International Standard ISO 8730

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION•МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ•ORGANISATION INTERNATIONALE DE NORMALISATION

Banking — Requirements for message authentication (wholesale)

Opérations bancaires — Spécifications liées à la normalisation de l'authentification des messages

First edition — 1986-11-15

UDC 336.717.131.3 **Ref. No. ISO 8730-1986 (E)**

Descriptors : banking, banking documents, messages, authentication.

Price based on 7 pages

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.

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.*

Users should note that all International Standards undergo revision from time to time and that any reference made herein to any other International Standard implies its latest edition, unless otherwise stated.

Printed in Switzerland

Banking — Requirements for message authentication (wholesale)

0 Introduction

A Message Authentication Code (MAC) is a data field attached to a set of data (i.e. a message) passing between correspondent financial institutions and transmitted along with that set of data. 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 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 a future International Standard. Techniques for wholesale key management will be described in ISO 8732[1]. 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 plain-text messages each containing its associated MAC derived from an unchanged authentication key. The security is then equal to the computational power required for the authentication key to be determined by the code breaker. Frequent changing of authentication keys will ensure that the MAC is virtually unbreakable, i.e. cannot be determined computationally during the life cycle of the authentication key.

1 Scope

This International Standard specifies methods to be used for protecting the authenticity of wholesale messages passing between financial 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. These specifications may be supplemented by a group of financial institutions with a community of interest and who have established their own operational arrangements (e.g. a banking consortium, a geographical grouping, an operating network, an industry-wide agreement). The authentication of messages is independent of the transmission process used.

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

This International Standard does not specify methods of protecting against duplication, loss and unauthorized reading and monitoring. For protection against duplication and loss, a method is described in annex B.

NOTE — One method of protecting against unauthorized reading and monitoring is by encryption of the message.

2 Field of application

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

3 References

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

ISO 2014, *Writing of calendar dates in all-numeric form.*

ISO 7982, *Telecommunication messages in banking — Part 1 : Funds transfer messages — Vocabulary.*[1]

ISO 8227, *Information processing — Data encipherment — Specification of algorithm DEA-1.*[1]

ISO 8731, *Banking — Approved algorithms for message authentication.*[1]

[1] At present at the stage of draft.

4 Definitions

For the purpose of this International Standard the following definitions apply.

4.1 algorithm : A clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

4.2 authentication : The technique used between the sender and receiver to validate the source, and part or all of the text of a message.

4.3 authentication algorithm : A mathematical process in which the output depends upon the text (plain or cipher) and on the authentication key input to it.

4.4 authentication element : A contiguous group of characters which are to be protected by being processed by the *authentication algorithm*.

4.5 authentication key : A cryptographic key designed to be known only to the correspondent parties. When this key and the text of the message are applied to the *authentication algorithm,* the result will be the *Message Authentication Code (MAC).*

4.6 beneficiary party(ies) : The ultimate party or parties to be credited or paid as a result of a transfer.

4.7 bias : A process with respect to the generation of random or pseudo-random numbers within a specified number range whereby the occurrence of some numbers is more likely than others.

4.8 date MAC computed : The date on which the *sender* computed the *MAC.*

4.9 delimiter : A group of characters used to delineate the beginning and end of data.

4.10 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 person is able to access or utilize the materials, e.g. cryptographic key.

4.11 hexadecimal digit : A single character selected from the range 0 — 9, A — F (upper case), representing a four-bit pattern.

4.12 Message Authentication Code (MAC) : A data field, the contents of which can be used to verify the authenticity of a message.

4.13 message identifier (MID) : A field of up to sixteen alphanumeric characters used to uniquely identify a financial message or transaction.

4.14 message text : Information being conveyed or transmitted between sender and receiver, excluding header and trailer information used for transmission purposes.

4.15 receiver : The person, institution or other entity responsible for the receipt of a message.

4.16 sender : The person, institution or other entity responsible for, and authorized to, send a message.

4.17 value date : Date on which funds are to be at the disposal of the receiver.

4.18 wire service : Any telecommunication service over which messages or transmissions can be sent between subscribers (e.g. telex, TWX, S.W.I.F.T., Fedwire or other public or private networks).

5 Protection

5.1 Protection of identities of originator and recipient

In order to protect the identities of the originator and recipient, the authentication key shall be protected, and shall be restricted to use by only these two parties (or their authorized agents).

5.2 Authentication elements

5.2.1 The following authentication elements shall always be included in the calculation of the MAC :

a) date MAC computed;

b) message identifier (MID).

5.2.2 The following authentication elements shall be included in the calculation of the MAC whenever they appear in the message :

a) transaction amount;

b) currency;

c) identification of parties to be credited and debited;

d) identification of beneficiary party;

e) value date.

5.3 Protection of total message

Where correspondents wish to protect the whole text of the message, the authentication process shall be applied to the whole text (see 7.1.1.).

