INTERNATIONAL STANDARD

ISO 16609

Second edition
2012-03-15

Financial services — Requirements for message authentication using symmetric techniques

Services financiers — Exigences pour l'authentification des messages utilisant des techniques symétriques

Reference number
ISO 16609:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. 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.

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.

ISO 16609 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

This second edition cancels and replaces the first edition (ISO 16609:2004), which has been technically revised.

Introduction

A MAC (message authentication code) is a data field used to verify the authenticity of a message, generated by the sender of the message and transmitted together with it. The MAC enables an intended recipient to detect whether the message has been altered. While non-keyed message integrity methods, e.g. checksums, only protect against accidental alteration of the message, MACs additionally protect against deliberate alteration since the adversary would not have access to the key used to generate the MAC.

This International Standard 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 International Standard identifies ciphers, hash functions and algorithms from ISO 9797 (all parts) that are specifically approved for secure banking purposes.

Financial services — Requirements for message authentication using symmetric techniques

1 Scope

This International Standard specifies procedures, independent of the transmission process, for protecting the integrity of transmitted banking messages and for verifying that a message has originated from an authorized source. A list of block ciphers approved for the calculation of a message authentication code (MAC) is also provided. The authentication methods it defines are applicable to messages formatted and transmitted both as coded character sets and as binary data.

This International Standard 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, nor does it provide for encipherment for the protection of messages against unauthorized disclosure. 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 referenced documents are indispensable for the application 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/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 9797-2, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a hash-function*

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 following terms and definitions apply.

3.1
algorithm
specified mathematical process for computation or set of rules which, if followed, will give a prescribed result

3.2
authentication
process used between a sender and a receiver to ensure data integrity and provide data origin authentication

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

3.4
authentication element
message element that is to be protected by authentication

3.5
authentication key
cryptographic key used for authentication

3.6
beneficiary
ultimate party to be credited or paid as a result of a transfer

NOTE There can be more than one beneficiary.

3.7
block cipher
algorithm 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

3.8
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

3.9
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

3.10
data integrity
property pertaining to data that has not been altered or destroyed in an unauthorized manner

3.11
DMC
date MAC computed
date on which the sender computed the MAC (message authentication code)

NOTE The DMC can be used to synchronize the authentication process through selection of the proper key.

3.12
data origin authentication
corroboration that the source of data received is as claimed

3.13
encipherment
(reversible) transformation of data by a cryptographic algorithm with a cryptographic key in order to produce ciphertext, i.e. to hide the information content of the data

3.14
identifier for authentication key
IDA
field that identifies the key to be used in authenticating the message

3.15
MAC
message authentication code
fixed-length string of bits used to verify the authenticity of a message, generated by the sender of the message, transmitted together with the message, and verified by the receiver of the message

3.16
MAC algorithm
keyed cryptographic algorithm that produces a fixed-length string of bits (the MAC) from a message of arbitrary length, such that it is not feasible to compute the MAC without knowledge of the key

3.17
message element
contiguous group of bytes designated for a specific purpose

3.18
MID
message identifier
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. DMC)

NOTE In ISO 8583, the MID was referred to as the systems trace audit number (STAN), which it supersedes.

3.19
message text
information conveyed or transmitted between sender and receiver, excluding header and trailer information used for transmission purposes

3.20
receiver
party intended to receive the message

3.21
sender
party responsible for, and authorized to, send a message

3.22
value date
date on which funds are to be at the disposal of the beneficiary

4 Protection

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 authentication algorithm. Keys shall be managed in accordance with ISO 11568-1 and ISO 11568-2.

4.2 Authentication elements

The MAC calculation shall include those message elements, as agreed between sender and receiver, which require protection against fraudulent alteration.

Subject to bilateral agreement, the MAC calculation may also cover data elements not transmitted in the 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 in a message, 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;

f) date and time;

g) indication as to the disposition of the transaction.

NOTE Integrity protection applies only to the selected authentication elements. Other parts of the message can be subject to undetected alterations. It is important that users ensure the integrity of data presentation.

