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 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 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.

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