8

SLS 1047 : 1995
(ISO 9807 : 1991)

Sri Lanka Standard

BANKING AND RELATED FINANCIAL SERVICES - REQUIREMENTS FOR MESSAGE AUTHENTICATION (RETAIL)

Gr. F

SRI LANKA STANDARDS INSTITUTION

SLS 1047 : 1995
ISO 9807 : 1991

Sri Lanka Standard
BANKING AND RELATED FINANCIAL SERVICES - REQUIREMENTS FOR MESSSAGE AUTHENTICATION (RETAIL)

NATIONAL FOREWORD

This standard was finalized by th Sectoral Committee on Information Technology and was authorized for adoption and publication as a Sri Lanka Standard by the Council of the Sri Lanka Standards Institution on 1995-05-25.

This Sri Lanka Standard is identical with ISO 9807:1991 Banking and related financial services - Requirements for message authentication (retail), published by the Internatioanl Organization for Standardization (ISO).

Terminology and conventions

The text of the International standard has been accepted as suitable for publication, without deviation, as a Sri Lanka Standard. Howevers, certain terminology and conventions are not identical with those used in Sri Lanka Standards, attention is therefore drawn to the following:

a) Wherever the words 'International Standard/Publication' appear, referring to this standard they should be interpreted as "Sri Lanka Standard".

Wherever page numbers are quoted, they are ISO page numbers.

CROSS - REFERENCES

International Standard	Corresponding Sri Lanka Standards
ISO 8730:1990, Banking - Require ments for message authentication (wholesale).	SLS 1053 : 1995 Banking- Require ments for message authentication (wholesale).
ISO 8731-1:1987, Banking - Approved algorithms for message authentication -Part 1 : DEA.	SLS 1054 : Part 1 1995,-Banking -Approved algorithms for message authentication Part 1 : DEA
ISO 7812-2:1987, Banking - Approved algorithms for message authentication-Part : Message authenticator algorithms.	SLS 1054 : Part 2 : 1995,-Banking -Approved algorithms for message authentication Part 2 : Message authenticatore algorithms.

-/ltf.

INTERNATIONAL STANDARD

ISO 9807

First edition
1991-12-15

Banking and related financial services — Requirements for message authentication (retail)

Banque et services financiers liés aux opérations bancaires — Spécifications liées à l'authentification des messages (service aux particuliers)

Reference number
ISO 9807:1991(E)

Contents

Annexes

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 voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 9807 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Sub-Committee SC 6, *Financial transaction cards, related media and operations*.

Annexes A, B and C form an integral part of this International Standard. Annexes D, E, F and G are for information only.

Introduction

A Message Authentication Code (MAC) may be used to authenticate the origin and text of a message sent between a sender and a receiver. It is generated by the sender of the message and is transmitted together with the message concerned.

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

A Message Authentication Code is a data field which may be used to verify the authenticity of a message. 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.

This International Standard is one of a series which describes the requirements for security in the retail banking environment. (See annex G.)

A related series of International Standards describes the requirement for security in the wholesale banking environment (see annex G).

The requirements of this International Standard are compatible with those in ISO 8730. Both this International Standard and ISO 8730 have a close relationship with ISO 8731, which describes algorithms which have been approved for use in message authentication.

Banking and related financial services — Requirements for message authentication (retail)

1 Scope

This International Standard specifies procedures to be used for protecting the integrity of retail banking messages and for verifying that the message originated from an authorized source. It also describes the method by which algorithms are approved for use for the authentication of retail banking messages.

Rules for data representation are not specified although it is necessary for both members of a communicating pair to use the same means for data representation. The procedures are also independent of the transmission process used.

A list of algorithms approved for the calculation of a Message Authentication Code (MAC) is given in annex A. The method to be used to approve authentication algorithms is given in annex B. The procedure to prevent exhaustive key determination is provided in annex C.

Annex D gives guidance on the selection of authentication elements. Annex E provides some general information on protection against internal fraud by sender or receiver, e.g. forgery of a Message Authentication Code by the receiver, while annex F describes a method for the generation of a pseudo-random key. Annex G consists of bibliographic references.

This International Standard does not provide for

a) encipherment for the protection of messages against unauthorized disclosure; or

b) protection against loss or duplication of messages, whether accidental or intentional.

This International Standard is applicable to institutions responsible for implementing techniques to authenticate messages used in a retail banking environment.

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

ISO 8730:1990, *Banking — Requirements for message authentication (wholesale)*.

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

ISO 8731-2:1987, *Banking — Approved algorithm for message authentication — Part 2: Message authenticator algorithms*.

3 Definitions

For the purposes of this International Standard, the following definitions apply.

