INTERNATIONAL STANDARD

ISO/IEC 18033-5

First edition
2015-12-01

AMENDMENT 1

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

PROOF/ÉPREUVE

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 κ = 128, *KDF2* uses SM3 as the hash function.

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

c) Compute Ha = KDF2-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 $MA.eval(K'', MS) = \mathrm{SM3}(MS \,||\, K'')$, 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:

b) Four hash functions:

Add new fourth list item as follows:

— H_4: $\{0,1\}^* \to Z_p^*$ where $H_4(s) = IHF2(0x01 \,||\, s \,||\, 0x03, p, \kappa)$

9.4

Add new Subclause 9.4 as follows:

9.4 The SM9 key encapsulation mechanism

9.4.1 Set up

The setup operation creates public system parameters and a master-secret key. This operation shall be completed by the private key issuer, an entity which shall be trusted by its subscribers.

The steps to create public system parameters and a master-secret key are:

a) Establish the set of base groups G_1, G_2, G_3, and a pairing e: $G_1 \times G_2 \to G_3$. The order of each group is p.

b) Select a random generator Q_1 in G_1 and a random generator Q_2 in G_2.

c) Generate a random master secret s in Z_p^*. Calculate the corresponding R as sQ_1.

d) Pre-calculate the pairing value $J = e(R, Q_2)$.

e) Make the system parameters and the master-public key set $params = <J, Q_1, Q_2, G_1, G_2, G_3, e, p>$ and $mpk = R$ available. Secure the master-secret key $msk = s$.

9.4.2 Private key extraction

The extract operation takes an arbitrary identity string ID_b in $\{0,1\}^*$ and calculates the corresponding private key sk_{ID} in G_2. The algorithm to compute the private key sk_{ID} corresponding to an identity string ID_b is as follows:

Input:

— The system parameters $params = <J, Q_1, Q_2, G_1, G_2, G_3, e, p>$

— The master-public key $mpk = R$

— The master-secret key $msk = s$

— An identity string ID_b

Output:

— The derived private key sk_{ID}, an element of G_2.

Operation: Use the following steps to compute sk_{ID}.

a) Compute $M = H_4(ID_b)$.

b) If $M + s = 0 \bmod p$, output "error" and stop.

c) Compute $t = (M+s)^{-1}s \bmod p$.

d) Compute $sk_{ID} = tQ_2$.

e) Output sk_{ID}.

The correctness of the value sk_{ID} can be verified by using the following algorithm:

Input:

— The system parameters *params* = $<J, Q_1, Q_2, G_1, G_2, G_3, e, p>$

— The master-public key *mpk* = R

— An identity string ID_b

— The corresponding private key sk_{ID}

Output:

— The value "valid" if sk_{ID} is consistent with *params*, *msk* and ID_b, and "invalid" otherwise.

Operation: Use the following steps.

a) Compute $M = H_4(ID_b)$.

b) Compute $T = e(MQ_1 + R, sk_{ID})$.

c) If $T = J$, then output the value "valid", otherwise output the value "invalid".

9.4.3 Session key encapsulation

The encapsulate operation (*KEM.Enc*) takes an arbitrary identity string ID_b in $\{0,1\}^*$ and the master-public key *mpk* = R with the system parameters *parms*, and outputs the pair $<K, CT_{KEM}>$ where K is a session key to be used to encrypt a message, and CT_{KEM} is the encapsulation of K to be transmitted to the receiver.

The steps to compute the encapsulation values are:

a) Select a random integer r in Z_p^*.

b) Compute $M = H_4(ID_b)$.

c) Compute $E = r(MQ_1 + R)$.

d) Compute $B = J^r$.

e) Compute $K = KDF2\text{-}a(EC2OSP(E) \,||\, FE2OSP(B) \,||\, ID_b, klen)$, where *klen* is the bit-length of the required session key.

f) Set $\mathrm{CT_{KEM}} = \mathrm{EC2OSP(E)}$.

g) Output $<K, CT_{KEM}>$.

