INTERNATIONAL STANDARD

ISO 16609

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

© ISO 2022 – All rights reserved

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**

© ISO 2022 – All rights reserved

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.

© ISO 2022 – All rights reserved

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.

© ISO 2022 – All rights reserved

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

© ISO 2022 – All rights reserved

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.

3.4
block cipher
algorithm (3.1) for computing a function which maps a fixed-length string of bits and a secret key to another string of bits with the same fixed length

3.5
checksum
fixed-length string of bits calculated from a message of arbitrary length, such that it is unlikely that a change of one or more bits in the message will produce the same string of bits, thereby aiding detection of accidental modification

3.6
cryptoperiod
defined period of time during which a specific cryptographic key is authorized for use or during which the cryptographic keys in a given system may remain in effect

3.7
date MAC computed
DMC
date on which the sender computed the *message authentication code (MAC)* (3.10)

Note 1 to entry: The DMC can be used to synchronize the authentication process through selection of the proper key.

3.8
encipherment
(reversible) transformation of data by a cryptographic *algorithm* (3.1) with a cryptographic key in order to produce ciphertext, i.e. to hide the information content of the data

3.9
identifier for authentication key
IDA
field that identifies the key to be used in authenticating the message

3.10
message authentication code
MAC
cryptographic check sum on data that uses a symmetric key to detect both accidental and intentional modification of data

3.11
MAC algorithm
keyed cryptographic *algorithm* (3.1) that produces a fixed-length string of bits – the *message authentication code (MAC)* (3.10) – from a message of arbitrary length, such that it is not feasible to compute the MAC without knowledge of the key

3.12
message authentication element
element that is to be protected by authentication

3.13
message element
contiguous group of bytes designated for a specific purpose

© ISO 2022 – All rights reserved

3.14
message identifier
MID
systems trace audit number (deprecated)
field used uniquely to identify a financial message or transaction (e.g. sending bank's transaction reference) within a given context [e.g. date MAC computed (DMC)]

Note 1 to entry: In ISO 8583-1, the MID is referred to as the systems trace audit number (STAN), which it supersedes.

3.15
receiver
party intended to receive the message

3.16
sender
party responsible for, and authorized to, send a message

3.17
universal hash function
function mapping strings of bits to fixed-length strings of bits, indexed by a parameter called the key, satisfying the property that for all distinct inputs, the probability over all keys that the outputs collide is small

[SOURCE: ISO/IEC 9797-3:2011, 3.6, modified — Note 1 to entry removed.]

3.18
value date
date on which funds are to be at the disposal of the beneficiary

4 Principles

4.1 Protection of authentication keys

Authentication keys are secret cryptographic keys that have been previously established by the sender and receiver and which are used by the MAC algorithm. Keys shall be managed in accordance with ISO 11568-1 and ISO 11568-2.

4.2 Message authentication elements

The MAC calculation shall include those data elements which require protection against fraudulent alteration. For messages, this is agreed between sender and receiver. Subject to bilateral agreement, the MAC calculation may also cover data elements not transmitted in a message (e.g. padding bits or data computable by both parties from information already shared).

The choice of data to be included in the MAC will depend on the specific application. When the following elements appear, they should be included in the calculation of the MAC:

a) transaction amount;

b) currency;

c) identifier for authentication key (IDA);

d) identification of payer and beneficiary and/or, if appropriate, their payment agent's value date;

e) message identifier (MID);

f) date and time;

© ISO 2022 – All rights reserved