3.1 algorithm: A specified mathematical process for computation.

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 cryptographic key: A parameter used, in conjunction with an algorithm, for the purposes of validation, authentication, encipherment, or decipherment.

3.7 cryptoperiod: The time span during which a specific cryptographic key is authorized for use or in which the cryptographic key for a given system remains in effect.

3.8 encipherment: A process of transforming plaintext into ciphertext for security or privacy.

3.9 Message Authentication Code (MAC): A code in a message between the sender and the 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.

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

3.11 receiver: The party intended to receive the message.

3.12 sender: The party responsible for, and authorized to send, a message.

4 Procedures for message authentication

4.1 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 pseudorandomly generated (see annex F). 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.

4.2 Authentication elements

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

NOTES

1 It is recommended that all message elements be included in the MAC calculation.

2 Untransmitted elements may be included in the MAC calculation.

The header and trailer message information used for transmission purposes shall be omitted from the MAC calculation.

4.3 MAC length

The MAC length shall be 32 bits.

4.4 MAC generation

The authentication algorithms shall be used with the authentication key and the authentication elements. The MAC shall be generated in accordance with the requirements of an approved authentication algorithm, as agreed to by the sender and receiver.

NOTES

3 See annex A for the list of approved authentication algorithms.

4 A change in the sequence of the authentication elements or their representation, after generation of the MAC, will result in an authentication failure.

4.5 Placement of MAC

The MAC shall be either

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

b) if there is not a specified MAC field, appended to the data portion of the message.

Where the field allocated has a length, for transport, greater than 32 bits, the MAC shall be positioned by left justifying it within the field.

5 Verification of the MAC

To verify the integrity of a message containing a MAC the receiver shall calculate a MAC (reference MAC) using the method of calculation specified in 4.4 and using identical data, in the identical sequence, from the authentication elements, the identical authentication key, and the identical authentication algorithm. The received MAC field shall not be included in the calculation of the reference MAC.

The reference MAC and the received MAC shall be compared. If identical, the integrity of the authentication elements together with their origination by an authorized sender are confirmed.

6 Approval procedure for authentication algorithms

Before an authentication algorithm is authorized for inclusion in annex A, it shall satisfy both of the following basic requirements:

a) it shall be designed to satisfy a need not already provided by the algorithm(s) specified in annex A, for example, be suitable for a different operational environment, or provide significant cost savings in implementation or operation, or offer a greater level of protection;

b) it shall be sufficiently secure to serve its stated purpose.

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

Annex A
(normative)

Algorithms approved for calculation of MAC for authentication of retail messages

The following algorithm(s) and mode(s) of operation have been approved for use in conjunction with this International Standard (see annex B for further information on the approval process):

- the algorithm described in ISO 8731-1, using the cipher-block chain mode of operation;

  NOTE 5 See annex C for the additional procedure to prevent exhaustive key determination.

- the algorithm described in ISO 8731-2.

Annex B
(normative)

Procedure for the review of alternative authentication algorithms

B.1 Origination

An alternative authentication algorithm which is to be proposed for incorporation in annex A of this International Standard shall be submitted by, or with the approval of, a national standards body to the Secretariat of ISO/TC 68.

B.2 Justification of proposal

The proposer shall justify the proposal by describing

a) the purpose the proposal is designed to achieve;

b) how this purpose is better achieved by the proposal than by algorithms already in annex A of this International Standard;

c) additional merits not described elsewhere;

d) experience in use with the new algorithm.

B.3 Documentation

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

a) a full description of the algorithm proposed;

b) a clear acknowledgement that the algorithm satisfies, or is compatible with, all the requirements contained in clause 6;

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 algorithm has been subjected, particularly concerning its security. 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 (i.e. sufficient information shall be provided to enable an independent agency to conduct the same tests and to compare the results so achieved).

B.4 Public disclosure

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

B.5 Examination of proposals

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

B.6 Public review

When a report 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 6 This period of public review may extend the 180 days allowed for the preparation of the report on the proposal (see B.5).

[1] *IEC/ISO Directives — Part 2: Methodology for the development of International Standards*, 1989, 5.7.

B.7 Appeals procedure

Originators whose proposals are rejected (see B.5) may ask the Secretariat of ISO/TC 68 to have the proposals subjected to public review (see B.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 ISO/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.

B.8 Incorporation of new authentication algorithms in this International Standard

New authentication algorithms recommended for acceptance, together with relevant reports on them, shall be circulated for letter ballot as proposed amendments to annex A of this International Standard.

B.9 Maintenance

An algorithm approved by the method described in this International Standard shall be reviewed at intervals of not greater than 5 years.

