

INTERNATIONAL STANDARD

**ISO
9807**

First edition
1991-12-15

Banking and related financial services — Requirements for message authentication (retail)

*Banque et services financiers liés aux opérations bancaires —
Spécifications liées à l'authentification des messages (service aux
particuliers)*



Reference number
ISO 9807 1991(E)



Documents
Document Sharing Hub

Contents

	Page
1 Scope	1
2 Normative references	1
3 Definitions	1
4 Procedures for message authentication	2
4.1 Authentication keys	2
4.2 Authentication elements	2
4.3 MAC length	2
4.4 MAC generation	2
4.5 Placement of MAC	2
5 Verification of the MAC	2
6 Approval procedure for authentication algorithms	2

Annexes

A Algorithms approved for calculation of MAC for authentication of retail messages	4
B Procedure for the review of alternative authentication algorithms	5
C Procedure to prevent exhaustive key determination	7
D Guidance on the selection of authentication elements	8
E Protection against duplication and loss	9
F Pseudo-random key generator	10
G Bibliography	11

© ISO 1991

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

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.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 9807 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Sub-Committee SC 6, *Financial transaction cards, related media and operations*.

Annexes A, B and C form an integral part of this International Standard. Annexes D, E, F and G are for information only.

Introduction

A Message Authentication Code (MAC) may be used to authenticate the origin and text of a message sent between a sender and a receiver. It is generated by the sender of the message and is transmitted together with the message concerned.

This International Standard has been prepared so that institutions involved in retail banking environments and wishing to implement message authentication can do so in a secure manner and in a way that facilitates interoperability between separate implementations.

A Message Authentication Code is a data field which may be used to verify the authenticity of a message. It is derived from the whole message or from specified data elements in the message which require protection against alteration, whether such alteration arises by accident or with intent to defraud.

This International Standard is one of a series which describes the requirements for security in the retail banking environment (See annex G.)

A related series of International Standards describes the requirement for security in the wholesale banking environment (see annex G)

The requirements of this International Standard are compatible with those in ISO 8730. Both this International Standard and ISO 8730 have a close relationship with ISO 8731, which describes algorithms which have been approved for use in message authentication.

Banking and related financial services — Requirements for message authentication (retail)

1 Scope

This International Standard specifies procedures to be used for protecting the integrity of retail banking messages and for verifying that the message originated from an authorized source. It also describes the method by which algorithms are approved for use for the authentication of retail banking messages.

Rules for data representation are not specified although it is necessary for both members of a communicating pair to use the same means for data representation. The procedures are also independent of the transmission process used.

A list of algorithms approved for the calculation of a Message Authentication Code (MAC) is given in annex A. The method to be used to approve authentication algorithms is given in annex B. The procedure to prevent exhaustive key determination is provided in annex C.

Annex D gives guidance on the selection of authentication elements. Annex E provides some general information on protection against internal fraud by sender or receiver, e.g. forgery of a Message Authentication Code by the receiver, while annex F describes a method for the generation of a pseudo-random key. Annex G consists of bibliographic references.

This International Standard does not provide for

- a) encipherment for the protection of messages against unauthorized disclosure, or
- b) protection against loss or duplication of messages, whether accidental or intentional.

This International Standard is applicable to institutions responsible for implementing techniques to authenticate messages used in a retail banking environment.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 8730 1990, *Banking — Requirements for message authentication (wholesale)*.

ISO 8731-1:1987, *Banking — Approved algorithms for message authentication — Part 1: DEA*.

ISO 8731-2 1987, *Banking — Approved algorithm for message authentication — Part 2: Message authenticator algorithms*.

3 Definitions

For the purposes of this International Standard, the following definitions apply.

3.1 algorithm: A specified mathematical process for computation.

3.2 authentication: A process used, between a sender and a receiver, to ensure data integrity and to provide data origin authentication.

3.3 authentication algorithm: An algorithm used, together with an authentication key and one or more authentication elements, for authentication.

3.4 authentication element: A message element that is to be protected by authentication.

3.5 authentication key: A cryptographic key used for authentication.