AS ISO 16609:2025
ISO 16609:2022

Australian STANDARD®

STANDARDS Australia

Financial services — Requirements for message authentication using symmetric techniques



AS ISO 16609:2025

This Australian Standard® was prepared by IT-005, Financial Transaction Systems. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 04 April 2025.

This Standard was published on 24 April 2025.

The following are represented on Committee IT-005:

ANZ Banking Group
Australian Payments Network
Australian Securities and Investments Commission
Coles Group
Commonwealth Bank of Australia
Diebold Nixdorf
EFTPOS Payments Australia
National Australia Bank
New Payments Platform Australia
Pacific Research
SWIFT
Thales Australia
Triton Systems of Delaware
UL Transaction Security
Verisec International

This Standard was issued in draft form for comment as DR AS ISO 16609:2025.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76175 146 2

AS ISO 16609:2025
ISO 16609:2022

Financial services — Requirements for message authentication using symmetric techniques

First published as AS ISO 16609:2025.

COPYRIGHT

© ISO 2025 — All rights reserved
© Standards Australia Limited 2025

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

How to read this Standard

This page explains the meaning of the language and structure of this Standard.

Refer to Standards Australia's Standardisation Guide 006 for more details about drafting rules.

Australian and Australian/New Zealand Standards are voluntary unless they are referenced in legislation or called up in contracts.

Requirements

To conform to a Standard, all requirements in the Standard need to be met.

A requirement is any statement in the Standard which uses the word "shall".

Recommendations, permissions and possibilities

The following words are commonly used in Standards, but statements using them do not have to be followed to conform to the Standard:

(a) "should" means that something is recommended.

(b) "may" means that something is permitted.

(c) "can" means that something is possible.

Structure of Standards

A Standard always has the following parts:

(i) The Preface states who developed the Standard, what the Standard is aiming to do, and how it relates to other documents.

(ii) The Scope states what the Standard is about, what it covers and what it does not cover.

(iii) The Normative references clause lists other documents that are referenced in the Standard as part of requirements.

(iv) The Terms and definitions clause defines important terms to help with understanding the Standard.

A Standard may also include other parts, such as the following:

(1) A normative appendix sets additional requirements that need to be conformed to.

(2) An informative appendix provides additional information or guidance. They usually do not contain requirements. If an informative appendix does contain requirements, the Standard will explain when those requirements apply

(3) A Bibliography lists documents referenced in the Standard but not as part of requirements.

Many Standards include notes. Notes provide recommendations and/or guidance only. They never contain requirements.

Preface

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems.

The objective of this document is to specify procedures, independent of the transmission process, for protecting the integrity of transmitted financial-service-related messages and for verifying that a message has originated from an authorized source, or that stored data has retained integrity. A list of block ciphers approved for the calculation of a message authentication code (MAC) is also provided. The authentication methods defined in this document are applicable to stored data and to messages formatted and transmitted both as coded character sets or as binary data.

This document is designed for use with symmetric algorithms where both sender and receiver use the same key. It does not specify methods for establishing the shared key. Its application will not protect the user against internal fraud perpetrated by the sender or the receiver, nor against forgery of a MAC by the receiver.

This document is identical to, and has been reproduced from, ISO 16609:2022, *Financial services — Requirements for message authentication using symmetric techniques*.

As this document has been reproduced from an international document, a comma is to be read as a full point when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

© Standards Australia Limited 2025

Contents

Preface ... **iii**

Foreword ... **v**

Introduction ... **vi**

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.

© Standards Australia Limited 2025

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.

© Standards Australia Limited 2025

Australian Standard®

Financial services — Requirements for message authentication using symmetric techniques

1 Scope

This document specifies procedures, independent of the transmission process, for protecting the integrity of transmitted financial-service-related messages and for verifying that a message has originated from an authorized source, or that stored data has retained integrity. A list of block ciphers approved for the calculation of a message authentication code (MAC) is also provided. The authentication methods defined in this document are applicable to stored data and to messages formatted and transmitted both as coded character sets or as binary data.

This document is designed for use with symmetric algorithms where both sender and receiver use the same key. It does not specify methods for establishing the shared key. Its application will not protect the user against internal fraud perpetrated by the sender or the receiver, nor against forgery of a MAC by the receiver.

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 8583-1, *Financial transaction card originated messages — Interchange message specifications — Part 1: Messages, data elements and code values*

ISO 11568-1, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-2, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 8583-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
algorithm
specified mathematical process for computation or set of rules which, if followed, will give a prescribed result

3.2
authentication key
cryptographic key used for authentication

3.3
beneficiary
ultimate party to be credited or paid as a result of a transfer

Note 1 to entry: There can be more than one beneficiary.

© Standards Australia Limited 2025