4.3 Detection of duplication, loss or sequence errors

A mechanism should be implemented to detect duplication or loss, or messages arriving out of sequence. Without recourse to further message exchanges, the recipient may only detect the replay of a previous transaction if able to identify transactions uniquely, and should then check that such unique identifying information has not already occurred. To detect sequence errors, messages should be identifiable as being in a sequence. Furthermore, in order to detect loss, transactions should be identifiable as being in a defined sequence, predictable by the recipient. These conditions are achieved by involving in the MAC computation some elements (i.e. message elements or key elements) that are unique to the transaction and that relate it uniquely to the previous transaction. This may be achieved in one of the following ways.

a) Include in the MAC calculation a unique transaction reference that does not repeat within the lifetime of the system. To detect loss, the reference would need to change in a defined sequence that is known by the recipient who calculates this value and compares it to the received value.

EXAMPLE The reference will include sender ID, recipient ID, key ID and transaction number, where the transaction number increases by one for each transaction.

b) Include in the MAC calculation a MID, i.e. a value that does not repeat before either

   — the change of date, i.e. DMC (usable if the date is included in MAC elements), or

   — the expiration of the cryptoperiod of the key used for authentication.

   The MID may consist of a unique sending bank's transaction reference number in a fixed format message as a message identifier. A method of protection is described in Annex A. The MID may either contain the DMC or be a separate field. To simplify detection of loss, the MID could increase in a defined sequence.

c) Use a unique key per transaction where the key of one transaction is derived from that of the previous transaction (see ISO 11568-2).

d) Combine the above techniques.

5 Procedures for message authentication

5.1 MAC generation

The sender of a message shall generate a MAC by processing in an agreed order (e.g. 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 mechanism (see 4.2). The mechanism 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.

5.2 MAC placement

The MAC shall be either

a) placed in the message, in an additional field specified for the transport of the MAC, or

b) appended to the data portion of the message, if there is no specified MAC field.

Where the field allocated has a length, for transport, greater than the MAC length, the MAC shall be positioned by left-justifying it within the field.

5.3 MAC verification

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 shall be considered to have been confirmed when the receiver's computed reference MAC agrees with that received with the message text.

A received MAC is not included in the algorithm computation.

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).

5.4 Approved authentication mechanisms based on ISO/IEC 9797

5.4.1 General

The MAC algorithm shall be one of those specified in ISO/IEC 9797-1 or ISO/IEC 9797-2.

5.4.2 Approved authentication mechanisms based on ISO/IEC 9797

ISO/IEC 9797-1 specifies six MAC algorithms that use a secret key and an n-bit block cipher to calculate an m-bit MAC, and which are based upon the cipher block chaining (CBC) mode of operation of a block cipher.

— MAC Algorithm 1 is a simple CBC-MAC using a single key.

— MAC Algorithm 2 is a variant on Algorithm 1, with an additional final transformation using a second key.

— MAC Algorithm 3 is a variant on Algorithm 1, ending with two additional transformations, the penultimate transformation uses a second key and the final transformation uses the first key.

— MAC Algorithm 4 is a variant on Algorithm 2, with an additional initial transformation using the second key.

— MAC Algorithm 5 is commonly known as CMAC.

— MAC Algorithm 6 uses two parallel instances of Algorithm 4, and combines the two results with a bit-wise exclusive-OR operation, while doubling the MAC algorithm key length.

The following table shows the authentication mechanisms based on ISO/IEC 9797-1 approved for the generation of MACs for financial services.

Table 1 — Approved algorithms from ISO/IEC 9797-1

ISO/IEC 9797-1 algorithm	ISO/IEC 18033-3 cipher	Key length (bits)	Padding method	MAC length (bits)	Applicable uses
1	AES	128, 192, 256	1	32-128	The length of the message needs to be known to the receiver in order to prevent message forgeries.
3	DEA	112	1	32-64	The length of the message needs to be known to the receiver in order to prevent message forgeries, backward-compatible with ANSI X9.19 and ISO 9807.
1	TDEA	112,168	1	32-64	The length of the message needs to be known to the receiver in order to prevent message forgeries, backward-compatible with ANSI X9.9, ISO 8730 and ISO 8731 (all parts).