9.4.4 Session key de-encapsulation

The de-encapsulate operation (*KEM.Dec*) takes an encapsulated value CT_{KEM} computed for identity ID_b and the private sk_{ID} that corresponds to ID_b, and computes the key value K that can be used to decrypt the message that was encrypted by the sender.

The steps to compute the de-encapsulation key are:

a) Parse CT_{KEM} as an element $E = OS2ECP(CT_{KEM})$.

b) Check whether E is in G_1; if not, output "error".

c) Compute $B = e(E, sk_{ID})$.

d) Compute $K = KDF2\text{-}a(EC2OSP(E) \,||\, FE2OSP(B) \,||\, ID_b, klen)$, where *klen* is the bit-length of the required session key.

e) Output K.

Annex A

Insert the following lines after ib-enc-mechanism-bf:

```
  ib-enc-mechanism-sm9a OID ::= { ib-enc sm9a(2) }   -- sm9 kem with DEM2 as in 7.4.1

  ib-enc-mechanism-sm9b OID ::= { ib-enc sm9b(3) }   -- sm9 kem with DEM3 as in 7.4.1
```

Insert the following lines after ib-kem-mechanism-bb1:

```
  ib-kem-mechanism-sm9 OID ::= { ib-kem sm9(3) }

  sm9-dem-one-time-mac OID ::= { ib-kem-mechanism-sm9 one-time-mac(1) }
```

Insert the following lines after { OID ib-enc-mechanism-bf PARMS HashFunction }:

```
      |{ OID ib-enc-mechanism-sm9a PARMS HashFunction }

      |{ OID ib-enc-mechanism-sm9b PARMS HashFunction }
```

Insert the following line after { OID ib-kem-mechanism-bb1 PARMS HashFunction }:

```
      |{ OID ib-kem-mechanism-sm9 PARMS HashFunction }
```

Annex B

Replace the last sentence with the following:

> Security analyses of the BF, SK, BB1 and SM9 mechanisms can be found in References [4], [5], [3] and [9], respectively.

Annex C

Add new Clause C.4 as follows:

C.4 SM9 ID-based key encapsulation mechanism

C.4.1 Example 1

C.4.1.1 Set up

This example makes use of the same Barreto-Naehrig elliptic curve $y^2 = x^3 + 5$ used in ISO/IEC 14888-3:2018, F.15.1. An element $\underline{A}_0$ in Fq^2 is represented as $\underline{A}_{0,1}\sigma+\underline{A}_{0,0}$, where $\underline{A}_{0,0}$ and $\underline{A}_{0,1}$ are elements of Fq and σ is an element of Fq^2 such that $\sigma^2 + 2 = 0 \bmod q$. Let ν be an element of Fq^4 such that $\nu^2 - \sigma = 0$ in Fq^2 and ω be an element of Fq^{12} such that $\omega^3 - \nu = 0$ in Fq^4, an element of Fq^{12} is represented as $\underline{A}\omega^2+\underline{B}\omega+\underline{C}$, where $\underline{A}$, $\underline{B}$, $\underline{C}$ are elements of Fq^4 which are represented as $\underline{A} = \underline{A}_1\nu + \underline{A}_0$, $\underline{B} = \underline{B}_1\nu + \underline{B}_0$, $\underline{C} = \underline{C}_1\nu + \underline{C}_0$ respectively, and $\underline{A}_0$, $\underline{A}_1$, $\underline{B}_0$, $\underline{B}_1$, $\underline{C}_0$, $\underline{C}_1$ are elements of Fq^2. In this towered fashion, an element of Fq^{12} is represented as a vector $(\underline{A}_{1,1}, \underline{A}_{1,0}, \underline{A}_{0,1}, \underline{A}_{0,0}, \underline{B}_{1,1}, \underline{B}_{1,0}, \underline{B}_{0,1}, \underline{B}_{0,0}, \underline{C}_{1,1}, \underline{C}_{1,0}, \underline{C}_{0,1}, \underline{C}_{0,0})$ with components in Fq. P is a point on the curve $y^2 = x^3 + 5$, Q is a point on the corresponding sextic twist $y^2 = x^3 + 5\sigma$. Pairing e is implemented as the optimal R-ate pairing on two input points P and $\phi(Q)$, i.e.,