

This is a preview of "ISO 16609:2022". [Click here to purchase the full version from the ANSI store.](#)

Third edition
2022-08

Financial services — Requirements for message authentication using symmetric techniques

*Services financiers — Exigences pour l'authentification des messages
utilisant des techniques symétriques*



Reference number
ISO 16609:2022(E)

© ISO 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

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

This is a preview of "ISO 16609:2022". [Click here to purchase the full version from the ANSI store.](#)

Contents

| | Page |
|---|-----------|
| Foreword | iv |
| Introduction | v |
| 1 Scope | 1 |
| 2 Normative references | 1 |
| 3 Terms and definitions | 1 |
| 4 Principles | 3 |
| 4.1 Protection of authentication keys..... | 3 |
| 4.2 Message authentication elements..... | 3 |
| 4.3 Detection of duplication, loss or sequence errors..... | 4 |
| 5 Procedures for message authentication | 4 |
| 5.1 MAC generation..... | 4 |
| 5.2 MAC placement..... | 5 |
| 5.3 MAC verification..... | 5 |
| 5.4 Approved authentication mechanisms based on the ISO/IEC 9797 series..... | 5 |
| 5.4.1 General..... | 5 |
| 5.4.2 Approved message authentication mechanisms based on ISO/IEC 9797-1..... | 5 |
| 5.4.3 Approved message authentication mechanisms based on ISO/IEC 9797-2..... | 6 |
| 5.4.4 Approved message authentication mechanisms based on ISO/IEC 9797-3..... | 7 |
| 5.4.5 Implementation recommendations..... | 8 |
| Annex A (informative) Protection against duplication and loss using MIDs | 9 |
| Annex B (informative) General tutorial information | 11 |
| Bibliography | 13 |

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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).

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 Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

This third edition cancels and replaces the second edition (ISO 16609:2012), which has been technically revised.

The main changes are as follows:

- updated to include newer hash functions specified in updated versions of the ISO/IEC 9797 series.

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.

This is a preview of "ISO 16609:2022". [Click here to purchase the full version from the ANSI store.](#)

Introduction

A message authentication code (MAC) is a data field used to verify the authenticity of a message, generated by the sender of the message using a key shared with the recipient. The message and the MAC are transmitted together. The recipient recalculates the MAC using the transmitted message and compares it with the transmitted MAC, which allows detection of an altered message. While non-keyed message integrity methods, such as checksums, only provide a method to detect *accidental* alteration of the message, MACs additionally detect deliberate alteration, as the adversary would not have access to the key used to generate the MAC.

A MAC can also be used as a means to confirm integrity of stored data.

This document has been prepared so that institutions involved in financial services activities wishing to implement message authentication can do so in a manner that is secure and facilitates interoperability between separate implementations.

This document identifies ciphers, hash functions and algorithms from the ISO/IEC 9797 series that are specifically approved for secure banking purposes.

General tutorial information can be found in [Annex B](#).