INTERNATIONAL STANDARD

ISO/IEC 18033-5

First edition
2015-12-01

Information technology — Security techniques — Encryption algorithms —

Part 5: Identity-based ciphers

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

Partie 5: Chiffrements identitaires

Reference number
ISO/IEC 18033-5:2015(E)

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

Contents

Page

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 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).

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

ISO/IEC 18033 consists of the following parts, under the general title *Information technology — Security techniques — Encryption algorithms*:

— *Part 1: General*

— *Part 2: Asymmetric ciphers*

— *Part 3: Block ciphers*

— *Part 4: Stream ciphers*

— *Part 5: Identity-based ciphers*

Further parts may follow.

Annex A forms a normative part of this part of ISO/IEC 18033. Annex B, Annex C and Annex D are informative only.

Introduction

Use of a public key encryption mechanism requires reliable identification of the correct public key to be used for encryption. A public key infrastructure (PKI) provides functions to give a trusted link between an entity and to enable the current status of the public key to be determined. In a PKI, a certification authority (CA) issues a certificate binding a public key to the owner's identifier together with other key specific information, e.g. the validity period. If a public key is deemed to be invalid before its expiry date, then potential users of the public key need to be notified, e.g. by the issue of a CA-signed Certificate Revocation List (CRL). The generation and distribution of certificates and CRLs poses a major management problem, which the mechanisms in this part of ISO/IEC 18033 are designed to address. On encrypting, an encryptor first obtains the CRL and checks the current status of the certificate. Then the encryptor verifies the certificate, and finally encrypts a message. Therefore, the encryptor has to be provided with some means of accessing the current CRL, and additionally it should not require excessive time and computational resources for checking the validity of a certificate whenever it encrypts a message.

Identity-based encryption (IBE) is a type of asymmetric encryption that allows a decryptor to set its public key to an arbitrary string. By setting the public key to an easily identifiable string (e.g. an e-mail address), an encryptor can gain assurance in its correctness without using a certificate. Moreover, if a short validity period can be arranged, significantly shorter than the updating period of a CRL in a conventional PKI, an encryptor can generate a ciphertext without checking the current status of the public key because revocation is unlikely to occur during such a short period. As a result IBE is expected to reduce the certificate management workload.

The use of IBE requires a Private Key Generator (PKG), which generates private keys for all decryptors using its master secret key; this contrasts with 'traditional' asymmetric encryption mechanisms, such as those specified in ISO/IEC 18033-2, in which entities generate their own public/private key pairs. As a result, use of IBE is only appropriate when it is acceptable for a third party to have decryption access to all encrypted data.

The identity-based encryption mechanisms are specified in Clauses 8 and 9. The specified mechanisms are the BF identity-based encryption mechanism, the SK identity-based key encapsulation mechanism, and the BB1 identity-based key encapsulation mechanism.

The specifications in this part of ISO/IEC 18033 do not prescribe protocols for reliably obtaining public values, for proof of possession of a private key, or for validation of either public values or private keys.

Certain sections of Clause 5, Clause 8 and Clause 9 of this part of ISO/IEC 18033 have been reprinted with permission from [7] IEEE Std 1363.3-2013 - IEEE Standard for Identity-Based Cryptographic Techniques using Pairings. Reprinted with permission from IEEE. Copyright 2013. All rights reserved.

Annex A gives the assignment of object identifiers to the algorithms specified in this part of ISO/IEC 18033. Annex B describes security considerations for each specified mechanism and 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.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 18033 may involve the use of patents. The 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 licences 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 the ISO and IEC. Information may be obtained from the following:

Patent holder name: Nippon Telegraph and Telephone Corporation

Postal address: Licensing Group, Intellectual Property Center

9-11, Midori-cho, 3-Chome Musashino-Shi, Tokyo 180-8585 Japan

Patent holder name: IBM Corporation

Postal address: IBM Intellectual Property Licensing

North Castle Drive, Armonk, NY 10504 USA

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 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.

Information technology — Security techniques — Encryption algorithms —

Part 5: Identity-based ciphers

1 Scope

This part of ISO/IEC 18033 specifies identity-based encryption mechanisms. For each mechanism the functional interface, the precise operation of the mechanism, and the ciphertext format are specified. However, conforming systems may use alternative formats for storing and transmitting ciphertexts.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18033-1, *Information technology — Security techniques — Encryption algorithms — Part 1: General*

ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18033-1 and the following apply.

3.1
decryptor
entity which decrypts ciphertexts

3.2
encryptor
entity which encrypts plaintexts

3.3
hybrid encryption
encryption performed using a hybrid cipher

3.4
identifier
object that represents something and enables one to identify it

3.5
identity string
string that represents an identity

3.6
identity-based cipher
asymmetric cipher in which the encryption algorithm takes an arbitrary string as a public key

3.7
identity-based hybrid cipher
cipher which is both a hybrid cipher and an identity-based cipher

3.8
identity-based key encapsulation mechanism
key encapsulation mechanism for which the encryption process takes an arbitrary string as a public key

3.9
master-public key
public value uniquely determined by the corresponding master-secret key

3.10
master-secret key
secret value used by the private key generator to compute private keys for an IBE algorithm

3.11
private key extraction algorithm
method used by the private key generator to compute private keys for an IBE algorithm

3.12
private key generator
entity or function which generates a set of private keys

3.13
public key encryption
encryption performed using an asymmetric cipher

3.14
string
ordered sequence of symbols

3.15
set up
process by which the system parameters for an IBE algorithm are selected

3.16
set up algorithm
process which generates a master-secret key and the corresponding master-public key, together with some part of the system parameters

3.17
system parameters
parameters for cryptographic computation including a selection of a particular cryptographic scheme or function from a family of cryptographic schemes or functions, or from a family of mathematical spaces

3.18
trusted third party
security authority, or its agent, trusted by other entities with respect to security related activities

4 Symbols, abbreviated terms and conversion functions

For the purposes of this part of ISO/IEC 18033, the symbols and abbreviated terms given in ISO/IEC 18033-1 and the following apply.

