INTERNATIONAL STANDARD

ISO/IEC 9797-1

Second edition
2011-03-01

AMENDMENT 1
2023-08

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

Part 1: Mechanisms using a block cipher

AMENDMENT 1

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

Partie 1: Mécanismes utilisant un chiffrement par blocs

AMENDEMENT 1

ISO/IEC 9797-1:2011/Amd 1:2023
https://standards.iteh.ai/catalog/standards/sist/f335-94f6-4c34-8065-e21d59f193b9/iso-iec-9797-1-2011-amd-1-2023

Reference number
ISO/IEC 9797-1:2011/Amd. 1:2023(E)

© ISO/IEC 2023

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9797-1:2011/Amd 1:2023
https://standards.iteh.ai/catalog/standards/sist/44def335-94f6-4c34-8065-e21d59f193b9/iso-iec-9797-1-2011-amd-1-2023

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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 2023 – 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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/IEC 9797-1:2011/Amd 1:2023
https://standards.iteh.ai/catalog/standards/sist/44de1555-94f0-4c54-8065-c21d59119 5b9/iso-iec-9797-1-2011-amd-1-2023

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 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 2023 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9797-1:2011/Amd 1:2023
https://standards.iteh.ai/catalog/standards/sist/44def335-94f6-4c34-8065-e21d59f193b9/iso-iec-9797-1-2011-amd-1-2023

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

Part 1:
Mechanisms using a block cipher

AMENDMENT 1

Clause 4

Add the following symbol after the description of $d_K(C)$:

e block cipher used in the MAC algorithm.

7.4

Add the following paragraph above Figure 4:

MAC Algorithm 3 should not be used in new applications because it was designed for use with an outdated cryptographic primitive.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 9797-1:2011/Amd 1:2023
https://standards.iteh.ai/catalog/standards/sist/44def335-94f6-4c34-8065-e21d59f193b9/iso-iec-9797-1-2011-amd-1-2023

C.2, first paragraph

Replace the last sentence of the paragraph with:

The motivation for this removal is that the additional security offered is lower than anticipated.

© ISO/IEC 2023 – All rights reserved