INTERNATIONAL STANDARD

ISO/IEC 9797-2

Third edition
2021-06

Information security — Message authentication codes (MACs) —

Part 2: Mechanisms using a dedicated hash-function

Sécurité de l'information — Codes d'authentication de message (MAC) —

Partie 2: Mécanismes utilisant une fonction de hachage dédiée

Reference number
ISO/IEC 9797-2:2021(E)

© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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

 © ISO/IEC 2021 – All rights reserved

Contents

Page

Foreword ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Symbols and notation **3**

5 Requirements **5**

6 MAC Algorithm 1 ..... **6**
6.1 General 6
6.2 Description of MAC Algorithm 1 7
6.2.1 General 7
6.2.2 Step 1 (key expansion) 7
6.2.3 Step 2 (modification of the constants and the ***IV***) 7
6.2.4 Step 3 (hashing operation) 8
6.2.5 Step 4 (output transformation) 8
6.2.6 Step 5 (truncation) 8
6.3 Efficiency 8
6.4 Computation of the constants 8
6.4.1 General 8
6.4.2 Dedicated hash-function 1 (RIPEMD-160) 9
6.4.3 Dedicated hash-function 2 (RIPEMD-128) 9
6.4.4 Dedicated hash-function 3 (SHA-1) 10
6.4.5 Dedicated hash-function 4 (SHA-256) 10
6.4.6 Dedicated hash-function 5 (SHA-512) 10
6.4.7 Dedicated hash-function 6 (SHA-384) 11
6.4.8 Dedicated hash-function 8 (SHA-224) 11
6.4.9 Dedicated hash-function 17 (SM3) 12

7 MAC Algorithm 2 ..... **12**
7.1 General 12
7.2 Description of MAC Algorithm 2 12
7.2.1 General 12
7.2.2 Step 1 (key expansion) 13
7.2.3 Step 2 (hashing operation) 13
7.2.4 Step 3 (output transformation) 13
7.2.5 Step 4 (truncation) 13
7.3 Efficiency 13

8 MAC Algorithm 3 ..... **13**
8.1 General 13
8.2 Description of MAC Algorithm 3 14
8.2.1 General 14
8.2.2 Step 1 (key expansion) 14
8.2.3 Step 2 (modification of the constants and the ***IV***) 14
8.2.4 Step 3 (padding) 15
8.2.5 Step 4 (application of the round-function) 15
8.2.6 Step 5 (truncation) 15
8.3 Efficiency 15

9 MAC Algorithm 4 ..... **15**
9.1 General 15
9.2 Description of MAC Algorithm 4 16
9.3 Encoding and padding 16
9.3.1 Integer to byte encoding 16
9.3.2 String encoding 17

© ISO/IEC 2021 – All rights reserved

9.3.3 Padding 17
9.4 KMAC128 18
9.4.1 General 18
9.4.2 Step 1 (Prepare ***newD***) 18
9.4.3 Step 2 (Prepare ***X***) 18
9.4.4 Step 3 (Generate MAC output) 18
9.5 KMAC256 18
9.5.1 General 18
9.5.2 Step 1 (Prepare ***newD***) 18
9.5.3 Step 2 (Prepare ***X***) 19
9.5.4 Step 3 (Generate MAC output) 19
9.6 KMACXOF128 19
9.6.1 General 19
9.6.2 Step 1 (Prepare ***newD***) 19
9.6.3 Step 2 (Prepare ***X***) 19
9.6.4 Step 3 (Generate MAC output) 20
9.7 KMACXOF256 20
9.7.1 General 20
9.7.2 Step 1 (Prepare ***newD***) 20
9.7.3 Step 2 (Prepare ***X***) 20
9.7.4 Step 3 (Generate MAC output) 20
Annex A (normative) **Object identifiers** **21**
Annex B (informative) **Numerical examples** **23**
Annex C (informative) **Security analysis of the MAC algorithms** **50**
Bibliography **52**

 © ISO/IEC 2021 – 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.

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 or www.iec.ch/members_experts/refdocs).

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 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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 9797-2:2011), which has been technically revised.

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

— Using dedicated hash-function 17 for MAC Algorithms 1 and 3 has been added;

— Using dedicated hash-functions 11, 12, 13 to 16, and 17 for MAC Algorithm 2 has been added;

— MAC Algorithm 4 based on Keccak, a primitive in the definition of dedicated hash-functions 13 to 16 has been added.

