INTERNATIONAL STANDARD

ISO/IEC 19772

Second edition
2020-11

Information security — Authenticated encryption

Sécurité de l'information — Chiffrement authentifié

Reference number
ISO/IEC 19772:2020(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

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.

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 http://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 JTC 1, *Information Technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 19772:2009) which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 19772:2009/Cor 1:2014.

The main changes compared to the previous edition are as follows:

— old Clause 6 has been removed following the deprecation of mechanism 1 (OCB 2.0);

— optional additional authenticated data has been included in mechanism 5.

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.

Introduction

When data is sent from one place to another, it is often necessary to protect it in some way while it is in transit, e.g. against eavesdropping or unauthorized modification. Similarly, when data is stored in an environment to which unauthorized parties can have access, it can be necessary to protect it.

If the confidentiality of the data needs to be protected, e.g. against eavesdropping, then one solution is to use encryption, as specified in ISO/IEC 18033 (all parts) and ISO/IEC 10116. Alternatively, if it is necessary to protect the data against modification, i.e. integrity protection, then message authentication codes (MACs) as specified in ISO/IEC 9797 (all parts), or digital signatures as specified in ISO/IEC 9796 (all parts) and ISO/IEC 14888 (all parts), can be used. If both confidentiality and integrity protection are required, then one possibility is to use both encryption and a MAC or signature. While these operations can be combined in many ways, not all combinations of such mechanisms provide the same security guarantees. As a result, it is desirable to define in detail exactly how integrity and confidentiality mechanisms should be combined to provide the optimum level of security. Moreover, in some cases, significant efficiency gains can be obtained by defining a single method of processing the data with the objective of providing both confidentiality and integrity protection.

In this document, authenticated encryption mechanisms are defined. These are methods for processing data to provide both integrity and confidentiality protection. They typically involve either a specified combination of a MAC computation and data encryption, or the use of an encryption algorithm in a special way such that both integrity and confidentiality protection are provided.

The methods specified in this document have been designed to maximize the level of security and provide efficient processing of data. Some of the techniques defined here have mathematical "proofs of security", i.e. rigorous arguments supporting their soundness.

Information security — Authenticated encryption

1 Scope

This document specifies five methods for authenticated encryption, i.e. defined ways of processing a data string with the following security objectives:

— data confidentiality, i.e. protection against unauthorized disclosure of data;

— data integrity, i.e. protection that enables the recipient of data to verify that it has not been modified;

— data origin authentication, i.e. protection that enables the recipient of data to verify the identity of the data originator.

All five methods specified in this document are based on a block cipher algorithm, and require the originator and the recipient of the protected data to share a secret key for this block cipher.

Key management is outside the scope of this document. Key management techniques are defined in ISO/IEC 11770 (all parts).

Four of the mechanisms in this document, namely mechanisms 3, 4, 5 (AAD variant only) and 6, allow data to be authenticated which is not encrypted. That is, these mechanisms allow a data string that is to be protected to be divided into two parts, *D*, the data string that is to be encrypted and integrity-protected, and *A* (the additional authenticated data) that is integrity-protected but not encrypted. In all cases, the string *A* can be empty.

NOTE Examples of types of data that can need to be sent in unencrypted form, but whose integrity is to be protected, include addresses, port numbers, sequence numbers, protocol version numbers and other network protocol fields that indicate how the plaintext is to be handled, forwarded or processed.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

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 following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
additional authenticated data
AAD
data that is integrity-protected but not encrypted by the *authenticated encryption mechanism* (3.3)

3.2
authenticated encryption
(reversible) transformation of data by a cryptographic algorithm to produce *ciphertext* (3.5) that cannot be altered by an unauthorized entity without detection, i.e. it provides data confidentiality, *data integrity* (3.6), and data origin authentication

3.3
authenticated encryption mechanism
cryptographic technique used to protect the confidentiality and guarantee the origin and integrity of data, and which consists of two component processes: an *encryption* (3.8) algorithm and a *decryption* (3.7) algorithm

3.4
block cipher
symmetric encryption system (3.15) with the property that the *encryption* (3.8) algorithm operates on a block of *plaintext* (3.13), i.e. a string of bits of a defined length, to yield a block of *ciphertext* (3.5)

[SOURCE: ISO/IEC 18033-1:2015, 2.9]

3.5
ciphertext
data which has been transformed to hide its information content

[SOURCE: ISO/IEC 10116:2017, 3.2]

