INTERNATIONAL STANDARD

ISO 8730

Second edition
1990-05-15

Banking — Requirements for message authentication (wholesale)

Opérations bancaires — Spécifications liées à l'authentification des messages

INTERNATIONAL ISO

Reference number
ISO 8730 : 1990 (E)

Contents

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 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) Annexes D and 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. Annexes B to 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.

This page intentionally left blank

Banking — Requirements for message authentication (wholesale)

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 10126 [1].

1) To be published.

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.*

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: —[1], *Banking — Procedures for message encipherment (wholesale) — Part 1: General principles.*

ISO 10126-2: —[1], *Banking — Procedures for message encipherment (wholesale) — Part 2: Algorithms.*

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(ies): 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*.

3.18 hexadecimal digit: A single character in the range 0-9, A-F (upper case), representing a four bit string, as follows:

Binary	Decimal	Hexadecimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1101	13	D
1110	14	E
1111	15	F

3.19 Identifier for Authentication Key (IDA): A field that identifies the key to be used in authenticating the message.

3.20 Message Authentication Code (MAC): A code in a message between a sender and a receiver used to validate the source and part or all of the text of the message. The code is the result of an agreed calculation.

3.21 message element: A contiguous group of characters designated for a specific purpose.

3.22 Message Identifier (MID): A field used uniquely to identify a financial message or transaction (e.g., sending bank's transaction reference).

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

3.24 receiver: The institution or other entity responsible for, and authorized to, receive a message.

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

3.26 value date: Date on which funds are to be at the disposal of the beneficiary.

3.27 wire service: Any telecommunication service over which messages or transmissions can be sent between subscribers.

4 Protection

4.1 Protection of the identity of the sender

To prevent misuse of the sender's identity the authentication key shall both be protected and restricted to use by only the sending and receiving parties (or their authorized agents).

4.2 Authentication elements

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

a) Date MAC computed (DMC);

b) Message identifier (MID).

4.2.2 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) Identifier for Authentication Key (IDA);

d) Identification of parties to be credited and debited;

e) Identification of beneficiary party;

f) Value date.

4.3 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 6.5 and 6.7).

4.4 Protection against duplication or loss

To protect against duplication or loss, a unique transaction reference (or message identifier) shall be used. The Message Identifier, (MID), is a value that does not repeat before either (i) the change of date (i.e. Date MAC Computed); or (ii) the expiration of the cryptoperiod of the key used for authentication, whichever occurs first, i.e., there must not be more than one message with the same date and the same message identifier that uses the same key. This requirement may be satisfied by the inclusion of a unique sending bank's transaction reference number in a fixed format message as a message identifier. In free format messages, the MID field shall be delimited in accordance with this International Standard (see 6.3.1). A method of protection is described in annex C.

5 Generation and checking of the Message Authentication Code (MAC)

5.1 Generation

The sender of a message shall generate a MAC by processing (in the sequence in which they appear in the message) those authentication elements of the transmitted message that are to be protected by an approved authentication algorithm (see ISO 8731). The algorithm shall be activated by means of an authentication key, which is a secret between the two correspondents. This process creates the MAC, which shall then be included with the original message text as an additional data field.

5.2 Checking

On receipt of the message the receiver shall compute a reference MAC using the authentication elements, an identical authentication key and an identical algorithm. Authenticity of the content of the authentication elements and the message source are confirmed when the receiver's computed reference MAC agrees with that transmitted with the message text.

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

When a received MAC does not equal the computed reference MAC, failure to authenticate shall be indicated in accordance with 6.9.2.

The process of generating the MAC is sensitive to the sequence in which the authentication elements are processed, i.e., a change in the sequence of authentication elements after the MAC is generated will result in a failure to authenticate.

Message authentication keys shall not be used as encipherment keys.

6 Procedures for message authentication

6.1 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 appended to the text of the transmitted message in such a way that it is identifiable by the receiver. (For free format messages see 6.3.3.) The receiver repeats the computation, using the same authentication method as defined in this section. The message authenticates if the received and computed reference MACs are identical.

6.2 Format options

This International Standard provides five options for the format of data to be authenticated:

1) binary data; (6.4);

2) coded characters; (6.5); entire message text; no editing

3) coded characters; (6.6); extracted message elements; no editing

4) coded characters; (6.7); entire message text; editing

5) coded characters; (6.8); extracted message elements; editing

Option 1 is designed for the authentication of a binary string of data.

Options 2 and 3 are designed for the authentication of data in coded character sets whenever the transmission medium provides character set transparency, e.g., systems and networks designed in accordance with the open systems interconnection (OSI) model.

Options 4 and 5 are designed for the authentication of data in a restricted coded character set for use whenever the transmission medium is not transparent to the character set being used, e.g., baudot, telex, and store and forward services such as those provided by many international record carriers.

Choice of the format option is the responsibility of the correspondents and shall be subject to bilateral agreement.

6.3 Codes character sets (as used in options 2 to 5)

6.3.1 Defined message element formats

The field formats for Date MAC Computed, Identifier for Authentication Key, Message Authentication Code, and Message Identifier are represented in the form specified in this International Standard. Formats of other message elements are not specified.