A list of all parts in the ISO/IEC 9797 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

© ISO/IEC 2021 – All rights reserved

Information security — Message authentication codes (MACs) —

Part 2: Mechanisms using a dedicated hash-function

1 Scope

This document specifies MAC algorithms that use a secret key and a hash-function (or its round-function or sponge function) to calculate an *m*-bit MAC. These mechanisms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorized manner.

NOTE A general framework for the provision of integrity services is specified in ISO/IEC 10181-6.

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 10118-3, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

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
block
bit-string of length L_1, i.e. the length of the first input to the round-function

[SOURCE: ISO/IEC 10118-3:2018, 3.1]

3.2
entropy
measure of the disorder, randomness or variability in a closed system

Note 1 to entry: The entropy of a random variable X is a mathematical measure of the amount of information provided by an observation of X.

[SOURCE: ISO/IEC 18031:2011, 3.11]

3.3
input data string
string of bits which is the input to a MAC algorithm

© ISO/IEC 2021 – All rights reserved

3.4
hash-code
string of bits which is the output of a hash-function

[SOURCE: ISO/IEC 10118-1:2016, 3.3]

3.5
hash-function
function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output

Note 1 to entry: Computational infeasibility depends on the specific security requirements and environment. Refer to ISO/IEC 10118-1:2016, Annex C.

[SOURCE: ISO/IEC 10118-1:2016, 3.4, modified — "feasability" in Note 1 to entry changed to "infeasability".]

3.6
initializing value
value used in defining the starting point of a hash-function

[SOURCE: ISO/IEC 10118-1:2016, 3.5, modified — Note 1 to entry removed]

3.7
MAC algorithm key
key that controls the operation of a MAC algorithm

[SOURCE: ISO/IEC 9797-1:2011, 3.8]

3.8
message authentication code
MAC
string of bits which is the output of a MAC algorithm

Note 1 to entry: A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2[1]).

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

3.9
message authentication code algorithm
MAC algorithm
algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties:

— for any key and any input string the function can be computed efficiently;

— for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the ith input string may have been chosen after observing the value of the first i-1 function values (for integer $i > 1$)

Note 1 to entry: A MAC algorithm is sometimes called a cryptographic check function (see for example ISO 7498-2).

Note 2 to entry: Computational infeasibility depends on the user's specific security requirements and environment.

© ISO/IEC 2021 – All rights reserved

[SOURCE: ISO/IEC 9797-1:2011, 3.10 modified — "feasability" in Note 2 to entry changed to "infeasability".]

3.10
output transformation
function that is applied at the end of the MAC algorithm, before the truncation operation

[SOURCE: ISO/IEC 9797-1:2011, 3.12]

3.11
padding
appending extra bits to a data string

[SOURCE: ISO/IEC 10118-1:2016, 3.7]

3.12
round-function
function ϕ (..,..) that transforms two binary strings of lengths L_1 and L_2 to a binary string of length L_2 that is used iteratively as part of a hash-function, where it combines a data string of length L_1 with the previous output of length L_2 or the initializing value

Note 1 to entry: The literature on this subject contains a variety of terms that have the same or similar meaning as round-function. Compression function and iterative function are some examples.

[SOURCE: ISO/IEC 10118-1:2016, 3.8]

3.13
security strength
number associated with the amount of work required to break a cryptographic algorithm or system and specified in bits such that security strength s bits implies the required number of operations is 2^s

Note 1 to entry: Computationally infeasible in 3.2, 3.6 and 3.10 implies the security strength is at least 112 bits. Refer to ISO/IEC 10118-1:2016, Annex C.

3.14
word
string of 32 bits used in dedicated hash-functions 1, 2, 3, 4, 8 and 17 or a string of 64 bits used in dedicated hash-functions 5, 6, 9 and 10 of ISO/IEC 10118-3:2018

[SOURCE: ISO/IEC 10118-3:2018, 3.2, modified — added specific bit lengths, 32 bits or 64 bits, for different dedicated hash-functions.]

4 Symbols and notation

C_i, C'_i	constant words used in the round-functions
D	input data string, i.e. the data string to be input to the MAC algorithm
$\bar{D}$	padded data string
$j \sim X$	string obtained from a string X at least j bits in length by taking the leftmost j bits of X
H	hash-code
H', H''	strings of L_2 bits which are used in the MAC algorithm computation to store an intermediate result
h	hash-function
h'	hash-function h with modified constants and modified IV

© ISO/IEC 2021 – All rights reserved