3.6
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO/IEC 9797-1:2011, 3.4]

3.7
decryption
reversal of a corresponding *encryption* (3.8)

[SOURCE: ISO/IEC 18033-1:2015, 2.16]

3.8
encryption
(reversible) transformation of data by a cryptographic algorithm to produce *ciphertext* (3.5), i.e., to hide the information content of the data

[SOURCE: ISO/IEC 18033-1:2015, 2.21]

3.9
encryption system
cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an *encryption* (3.8) algorithm, a *decryption* (3.7) algorithm, and a method for generating *keys* (3.10)

[SOURCE: ISO/IEC 18033-1:2015, 2.23]

3.10
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment)

[SOURCE: ISO/IEC 18033-1:2015, 2.27]

3.11
message authentication code
MAC
string of bits which is the output of a MAC algorithm

[SOURCE: ISO/IEC 9797-1:2011, 3.9]

3.12
partition
process of dividing a string of bits of arbitrary length into a sequence of blocks, where the length of each block is n bits, except for the final block which shall contain r bits, $0 < r \leq n$

3.13
plaintext
unencrypted information

[SOURCE: ISO/IEC 10116:2017, 3.11]

3.14
secret key
key (3.10) used with symmetric cryptographic techniques by a specified set of entities

[SOURCE: ISO/IEC 18033-1:2015, 2.33]

3.15
symmetric encryption system
encryption (3.8) system based on symmetric cryptographic techniques that uses the same *secret key* (3.14) for both the *encryption* (3.8) and *decryption* (3.7) algorithms

[SOURCE: ISO/IEC 18033-1:2015, 2.40]

4 Symbols and abbreviated terms

A	additional authenticated data
C	authenticated-encrypted data string
D	data string to which an authenticated encryption mechanism is to be applied
d	block cipher decryption algorithm; $d_K(Y)$ denotes the result of block cipher decrypting the n-bit block Y using the secret key K
e	block cipher encryption algorithm; $e_K(X)$ denotes the result of block cipher encrypting the n-bit block X using the secret key K
K	secret block cipher key shared by the originator and recipient of the data to which the authenticated encryption mechanism is to be applied
m	number of blocks in the partitioned version of D
n	block length (in bits) for a block cipher
t	tag length (in bits)

0^i block of i zero bits

1^i block of i one bits

$\oplus$ bit-wise exclusive-or of strings of bits (of the same bit-length)

|| concatenation of bit strings, i.e. if A and B are blocks of bits, then $A||B$ is the block of bits obtained by concatenating A and B in the order specified

function converting a number into an a-bit block of bits

If k is an integer ($0 \le k < 2^a$), then $\#_a(k)$ is the a-bit block which, when regarded as the binary representation of a number with the most significant bit on the left, equals k.

$\#^{-1}$ function converting a block of bits to a number

If A is a block of bits, then $\#^{-1}(A)$ is the unique non- negative integer whose binary representation is A. Hence, if A has n bits, then $\#_n(\#^{-1}(A)) = A$.

$X|_s$ left-truncation of the block of bits X

If X has bit-length greater than or equal to s, then $X|_s$ is the s-bit block consisting of the left-most s bits of X.

$X|^s$ right-truncation of the block of bits X

If X has bit-length greater than or equal to s, then $X|^s$ is the s- bit block consisting of the right-most s bits of X.

$X<<1$ left shift of a block of bits X by one position

The rightmost bit of $Y = X<<1$ is always set to zero.

$X>>1$ right shift of a block of bits X by one position

The leftmost bit of $Y = X>>1$ is always set to zero.

len function taking a bit-string X as input, and which gives as output the number of bits in X

mod if a and $b > 0$ are integers, then a mod b denotes the unique integer c such that:

1) $0 \le c < b$; and

2) a-c is an integer multiple of b.

5 Requirements

The authenticated encryption mechanisms specified in this document have the following requirements.

The originator and recipient of the data to which the authenticated encryption mechanism is to be applied, shall:

a) agree on the use of a particular mechanism from those specified in this document;

b) agree on the use of a particular block cipher to be used with the mechanism (one of the block ciphers standardized in ISO/IEC 18033-3 shall be used);

c) share a secret key K: in all mechanisms except for authenticated encryption mechanism 5, this shall be a key for the selected block cipher, and in mechanism 5 it shall be a key used as input to a key derivation procedure.

In addition, each mechanism has specific requirements listed immediately before the mechanism description.