4.1 Symbols

$[a,\ldots,b)$	the set of integers $\{x : a \leq x < b\}$.
$\tilde{x} \oplus \tilde{y}$	if $\tilde{x}$ and $\tilde{y}$ are bit/octet strings of the same length, the bit-wise exclusive-or (XOR) of the two strings.
$\langle x_1, \ldots, x_l \rangle$	a tuple $x_1, \ldots, x_l$ of elements.
$\tilde{x} \| \tilde{y}$	if $\tilde{x}$ and $\tilde{y}$ are bit/octet strings, the concatenation of the two strings $\tilde{x}$ and $\tilde{y}$, resulting in the string consisting of $\tilde{x}$ followed by $\tilde{y}$.
$\gcd(a,b)$	for integers a and b, the greatest common divisor of a and b, i.e., the largest positive integer that divides both a and b (or 0 if $a = b = 0$).
$a \mid b$	a relation between integers a and b that holds if and only if a divides b i.e., there exists an integer c such that $b = ac$.
$a \nmid b$	a relation between integers a and b that holds if and only if a does not divide b i.e., there does not exist any integer c such that $b = ac$.
$a \equiv b \pmod{n}$	for a non-zero integer n, a relation between integers a and b that holds if and only if a and b are congruent modulo n, i.e., $n \mid (a - b)$.
$a \pmod{n}$	for integer a and positive integer n, the unique integer $r \in [0,\ldots,n)$ such that $r \equiv a \pmod{n}$.
$a^{-1} \pmod{n}$	for integer a and positive integer n, such that $\gcd(a,n) = 1$, the unique integer $b \in [0,\ldots,n)$ such that $ab \equiv 1 \pmod{n}$.
$GF(q)$	the finite field containing q elements, where q is a power of a prime.
$E / GF(q)$	an elliptic curve defined over the field $GF(q)$.
$E(GF(q))$	the additive group of points on the elliptic curve $E / GF(q)$.
$E(GF(q))[n]$	the subgroup of $E(GF(q))$ consisting of all points of order n.
$\#E(GF(q))$	the number of points of an elliptic curve defined over the field $GF(q)$.

4.2 Abbreviated terms

CT	ciphertext, an octet string.
DEM	data encapsulation mechanism.
IBE	identity-based encryption.
IBhE	identity-based hybrid encryption.
ID	octet string uniquely assigned to a decryptor.
ID_b	binary representation of ID.
K	session key for DEM.
κ	security parameter.

KEM key encapsulation mechanism.

L label, an octet string.

mpk master-public key of IBE.

Msg plaintext, an octet string.

Msg_b binary representation of Msg.

msk master-secret key of IBE.

$parms$ system parameters of IBE.

PKG private key generator.

sk_{ID} private key corresponding to ID of IBE.

4.3 Conversion functions

The following conversion functions are given in ISO/IEC 18033-2.

$BS2IP$ bit string to integer conversion primitive.

$BS2OSP$ bit string to octet string conversion primitive.

$EC2OSP$ elliptic curve to octet string conversion primitive.

$FE2OSP$ field element to octet string conversion primitive.

$FE2IP$ field element to integer conversion primitive.

$I2BSP$ integer to bit string conversion primitive.

$I2OSP$ integer to octet string conversion primitive.

$OS2ECP$ octet string to elliptic curve conversion primitive.

$OS2FEP$ octet string to field element conversion primitive.

$OS2IP$ octet string to integer conversion primitive.

$OS2BSP$ octet string to bit string conversion primitive.

$Oct(m)$ the octet whose integer value is m.

$Len(n)$ the number of octets of an integer n.

5 Cryptographic transforms

5.1 General

The schemes specified in this part of ISO/IEC 18033 make use of three cryptographic transformations, *IHF1*, *SHF1* and *PHF1* as specified below. These transformations make use of hash-functions specified in ISO/IEC 10118-3.

5.2 The function *IHF*1

IHF1 is based on four hash-functions specified in ISO/IEC 10118-3, namely SHA-224, SHA-256, SHA-384 and SHA-512. It inputs a string of bits and outputs an integer in a specified range.

Input:

— A string $str \in \{0,1\}^*$

— A security parameter $\kappa \in \{112, 128, 192, 256\}$

— An integer n, $0 < n < 2^{4\kappa}$

Output:

— An integer $v, 0 \le v < n$.

Operation: Perform the following steps.

a) If $\kappa = 112$ then let H be SHA-224;

else if $\kappa = 128$ then let H be SHA-256;

else if $\kappa = 192$ then let H be SHA-384;

else if $\kappa = 256$ then let H be SHA-512.

b) Let h_0 be an all-zero bit string of length 2κ.

c) Let $t_1 = h_0 || str$.

d) Let $h_1 = H(t_1)$.

e) Let $v_1 = BS2IP(h_1)$.

f) Let $t_2 = h_1 || str$.

g) Let $h_2 = H(t_2)$.

h) Let $a_2 = BS2IP(h_2)$.

i) Let $v_2 = 2^{2\kappa} v_1 + a_2$.

j) Output v_2 mod n.

5.3 The function *SHF*1

Returns an n-bit string that is based on a cryptographic hash function applied to an input string.

Input:

— A string $str \in \{0,1\}^*$

