

Implementation of
ISO 8730:1990

Banking — Requirements for message authentication (wholesale)

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the Information Technology Systems Standards Policy Committee (IST/-) to Technical Committee IST/12, upon which the following bodies were represented:

- American Banks and Securities Association of London (ABSAL)
- Association for Payment Clearing Services
- British Computer Society
- Building Societies Association
- International Stock Exchange
- User Standard Forum for Information Technology (Institute of Data Processing Management)

This British Standard, having been prepared under the direction of the Information Technology System Standards Policy Committee, was published under the authority of the Board of BSI and comes into effect on 31 October 1990

© BSI 03-2000

The following BSI references relate to the work on this standard:
Committee reference IST/12
Draft for comment 88/65592 DC

ISBN 0 580 19032 3

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Foreword	iii
Text of ISO 8730	1

National foreword

This British Standard reproduces verbatim ISO 8730:1990 and implements it as the UK national standard.

This British Standard is published under the direction of the Information Technology Systems Standards Policy Committee whose Technical Committee IST/12 has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international committee any enquiries on interpretation, or proposals for change, and keep UK interests informed;
- monitor related international and European developments and promulgate them in UK.

NOTE International and European Standards, as well as overseas standards, are available from BSI Sales Department, BSI, Linford Wood, Milton Keynes, MK14 6LE

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the ISO title page, pages ii to iv, pages 1 to 22 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

INTERNATIONAL STANDARD

**ISO
8730**

Second edition
1990-05-15

Banking — Requirements for message authentication (wholesale)

Opérations bancaires — Spécifications liées à l'authentification des messages



Reference number
ISO 8730 : 1990 (E)

AVA Documents
Document Sharing Hub

Contents

	Page
Foreword	iii
Introduction	1
1 Scope	1
2 Normative references	1
3 Definitions	2
4 Protection	3
5 Generation and checking of the Message Authentication Code (MAC)	4
6 Procedures for message authentication	4
7 Approval procedure for authentication algorithms	6
Annex A (normative) Procedure for review of alternative authentication algorithms	7
Annex B (informative) Risks associated with communications control characters	8
Annex C (informative) Protection against duplication and loss	9
Annex D (informative) Example of message authentication for coded character sets: DEA	10
Annex E (informative) Example of message authentication for coded character sets: MAA	15
Annex F (informative) Framework for message authentication of standard telex formats	19
Annex G (informative) A pseudo-random key generator	22

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 approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75 % approval by the member bodies voting.

International Standard ISO 8730 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*.

This second edition cancels and replaces the first edition (ISO 8730:1986), which has been technically revised to provide an enhancement of the facilities provided in that edition.

These enhanced facilities are already available in ANSI X9.9, published in August 1986, and the new text maintains consistency with the published ANSI text.

Specific changes Introduced in this edition are

- a) Data presented for authentication may be formatted in one of five different ways. This selection process allows users to authenticate messages in the format option most suitable for the transmission process used. Correspondents must now agree upon the format option for authentication of any particular message, but this will generally be no major imposition on these parties since the mode selection will be determined by the choice of transmission process;
- b) Introduction of a new field for identifying the authentication key used (IDA field);
- c) Several definitions have also been changed to ensure consistency across related TC 68 International Standards.

Four new annexes have also been Introduced, all of which are Intended to simplify Implementation of this International Standard.

- a) Annex B describes the risks associated with the unintentional Introduction of control characters during a reformatting process, and how such risks may be minimized;
- b) Annex D and Annex E provide examples of authentication calculations using the algorithms specified in ISO 8731:1987, Parts 1 and 2;
- c) Annex F describes a means of applying this International Standard to a telex payment order formatted in accordance with the requirements of ISO 7746.

Annex A forms an integral part of this International Standard. Annex B to Annex G are for information only.

Introduction

A Message Authentication Code (MAC) is a data field transmitted with a financial message passing between correspondent financial Institutions. 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.