Annex A provides guidance on the use of the mechanisms defined in this document.

Annex B contains numerical examples of the operation of the mechanisms specified in this document.

Annex C provides the object identifiers which shall be used to identify the mechanisms defined in this document.

6 Authenticated encryption mechanism 2 (key wrap)

6.1 General

This clause defines an authenticated encryption mechanism commonly known as key wrap.

NOTE 1 This scheme was originally designed for authenticated encryption of keys and associated information. That is, it is designed for use with short data strings. However, the scheme can be used with arbitrary length data strings (up to a maximum of around 2^{67} bits), although it is not efficient for protecting long messages.

NOTE 2 This mode is known as AES key wrap when the AES block cipher is used, where AES stands for advanced encryption standard, a block cipher algorithm specified in ISO/IEC 18033-3:2010. AES key wrap is also specified in References [7] and [9].

6.2 Specific notation

For the purposes of the specification of this mechanism, the following symbols and notation apply:

$C_0, C_1, \ldots, C_m$	sequence of (m+1) 64-bit blocks obtained as the output of the authenticated encryption process
$D_1, D_2, \ldots, D_m$	sequence of m 64-bit blocks obtained by partitioning D, i.e. $64m$ = len(D)
$R_1, R_2, \ldots, R_m$	sequence of m 64-bit blocks computed during the encryption and decryption processes
Y	64-bit block used during the encryption and decryption processes
Z	128-bit block computed during the encryption and decryption processes

6.3 Specific requirements

The block cipher to be used with this mechanism shall be a 128-bit block cipher, i.e. it shall have n=128.

The data string D to be protected using this mechanism shall contain at least 128 bits and a multiple of 64 bits (i.e. the bit-length of D shall be $64m$ for some integer $m > 1$).

6.4 Encryption procedure

The originator shall perform the following steps to protect a data string D.

a) Partition D into a sequence of m 64-bit blocks $D_1, D_2, \ldots, D_m$, so that D_1 contains the first 64 bits of D, D_2 the next 64 bits, and so on.

b) Let Y be the 64-bit block having hexadecimal representation A6A6A6A6A6A6A6A6, i.e. in binary it equals (10100110 10100110 ... 10100110).

c) For $i = 1, 2, \ldots, m$:

   let $R_i = D_i$.

d) For $i = 1, 2, \ldots, 6m$, perform the following four steps:

   1) Let $Z = e_K(Y \,||\, R_1)$;

2) Let $Y = Z|_{64} \oplus \#_{64}(i)$;

3) For $j = 1, 2, \ldots, m\text{-}1$:

let $R_j = R_{j+1}$;

4) Let $R_m = Z|^{64}$.

e) Let $C_0 = Y$.

f) For $i = 1, 2, \ldots, m$:

let $C_i = R_i$.

The output of the above process, i.e. the authenticated-encrypted version of D, shall be the bit-string:

$C = C_0 \,||\, C_1 \,||\, \ldots \,||\, C_m$

That is, a string of $64(m+1)$ bits, that is C contains precisely 64 bits more than D.

6.5 Decryption procedure

The recipient shall perform the following steps to decrypt and verify an authenticated-encrypted string C.

a) If len(C) is not a multiple of 64 or is less than 192, then halt and output INVALID.

b) Partition C into a sequence of $m+1$ 64-bit blocks $C_0, C_1, \ldots, C_m$ so that C_0 contains the first 64 bits of C, C_1 the next 64 bits, and so on.

c) Let $Y = C_0$.

d) For $i = 1, 2, \ldots, m$:

let $R_i = C_i$.

e) For $i = 6m, 6m\text{-}1$, down to 1, perform the following four steps:

1) Let $Z = d_K([Y \oplus \#_{64}(i)] \,||\, R_m)$;

2) Let $Y = Z|_{64}$;

3) For $j = m, m\text{-}1, \ldots, 2$:

let $R_j = R_{j\text{-}1}$;

4) Let $R_1 = Z|^{64}$.

f) If Y = (10100110 10100110 … 10100110), then output $D = R_1 \,||\, R_2 \,||\, \ldots \,||\, R_m$. Otherwise, output INVALID.

7 Authenticated encryption mechanism 3 (CCM)

7.1 General

This clause defines an authenticated encryption mechanism commonly known as CCM (for counter with CBC-MAC).

NOTE CCM is due to Whiting, Housley and Ferguson.[10] The version of CCM defined here is a special case of CCM as defined in References [8] and [10].