6 Creation and processing of the Message Authentication Code (MAC)

The sender of a message shall generate a MAC by entering (in the sequence in which they appear in the message) those authentication elements of the transmitted message that are to be protected into a standard authentication algorithm. The algorithm shall be activated by means of an authentication key, previously exchanged with the receiver, and secret to the two correspondents. This process creates the MAC, which shall then be included in the original message text as an additional data field. On receipt of the message, the receiver shall compute a reference MAC using identical data from the authentication elements, an identical authentication key and an identical algorithm. Authenticity of the data element content of the message and its source are confirmed if the receiver's computed reference MAC agrees with that transmitted within the message text.

A received MAC (and its delimiters) shall not be included in the algorithm computation.

7 Procedures for message authentication

7.1 Authentication process

Correspondents shall agree upon the algorithm to be applied and they shall also exchange a secret authentication key. The sender shall calculate a MAC using these elements. This MAC shall be included in the text of the transmitted message in such a way that it is identifiable by the receiver.

7.1.1 Entire message text

Except as specified in 7.1.2, the authentication algorithm shall be applied to the entire message text.

7.1.2 Selected authentication elements of the message

Where authentication of the entire message is impractical, the algorithm shall be applied only to the specified authentication elements (see 5.2). Such elements shall be distinguished by the techniques described in 7.4.

7.1.2.1 Authentication elements shall be taken in the order in which they appear in the message.

7.1.2.2 The sender shall select the authentication key for the receiver, according to the date, which shall also appear in the message (see 7.3).

7.1.2.3 The editing criteria (see 7.4.3) shall be applied.

7.1.2.4 The edited authentication elements shall be processed by the algorithm.

7.1.2.5 The resultant MAC shall be added to the message before transmission.

7.1.2.6 The receiver shall repeat the extraction and computation processes. The message elements shall be regarded as authenticated if the resulting reference MAC is identical to that in the received message.

7.2 Authentication key generation process

Authentication keys shall be generated using a random or pseudo-random process to ensure that :

a) the sequence of elements (e.g. bits) that constitute the key all have an equally likely chance of being generated so that any such sequence produced is drawn from the total population of all such sequences;

b) each sequence of elements produced by the generation algorithm does not appear to have any relation to its predecessor or successor;

c) the generation process is free from bias.

NOTE — Annex C is an example of a method of generating sequences that satisfies these requirements.

Dual control, where implemented, shall be accomplished by the independent generation of two, full-length preliminary keys which are combined by the modulo-2 function within the authentication device at each site.

NOTE — This process implies that no individual sees the authentication key used to compute the MAC.

7.3 Field formats

The field formats for "MAC", "Date MAC computed" and "Message identifier" shall be represented in all messages in the standard form specified below.

7.3.1 MAC

The MAC shall be expressed as eight hexadecimal digits written in two groups of four, separated by a space (hhhh hhhh); for example 5A6F 09C3.

7.3.2 Date MAC computed

The date on which the sending institution originates the message shall be expressed in accordance with ISO 2014 as year, month, day (preferably compacted, i.e. YYMMDD); for example 851101 for 1 November 1985.

7.3.3 Message identifier (MID)

The message identifier shall be expressed as one to sixteen alphanumeric characters (aaaaaaaaaaaaaaaa). Permitted characters are 0 — 9, A — Z (upper case), space, comma (,), fullstop (.), solidus (/) and hyphen (-); for example FNBC25.

7.4 Delineation and extraction of selected authentication elements

The authentication process shall be applied to authentication elements in their order of appearance in messages, and shall be subject to specific requirements for the delimiting of such elements and the editing of characters. For the purposes of delineation the authentication elements shall be either implicitly or explicitly delimited.

7.4.1 Implicit field delimiters

Implicit delimitation of an authentication element shall be achieved if its position in the message is fixed or unambiguously identified by standardized format rules. Field names, numbers, or identifying field tags, where specified by the wire service as implicit delimiters, shall be processed for authentication.

7.4.2 Explicit field delimiters

If used, explicit delimiters shall identify the beginning and end of the authentication elements and the MAC. Explicit delimiters shall be used in both variable format messages and free format areas of fixed format messages.

Beginning and ending explicit delimiters, when present, shall occur in complementary pairs without intervening explicit delimiters. There is no restriction on the number of delimited text fields in any one message; however, the Date, MID and MAC fields shall appear only once in the message. The hyphen shall appear in all explicit delimiters.

7.4.2.1 Date MAC computed : QD- and -DQ

For example QD-YYMMDD-DQ

7.4.2.2 Message identifier (MID) : QX- and -XQ

For example QX-aaaaaaaaaaaaaaaa-XQ

7.4.2.3 Other authentication elements: QT- and -TQ

For example QT-text-TQ. The text delimited in "QT-text-TQ", may be of any length allowed by the wire service. It is subject to the editing criteria specified in 7.4.3.

7.4.2.4 MAC : QM- and -MQ

For example QM-hhhh hhhh-MQ

7.4.3 Text editing for MAC calculation

All characters of authentication elements which are input to the algorithm shall be represented as 8-bit characters comprising the 7-bit code of ISO 646 preceded by a zero (e.g. 0, b7, b6 ...b1). Where this necessitates a code translation, the translation shall be for internal computational purposes only.