For any form of alteration the level of protection provided for a given algorithm is related to the length of the Message Authentication Code and of the authentication key, and to the extent to which the two correspondents are able to keep their authentication key secret. Operation of this International Standard implies acceptance of this responsibility by the correspondent parties. Approved algorithms are listed and specified in ISO 8731. Techniques for wholesale key management are specified in ISO 8732. For fraudulent attack, the mathematical security of a standard algorithm is calculated on the assumption that the potential code breaker has an arbitrary large number of plaintext messages each containing its associated MAC derived from an unchanged authentication key. The security is determined by the computational power required for the authentication key to be determined by the code breaker and by the length of the MAC.

1 Scope

This International Standard is designed for use by correspondent institutions exchanging financial messages. It may be used to authenticate messages using any wire service or other mode of communication.

This International Standard specifies methods to be used for protecting the authenticity of wholesale financial messages passing between institutions (e.g. between banks, between a bank and a corporate customer or government), by means of a Message Authentication Code (MAC). It specifies the method by which authentication algorithms are to be approved for inclusion in ISO 8731.

Application of this International Standard does not protect against internal fraud by sender or receiver, e.g., forgery of a MAC by the receiver.

This International Standard specifies a technique for protecting either the whole of the message or specified elements within it. Data presented for authentication may be formatted in one of five optional forms. These specifications may be supplemented by a group of financial institutions with a community of interest who have established their own operational arrangements (e.g., a banking consortium, a geographical grouping, an operating network, an industry-wide agreement). Selection of the appropriate option permits the authentication of messages in a manner compatible with the transmission process used.

Integrity protection applies only to the selected authentication elements. Other parts of the message are subject to undetected alterations. Assuring the integrity of the presentation of the data is the responsibility of the users (see Annex B). This International Standard provides a means for protection against duplication and loss, and a method is described in Annex C.

This International Standard is designed for use with symmetric algorithms where sender and receiver use the same key. It is intended that provision will, in due course, be made to cover the use of asymmetric algorithms. The authentication method is applicable to messages formatted and transmitted both as coded character sets and as binary data.

The standard does not specify methods of protecting against unauthorized reading and monitoring. Such protection may be achieved by encipherment of the message as described in ISO 10126¹⁾.

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. Member of IEC and ISO maintain registers of currently valid International Standards.

ISO 646:1983, *Information processing — ISO 7-bit coded character set for information interchange*.

ISO 7746:1988, *Banking — Telex formats for inter-bank messages*.

ISO 7982-1:1987, *Bank telecommunication — Funds transfer messages — Part 1: Vocabulary and data*.

¹⁾ To be published.

ISO 8601:1988, *Data elements and interchange formats — Information interchange — Representation of dates and times*.

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

ISO 8732:1988, *Banking — Key management (wholesale)*.

ISO 10126-1:—, *Banking — Procedures for message encipherment (wholesale) — Part 1: General principles²⁾*.

ISO 10126-2:—, *Banking — Procedures for message encipherment (wholesale) — Part 2: Algorithms²⁾*.

3 Definitions

For the purpose of this International Standard the following definitions apply. Terms printed in italic in the definitions are defined elsewhere in this clause.

3.1 algorithm

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

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

3.6 beneficiary; beneficiary party(les)

the ultimate party (or parties) to be credited or paid as a result of a transfer

3.7 bias

the condition where, during the generation of random or pseudo-random numbers, the occurrence of some numbers is more likely than others

3.8 cryptoperiod

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

3.9 data integrity

the property that data has not been altered or destroyed in an unauthorized manner

3.10 Date MAC Computed (DMC)

the date on which the *sender* computed the *Message Authentication Code*. This date may be used to synchronize the authentication process through selection of the proper key

3.11 data origin authentication

the corroboration that the source of data received is as claimed

3.12 decipherment

the reversal of a corresponding reversible *encipherment*

3.13 decryption

see *decipherment*

3.14 delimiter

a group of characters used to delineate the beginning and end of a data field or fields

3.15 dual control

a process of utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information whereby no single entity is able to access or utilize the materials, e.g., cryptographic key

3.16 encipherment

the cryptographic transformation of data to produce ciphertext

3.17 encryption

see *encipherment*

²⁾ To be published.