International Standard

ISO/IEC 9797-2

Third edition
2021-06

TECHNICAL CORRIGENDUM 1
2024-11

# Information security — Message authentication codes (MACs)

## Part 2: Mechanisms using a dedicated hash-function

## TECHNICAL CORRIGENDUM 1

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

*Partie 2:*
*Mécanismes utilisant une fonction de hachage dédiée*

*RECTIFICATIF TECHNIQUE 1*

Reference number
ISO/IEC 9797-2:2021/Cor.1 :2024(en)

## COPYRIGHT PROTECTED DOCUMENT



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

Technical Corrigendum 1 to ISO/IEC 9797-2:2021 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cyber security, and privacy protection*.

# Information security — Message authentication codes (MACs) —
# Part 2:
# Mechanisms using a dedicated hash-function
## TECHNICAL CORRIGENDUM 1

*Clause 4*

Add the following at the end of the clause:

$\lceil x \rceil$ the smallest integer greater than or equal to the real number $x$

*6.2.2*

Replace the first sentence with the following:

If $K$ is shorter than 128 bits, concatenate $K$ to itself $\lceil 128/k \rceil$ times and select the leftmost 128 bits of the result to form the 128-bit key $K'$:

Replace the last equation with the following:

$$K_1 = K_1[0] \parallel K_1[1] \parallel K_1[2] \parallel K_1[3] \parallel K_1[4] \parallel K_1[5] \parallel K_1[6] \parallel K_1[7]$$

*6.4.2*

Replace the last line with the following:

$C_i' = K_1[1]$ $(64 \leq i \leq 79)$

*6.4.3*

Replace the last line with the following:

$C_i' = K_1[3]$ $(48 \leq i \leq 63)$

*6.4.5*

Replace the first sentence with the following:

The 128-bit constant strings $T_i$ for dedicated hash-function 4 are defined as follows (in hexadecimal representation):

*6.4.6*

Replace the first sentence with the following:

The 128-bit constant strings $T_i$ for dedicated hash-function 5 are defined as follows (in hexadecimal representation):

*6.4.7*

Replace the first sentence with the following:

The 128-bit constant strings $T_i$ for dedicated hash-function 6 are defined as follows (in hexadecimal representation):

*6.4.8*

Replace the first sentence with the following:

The 128-bit constant strings $T_i$ for dedicated hash-function 8 are defined as follows (in hexadecimal representation):

*8.2.2*

Replace the first sentence with the following:

If $K$ is shorter than 128 bits, concatenate $K$ to itself $\lceil 128/k \rceil$ times and select the leftmost 128 bits of the result to form the 128-bit key $K'$:

*9.4.3*

Replace the last three sentences with the following:

The characters 00 in item c) specify two zero bits.

NOTE The number 168 is the rate (in bytes) of SPONGE[*f*, *pad*, 1 344], where $f =$ KECCAK-$p$[1 600, 24]. SPONGE[*f*, *pad*, 1 344] is referred to as KECCAK[256] in Reference [12].

*9.5.3*

Replace the last three sentences with the following:

The characters 00 in item c) specify two zero bits.

NOTE The number 136 is the rate (in bytes) of SPONGE[*f*, *pad*, 1 088], where $f =$ KECCAK-$p$[1 600, 24]. SPONGE[*f*, *pad*, 1 088] is referred to as KECCAK[512] in Reference [12].

*9.6.2*

Replace the first sentence of NOTE with the following:

When used as a XOF, KMAC is computed by setting the encoded output length to 0, as shown in *right_encode*(0) in item b).

*9.6.3*

Replace the last three sentences with the following:

The characters 00 in item c) specify two zero bits.

NOTE The number 168 is the rate (in bytes) of SPONGE[*f*, *pad*, 1 344], where $f =$ KECCAK-$p$[1 600, 24]. SPONGE[*f*, *pad*, 1 344] is referred to as KECCAK[256] in Reference [12].

*9.7.3*

Replace the last three sentences with the following:

The characters 00 in item c) specify two zero bits.

NOTE The number 136 is the rate (in bytes) of SPONGE[*f*, *pad*, 1 088], where $f =$ KECCAK-$p$[1 600, 24]. SPONGE[*f*, *pad*, 1 088] is referred to as KECCAK[512] in Reference [12].

*B.2.7*

Replace the element in the second row and second column with the following:

192-bit MAC result: leftmost 192 bits of

*B.3.1*

Replace the third bullet point with the following:

$m = 128$ for dedicated hash-functions 4, 12, 14 and 17;

*B.3.1*

Replace the fifth bullet point with the following:

$m = 192$ for dedicated hash-functions 6 and 15; and

*B.4.1*

Replace the two bullet points with the following:

$m = 80$ for dedicated hash-functions 1 and 3;

$m = 64$ for dedicated hash-function 2;

$m = 128$ for dedicated hash-functions 4 and 17;

$m = 256$ for dedicated hash-function 5;

$m = 192$ for dedicated hash-function 6; and

$m = 112$ for dedicated hash-function 8.

*Annex C*

Replace the sentence below the NOTE with the following:

— It has been proven that MAC Algorithm 2 is secure if the following assumption holds:[8]

*Annex C*

Replace the first sentence of the last paragraph with the following:

For KMAC256, $c = 512$ and $r = 1\,088$.

*Bibliography*

Remove entry [7] from the list.

ICS 35.030



iso.org