INTERNATIONAL STANDARD

ISO/IEC 9797-3

First edition
2011-11-15

AMENDMENT 1
2020-02

Information technology — Security techniques — Message Authentication Codes (MACs) —

Part 3: Mechanisms using a universal hash-function

AMENDMENT 1

Technologies de l'information — Techniques de sécurité — Codes d'authentification de message (MAC) —

Partie 3: Mécanismes utilisant une fonction de hachage universelle

AMENDEMENT 1

Reference number
ISO/IEC 9797-3:2011/Amd.1:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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

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.

Information technology — Security techniques — Message Authentication Codes (MACs) —

Part 3:
Mechanisms using a universal hash-function

AMENDMENT 1

Clause 5

Insert the following paragraph at the end of Clause 5 (after the NOTE):

> Annex A defines object identifiers that shall be used to identify the algorithms specified in this document. Annex B provides numerical examples for the algorithms specified in this document, and Annex C gives information on the security properties of these algorithms.

6.5.1

Replace the first sentence with the following:

> GMAC can be used with any block cipher from ISO/IEC 18033-3 that has a block length of 128 bits. The resulting MAC is t bits long, where t is a multiple of 8 satisfying $96 \leq t \leq 128$ ($t = 64$ is also permitted for specialized applications – see 6.5.2).

6.5.2

Replace the second list item with the following:

— The tag length, t, shall be selected such that t is a multiple of 8 satisfying $96 \leq t \leq 128$. The only permitted exception to this is tag length $t = 64$. However, this tag length is only permitted for specialized applications, and should only be used with great care.

NOTE For some voice or video applications, short authentication tags (i.e. where $t = 64$) can be appropriate. In such applications the forgery of some fraction of individual authenticated "packets" can be tolerable, because each packet of data in a large stream can carry very little of the overall meaning. However, even for such applications, short tags can be problematic for GMAC as a result of targeted forgery attacks of the type documented in Appendix B of [9]. Detailed guidance on use of tag length $t = 64$ is provided in Appendix C of [9].

Annex B

Change the title to Numerical examples.

Annex B, text and table titles

Change all occurrences of "test vector" to "numerical example".

Bibliography

Change Bibliographic entry [9] to:

[9] National Institute of Standards and Technology, *NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. November 2007