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/IEC 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, 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

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Symbols, abbreviated terms and conversion functions **2**
4.1 Symbols 3
4.2 Abbreviated terms 3
4.3 Conversion functions 4

5 Cryptographic transforms **5**
5.1 General 5
5.2 The function *IHF*1 5
5.3 The function *SHF*1 5
5.4 The function *PHF*1 6

6 General model for identity-based encryption **7**
6.1 Composition of algorithms 7
6.2 Plaintext length 7
6.3 Use of labels 8
6.4 Ciphertext format 8
6.5 IBE operation 8

7 General model for identity-based hybrid encryption **9**
7.1 General 9
7.2 Identity-based key encapsulation 9
7.2.1 Composition of algorithms 9
7.2.2 Prefix-freeness 10
7.3 Data encapsulation 10
7.3.1 Composition of algorithms 10
7.4 Identity-based hybrid encryption operation 10
7.4.1 System parameters 10
7.4.2 Set up 11
7.4.3 Private key extraction 11
7.4.4 Encryption 11
7.4.5 Decryption 11

8 Identity-based encryption mechanism **11**
8.1 General 11
8.2 The BF mechanism 12
8.2.1 Set up 12
8.2.2 Private key extraction 12
8.2.3 Encryption 13
8.2.4 Decryption 14

9 Identity-based hybrid encryption mechanisms **14**
9.1 General 14
9.2 The SK key encapsulation mechanism 14
9.2.1 Set up 14
9.2.2 Private key extraction 15
9.2.3 Session key encapsulation 16
9.2.4 Session key de-encapsulation 16
9.3 The BB1 key encapsulation mechanism 17
9.3.1 Set up 17
9.3.2 Private key extraction 17
9.3.3 Session key encapsulation 18

© ISO/IEC 2015 – All rights reserved

9.3.4 Session key de-encapsulation 18
Annex A (normative) **Object identifiers** **20**
Annex B (informative) **Security considerations** **21**
Annex C (informative) **Numerical examples** **22**
Annex D (informative) **Mechanisms to prevent access to keys by third parties** **35**
Bibliography **36**

 © ISO/IEC 2015 – All rights reserved

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.

© ISO/IEC 2015 – All rights reserved

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

 © ISO/IEC 2015 – All rights reserved

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.

© ISO/IEC 2015 – All rights reserved

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

© ISO/IEC 2015 – All rights reserved