmod \mu,\ \hat{x}_2 = \nu^{-1} x_2 \bmod \mu,\ \hat{y}_1 = \nu^{-1} y_1 \bmod \mu,\ \hat{y}_2 = \nu^{-1} y_2 \bmod \mu.$$

e) Compute the integer:

$$\alpha = OS2IP\left(Hash.eval\left(EU_1 \| EU_2\right)\right).$$

f) Compute the integers:

$$t_1 = \hat{x}_1 + \alpha \hat{y}_1 \bmod \mu,\ t_2 = \hat{x}_2 + \alpha \hat{y}_2 \bmod \mu.$$

g) Compute the group element:

$$\mathbf{v} = t_1 \cdot \hat{\boldsymbol{u}}_1 + t_2 \cdot \hat{\boldsymbol{u}}_2 .$$

h) Set $EV = \mathcal{E}(\mathbf{v}, fmt)$.

i) Set $Len = KeyLen + TagLen$.

j) Set $W = KDF(EV, Len)$.

k) Parse W as $L = \langle W_1, \ldots, W_{Len} \rangle$ of Len octets.

l) Set $K = \langle W_1, \ldots, W_{KeyLen} \rangle$ of $KeyLen$ octets.

m) Set $T_{dec} = \langle W_{KeyLen+1}, \ldots, W_{Len} \rangle$ of $TagLen$ octets.

n) Test if $T_{dec} = T$; if not then **fail**.

o) Output the secret key K.

Annex A

Replace the title:

ASN.1 syntax for object identifiers

with the following:

Object identifiers

Annex A

Replace the first paragraph:

This annex gives ASN.1 syntax for object identifiers, public keys, and parameter structures to be associated with the algorithms specified in this part of ISO/IEC 18033.

with the following:

Annex A gives object identifiers, public keys, and parameter structures to be associated with the algorithms specified in this document.

Annex A

Replace:

```
-- Key encapsulation mechanisms --
id-kem-ecies OID::= { id-kem ecies(1) }
id-kem-psec OID::= { id-kem psec(2) }
id-kem-ace OID::= { id-kem ace(3) }
id-kem-rsa OID::= { id-kem rsa(4) }
```

with the following:

```
-- Key encapsulation mechanisms --
id-kem-ecies OID::= { id-kem ecies(1) }
```