

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)

**Documents**  
Document Sharing Hub  
© ISO/IEC 2017



## **COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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  
Ch. de Blandonnet 8 • CP 401  
CH-1214 Vernier, Geneva, Switzerland  
Tel. +41 22 749 01 11  
Fax +41 22 749 09 47  
copyright@iso.org  
www.iso.org

## 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](http://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](http://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](http://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](http://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:

- $\Gamma$ : a concrete group  
$$\Gamma = (\mathcal{H}, \mathcal{G}, \mathbf{g}, \mu, \nu, \mathcal{E}, \mathcal{D}, \mathcal{E}', \mathcal{D}');$$
- *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.