INTERNATIONAL STANDARD

ISO 16609

First edition
2004-03-01

Banking — Requirements for message authentication using symmetric techniques

Banque — Exigences pour authentification des messages utilisant des techniques symétriques

Reference number
ISO 16609:2004(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

Contents

Page

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, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

This first edition of ISO 16609 cancels and replaces ISO 8730:1990, ISO 8731-1:1987, ISO 8731-2:1992 and ISO 9807:1991, of which it constitutes a technical revision.

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 if the message has been altered and, if so, whether such an alteration arises by accident or with intent to defraud.

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

The requirements of this International Standard are compatible with those in the editions of ISO 8730 and ISO 9807 it replaces.

Banking — 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. It also specifies a method by which block ciphers can be approved for use in the authentication of banking messages. In addition, because of the necessity for both members in a communicating pair to use the same means for data representation, it defines some methods for data representation. A list of block ciphers approved for the calculation of a message authentication code (MAC), as well as the method to be used to approve additional block ciphers, 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 by sender or receiver, or 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 7746:1998, *Banking — Telex formats for inter-bank messages*

ISO 8583:1993, *Financial transaction card originated messages — Interchange message specifications*

ISO 8601:2000, *Data elements and interchange formats — Information interchange — Representation of dates and times*

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

ISO/IEC 9797-1:1999, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 9797-2:2002, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a hash-function*

ISO/IEC 10116:1997, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO/IEC 10118-3:1998, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO 11568-1:1994, *Banking — Key management (retail) — Part 1: Introduction to key management*

ISO 11568-2:1994, *Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers*

ISO 11568-3:1994, *Banking — Key management (retail) — Part 3: Key life cycle for symmetric ciphers*

ISO 13491 (all parts) *Banking — Secure cryptographic devices (retail)*

ANSI X3.92:1981, *American National Standard for Information Systems — Data encryption algorithm*

ANSI X9.52:1998, *American National Standard for Financial Services — Triple data encryption algorithm, modes of operation*

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 [party]
ultimate party (can be more than one) to be credited or paid as a result of a transfer

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

3.9
cryptoperiod
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

3.10
cryptanalysis
art and science of breaking ciphertext

3.11
data integrity
property defining data that has not been altered or destroyed in an unauthorized manner

3.12
date MAC computed
DMC
date on which the sender computed the message authentication code (MAC)

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

3.13
data origin authentication
corroboration that the source of data received is as claimed

3.14
decipherment
decryption
reversal of a corresponding encipherment

3.15
delimiter
group of characters used to delineate the beginning and end of a data field or fields

3.16
encipherment
encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext (i.e. to hide the information content of the data)

3.17
hexadecimal digit
single character in the range 0 to 9, A to F (upper case), representing a four-bit string

3.18
identifier for authentication key
IDA
field that identifies the key to be used in authenticating the message

3.19
message authentication code
MAC
string of bits that is the output of a MAC algorithm

3.20
MAC algorithm
cryptographic check function
algorithm for computing a function, which maps strings of bits and a secret key to fixed length strings of bits

NOTE 1 It must satisfy the following two properties:

— for any key and any input string, the function can be computed efficiently;

— for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the ith input string may have been chosen after observing the value of the first i to 1 function values.

NOTE 2 Computational feasibility depends on the user's specific security requirements and environment.

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

3.22
message identifier
MID
systems trace audit number (superseded)
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.

3.23
message text
information conveyed or transmitted between sender and receiver, excluding header and trailer information used for transmission purposes

3.24
nonce
number used once

3.25
receiver
party intended to receive the message

3.26
sender
party responsible for, and authorized to, send a message

3.27
value date
date on which funds are to be at the disposal of the beneficiary

4 Protection

IMPORTANT — 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 the presentation of the data.

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. Such keys shall be deterministically or pseudo-randomly generated (see Annex F and Annex G). Any key used for authentication shall be protected against disclosure to unauthorized parties. Use of the authentication keys shall be restricted to the sending and receiving parties (or their authorized agents) and only used for authentication. Keys shall be managed in accordance with ISO 11568 or ISO 8732.

Authentication keys can best be protected if the MAC is computed by a secure cryptographic device, the keys are in plaintext only within such a device and the device is compliant with ISO 13491.

4.2 Authentication elements

The MAC calculation shall include those message elements, as agreed between sender and receiver, which require protection against fraudulent alteration. All such message elements should be included in the MAC calculation.

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. The following 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;

g) message identifier;

h) date and time;

i) indication as to the disposition of the transaction.

4.3 Detection of duplication or loss

A mechanism shall be implemented to detect duplication or loss. Without recourse to further message exchanges, the recipient may only detect the replay of a previous transaction if able to identify transactions uniquely, and shall then check that such unique identifying information has not already occurred. Furthermore, in order to detect loss, transactions shall be identifiable as being in a sequence. Both conditions are thus 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 shall 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.

   EXAMPLE The reference will include sender ID, recipient ID, key ID, transaction number and date.

b) Include in the MAC calculation a message identifier (MID), a value that does not repeat before either

   — the change of date, i.e. date MAC computed (DMC), or

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

   whichever occurs first: i.e. there shall not be more than one message with the same date and the same message identifier that uses the same key.

   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 E. The MID may either contain the DMC or be a separate field.

c) Use a unique key per transaction where either

— the key of one transaction is derived from that of the previous transaction (see, for instance, ISO 11568-2 and Annex G), or

— the key is derived using a unique transaction reference (see Annex G).

d) Combine the above techniques.

5 Procedures for message authentication

5.1 Preliminaries

Implementers shall conduct a risk assessment of the application to determine the data to be protected (see Clause 4), the required key length and MAC algorithm, and shall agree upon the following:

— a block cipher (if MAC algorithm chosen from ISO/IEC 9797-1);

— a hash-function (if MAC algorithm chosen from ISO/IEC 9797-2);

— a padding method (if MAC algorithm chosen from ISO/IEC 9797-1);

— the length in bits of the MAC;

— the key change frequency (this should take into consideration the current state of the art of cryptanalysis);

— a common key derivation method (if required by the MAC algorithm).

Approved block ciphers are given in Annex A.

The correspondents shall also exchange a secret authentication key.

Financial service applications should use a key with a length of less than 112 bits only with caution, and with a full understanding of underlying risk management and assessment (see ISO 13491). The ISO/IEC 9797-1:1999-specified MAC Algorithms 1 and 3 (see Clause 6) are recommended for applications requiring 112-bit MAC algorithm keys.

The sender shall calculate a MAC using the selected data elements. This MAC shall be appended to the text of the transmitted message such that it is identifiable by the receiver. The receiver shall repeat the computation, using the same authentication method as defined in this clause. The message authenticates if the received and computed reference MACs are identical.

Implementers should also consider the performance characteristics given in 6.3.

5.2 Message format

The sender shall format and code the message by a method agreed with the recipient.

5.3 Key generation

Subject to agreement with the receiving party, the sender of a message may generate a new key with which to compute the MAC. The derivation of such a key may involve transaction and message-dependent data. Annex F and Annex G provide some examples of key generation and derivation.