The field formats shall be verified as part of the authentication process. If an authentication option that employs editing is used, then the field formats shall be verified prior to editing. If a formatting error occurs, the message will fail to authenticate. The following field formats are defined:

a) Date MAC Computed (DMC). The date on which the sending institution originates the message shall be expressed in accordance with ISO 8601 as year, month, day (preferably compacted, i.e., YYMMDD); for example 851101 for 1 November 1985;

b) Identifier for Authentication Key (IDA). This field is the identifier of the key for authentication which shall conform to the requirements for key identifiers specified in ISO 8732;

c) Message Authentication Code (MAC). The MAC shall be expressed as eight hexadecimal digits written in two groups of four, separated by a space (hhhhbhhhh); for example, 5A6Fb09C3;

d) Message Identifier (MID). The message identifier shall be expressed as one to sixteen printable characters (aaaaaaaaaaaaaaaa). Permitted characters are 0-9, A-Z (upper case), space (b), comma (,), fullstop (.), solidus (/), asterisk (*) and hyphen (-); for example, FN-BC/2.5.

6.3.2 Implicit field delimiters

Implicit delimitation of an authentication element may 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.

6.3.3 Explicit field delimiters

Explicit delimiters may be used to identify the beginning and end of message elements, including the MAC. They may be used in all coded character set options. The following explicit delimiters are specified:

a) Date MAC computed (DMC): QD- and -DQ, for example, QD-YYMMDD-DQ;

b) Identifier for Authentication Key (IDA) QK- and -KQ, for example, QK-1357BANKATOBANKB-KQ;

c) Message Authentication Code (MAC): QM- and -MQ, for example, QM-hhhhbhhhh-MQ;

d) Message Identifier (MID): QX- and -XQ, for example, QX-aaaaaaaaaaaaaaaa-XQ;

e) Other message 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.

6.3.4 Use of delimiters

Beginning and ending delimiters, when present, shall occur in complementary pairs without intervening explicit delimiters.

NOTE - If this condition is not satisfied, the message will fail to authenticate.

The message may contain any number of delimited "text" fields; however, the DMC, MID, IDA, and MAC fields shall not appear more than once each in a message.

The hyphen (-) shall appear in all explicit delimiters.

6.3.5 Character representation

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 (excluding national character assignments) 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. If the message is transformed into a different character set, the inverse transformation must be applied before beginning the authentication process.

6.3.6 Header and trailer information

Header and trailer message information added (e.g., by a network) for transmission purposes shall be omitted, i.e., shall not be part of the message text nor be included in the algorithm calculation.

6.4 Option 1: Binary data

The authentication algorithm shall be applied to the entire message text, or to parts of the message text, according to a bilateral agreement between the sender and the receiver.

6.5 Option 2: Coded characters; entire message; no editing

Where message processing is automated and the precise content of the body of the message does not change between sender and receiver, the algorithm can be applied to the entire message.

The MAC is computed over the entire message text (see example in annex D).

6.6 Option 3: Coded characters; extracted message elements; no editing

6.6.1 Use

Where authentication of the entire message is impractical, the authentication algorithm shall be applied only to the selected message elements.

The message elements shall be extracted according to the rules of 6.6.2. A MAC shall be computed on the extracted elements, taken in the order in which they appear (see example in annex D).

6.6.2 Extraction of message elements

Message elements to be authenticated shall be extracted in accordance with the following rules:

6.6.2.1 Delete all characters other than the message elements and their corresponding delimiters.

6.6.2.2 Insert a single space after each implicitly delimited message element.

6.7 Option 4: Coded characters; entire message; editing

6.7.1 Use

The MAC shall be computed on the message text following editing according to the rules of 6.7.2 (see example in annex D).

6.7.2 Editing

The following editing rules shall apply, in the sequence shown, on all message elements - implicitly and explicitly delimited - before processing by the authentication algorithm:

6.7.2.1 Each carriage return and each line feed shall be replaced by a single space.

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

6.7.2.3 Any characters other than the letters A-Z, digits 0-9, space, comma (,), fullstop (.), solidus (/), asterisk (*), open and close parentheses, and hyphen (-) shall be deleted; thus end-of-text, and other formatting and control characters shall be deleted.

6.7.2.4 All leading spaces shall be deleted.

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

6.8 Option 5: Coded characters; extracted message elements; editing

6.8.1 Use

See 6.6.1.

6.8.2 Extraction of message elements

The extraction rules of 6.6.2 shall be applied.

6.8.3 Editing

The editing rules of 6.7.2 shall be applied.

6.9 "Failed" Message Authentication Code (MAC)

6.9.1 Inability to generate 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) as a minimum the failure shall be indicated by eight spaces (if available) written in two groups of four, separated by a character that is not a hexadecimal digit, preferably an asterisk, e.g., bbbb*bbbb. Where spaces are not available, zeros shall be substituted (i.e., 0000*0000).

6.9.2 Received MAC does not authenticate

When a received MAC does not equal the reference MAC generated during the authentication process, where human readability is required, failure to authenticate shall be indicated by the insertion of a non-hexadecimal printable character in place of the space in the received MAC. Where available in the character set, an asterisk shall be used, for example, 5A6F*09C3.

6.10 Authentication keys

Authentication keys are secret cryptographic keys that have been previously exchanged by the sender and receiver and are used by the authentication algorithm. Such keys shall be randomly or pseudo-randomly generated (see annex G). Keys used for message authentication shall not be used for any other purpose. Any key used for authentication shall be protected against disclosure to unauthorized parties.

7 Approval procedure for authentication algorithms

Before an authentication algorithm 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, provide significant cost savings in implementation or in operation, offer a greater degree of protection);

b) Be sufficiently secure to serve its stated purpose.

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