The following editing rules shall apply in the sequence shown on all authentication elements — implicitly and explicitly delimited — before processing by the authentication algorithm.

7.4.3.1 Each leading explicit delimiter shall be deleted and each trailing explicit delimiter shall be replaced by a single space.

7.4.3.2 Except where 7.4.3.6 would otherwise apply, a single space shall be inserted following each implicitly delimited field and at the end of each line.

7.4.3.3 Lower-case alphabetic characters (a — z) shall be translated to upper case (A — Z).

7.4.3.4 Any characters other than the letters A — Z, digits 0 — 9, space, comma (,), fullstop (.), solidus (/), asterisk (*) and hyphen (-) shall be deleted; thus carriage return, line feed, end-of-text, and other formatting and control characters shall be deleted.

7.4.3.5 All leading spaces shall be deleted.

7.4.3.6 Each sequence of consecutive spaces (internal and trailing) shall be replaced by a single space.

7.5 "Failed" MAC

When the MAC is automatically generated, i.e. by automatic extraction of authentication elements, the process may fail because of rule violations (e.g. due to nested delimiters). In that event, where human readability is required (e.g. paper, screen, or microfiche) the failure shall be indicated by eight blanks (if available) written in two groups of four, separated by a character that is not a hexadecimal digit as defined in 7.3.1, e.g. bbbb*bbbb. Where blanks are not available, zeros shall be substituted (i.e. 0000*0000).

When a received MAC does not compare with the reference MAC generated during the authentication process, failure to authenticate shall be indicated by the insertion of a non-hexadecimal printable character in place of the blank in the received MAC. Where available in the character set, an asterisk shall be used, e.g. 5A6F*09C3.

8 Approval procedure for authentication methods

Before an authentication method is authorized for inclusion in ISO 8731, it shall satisfy both of the following basic requirements :

a) be designed to serve a purpose not already covered by ISO 8731 (for example : be suitable for a different operational environment; or provide significant cost savings in implementation or in operation; or offer a greater degree of protection);

b) be sufficiently secure, reliable and stable to serve its stated purpose.

Annex A describes the way in which these objectives shall be achieved.

Annex A

Procedure for review of alternative authentication methods

(This annex forms part of the standard.)

A.1 Origination

An alternative authentication method which is to be proposed for incorporation in ISO 8731 shall be submitted by, or with the approval of, a national standards body, to the Secretariat of ISO/TC 68.

A.2 Justification of proposal

The originator shall justify a proposal by describing :

a) the purpose the proposal is designed to serve;

b) how this purpose is better achieved by the proposal than methods already in ISO 8731;

c) additional merits not described elsewhere;

d) experience in use with the new method.

A.3 Documentation

The proposed method shall be completely documented when submitted for consideration. The documentation shall include :

a) a full description of the method proposed;

b) a clear acknowledgement that the method satisfies, or is compatible with, all the requirements contained in clause 5;

c) a logic flow diagram showing the processing steps used to compute the MAC;

d) a definition and explanation of any new terms, factors, or variables introduced;

e) authentication key requirements, usage, and handling;

f) a step-by-step computation example illustrating the computation of the MAC using a typical financial message;

g) detailed information on any prior testing to which the proposed method has been subjected, particularly concerning its security, reliability and stability. Such information shall include an outline of the testing procedures used, the results of the tests, and the identity of the agency or group performing the tests and certifying the results (that is, sufficient information shall be provided to enable an independent agency to conduct the same tests and to compare the results achieved).

A.4 Public disclosure

Any method submitted for consideration shall be free from security classification. If copyright patent application has been made on the method, it shall be assessed in accordance with ISO procedures[1]. All documentation and information submitted with the request for consideration of the method shall be considered public information available to any individual, organization or agency for review and testing.

A.5 Examination of proposals

Each new proposal will be examined by ISO and a report on it prepared within 180 days of receipt (but see A.6). The report shall state if the proposal is adequately documented, if it has been properly tested and certified already, and if the proposed method satisfies the conditions and requirements of the standard. The examination may also include submission of the proposal for public review (see A.6).

A.6 Public review

When the report (A.5) recommends that public review is necessary, proposals considered suitable for acceptance shall be forwarded (with the consent of the originator) to selected agencies and institutions with an international reputation in this field. These agencies and institutions will be requested to examine and report on the proposals within 90 days of receipt.

NOTE — This period of public review may extend the 180 days allowed for preparation of the report on the proposal (see A.5).

A.7 Appeal procedure

Originators whose proposals are rejected (see A.5) may ask the Secretariat of ISO/TC 68 to have the proposals subjected to public review (see A.6) if this has not already been done. If, following submission of the public review reports, rejection is still recommended, the originator may request the TC 68 Secretariat to circulate the proposal, together with copies of all relevant reports on it, for ballot by the P-members of the technical committee, whose ruling in the matter by a simple majority of those voting shall be final.

[1] Currently the *Directives for the technical work of ISO,* 14th edition (1985), annex 1E.