INTERNATIONAL STANDARD

**ISO/IEC 18033-5**

First edition
2015-12-01

**AMENDMENT 1**
2021-02

# Information technology — Security techniques — Encryption algorithms —

## Part 5: Identity-based ciphers

## AMENDMENT 1: SM9 mechanism

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

*Partie 5: Chiffrements identitaires*

*AMENDEMENT 1: Mécanisme SM9*



Reference number
ISO/IEC 18033-5:2015/Amd.1:2021(E)



ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

 

# 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC 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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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.

This document was prepared by Technical Committee ISO/IEC JTC1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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

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.

# Information technology — Security techniques — Encryption algorithms —

# Part 5: Identity-based ciphers

## AMENDMENT 1: SM9 mechanism

*Introduction*

Replace the second sentence of the fourth paragraph with the following:

> The specified mechanisms are the BF identity-based encryption mechanism, the SK identity-based key encapsulation mechanism, the BB1 identity-based key encapsulation mechanism and the SM9 identity-based key encapsulation mechanism and encryption mechanisms.

Insert the following sentence between the sixth and seventh paragraphs.

> The content of 9.4 follows Reference [8].



*4.1*

Insert the following line at the end of the table:

$\lceil x \rceil$ smallest integer greater than or equal to the real number $x$.



*5.1*

Replace the first sentence with the following:

> The schemes specified in this document make use of four cryptographic transformations, *IHF1*, *SHF1*, *PHF1* and *IHF2* as specified below.

*5.1*

Add the following to the end:

> Annex A lists the object identifiers which shall be used to identify the algorithms specified in this document.
>
> Annex B describes security considerations for each specified mechanism.
>
> Annex C provides numerical examples.
>
> Annex D introduces techniques which can be used to remove the decryption capability of the PKG, and thereby reduce the level of trust required in this entity.

*5.5*

Add new subclause 5.5 as follows:

### 5.5 The function *IHF2*

*IHF2* is based on the key derivation function *KDF2* defined in ISO/IEC 18033-2. *KDF2*($x$, $l$) parameterized by a cryptographic hash function takes an octet string $x$ and a non-negative integer $l$ as input, and outputs an octet string of length $l$. *KDF2-a*($x$, $b$) outputs the first $b$ bits from *KDF2*($x$, $\lceil b/8 \rceil$). *IHF2* take three items as input and outputs an integer in a specified range.

Input:

— A bit string $str \in \{0,1\}^*$

— A security parameter $\kappa \in \{128\}$

— A non-negative integer $n$ with bit-length $b_n$

Output:

— An integer $x$, $0<x<n$.

Operation: Perform the following steps.

a) If $\kappa = 128$, *KDF2* uses SM3 as the hash function.

b) Let $hlen = 8\lceil(5\ b_n)/32\rceil$.

c) Compute $Ha = KDF2\text{-}a(str, hlen)$.

d) Output (*BS2IP* (*Ha*) mod ($n$-1)) + 1.



*7.3.1*



Replace the fifth paragraph with the following:

The allowable data encapsulation mechanisms are those described in ISO/IEC 18033-2.

*7.4.1*

Insert new NOTE 4 at the end as follows:

NOTE 4 The third mechanism defined in 9.4 will work to encrypt messages with either DEM2 or DEM3, which are specified in ISO/IEC 18033-2. In these DEMs, the required hash function is SM3, specified in ISO/IEC 10118-3, and the required block cipher is described in ISO/IEC 18033-3. The required message authentication code is generated by the evaluation function $MA.eval(K'', MS) = \text{SM3}(MS \,||\, K'')$, where $K''$ is a secret key which is part of the session key $K$, and $MS$ is the octet string to be authenticated as specified in DEM2 and DEM3. The label input to both DEMs is empty.

*9.1*

Replace the first sentence with the following:

In this clause, three identity-based key encapsulation mechanisms are specified. These mechanisms use the following primitives.

Replace list item b) with the following:

 