Annex C
(normative)

Procedure to prevent exhaustive key determination

The following procedure may be used to prevent exhaustive key determination if the algorithm described in ISO 8731-1 is used.

Exhaustive key determination can be prevented by the use of two DEA keys for MAC generation in accordance with a pre-defined agreement between sender and receiver. When this technique is utilized, the 64-bit cipher text output block O is generated using the first key (K) as specified in ISO 8731-1:1987, 4.2.

Two additional steps shall then be followed (see figure C.1):

a) decipher the ciphertext output (O_n) using the second key (K_2);

b) encipher the result of a), O_n^*, using the first key (K). This result becomes the new ciphertext output (O_n^{**}).

The left-most 32 bits O_n^{**} are used as the MAC.

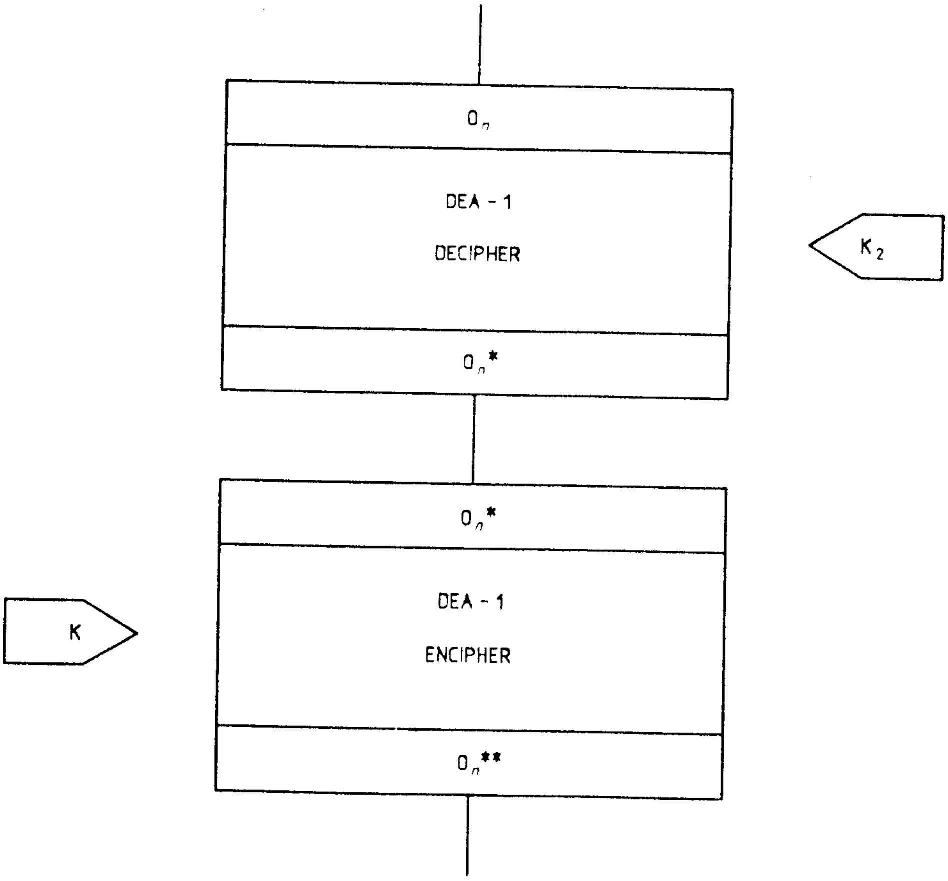

Figure C.1

Annex D
(informative)

Guidance on the selection of authentication elements

This International Standard does not require the entire message to be authenticated, but permits selected authentication elements to be included in the MAC calculation. The purpose of this annex is to provide guidance in the selection of these authentication elements. This annex indicates which authentication elements, at a minimum, should be included in the MAC computation in order to maintain the financial integrity of the transaction.

With the exceptions noted, the following elements whenever present, should be included in the MAC calculation:

a) account number (e.g. Field P-2 of ISO 8583);

b) transaction amount (e.g. Field P-4 of ISO 8583);

c) indication of whether the transaction represents a debit or credit to the cardholder's account (e.g. the Processing Code, Field P-3 of ISO 8583);

d) message identifier (e.g. the System Trace and Audit Number, Field P-11 of ISO 8583) (see note 7)[2];

e) enciphered PIN (e.g. Field P-52 of ISO 8583)[2];

f) indication as to the disposition of the transaction (e.g. the Response Code, Field P-39 of ISO 8583).

NOTE 7 Only if the message recipient is able to verify the uniqueness of a message identifier can fraudulent replay of a previously valid transaction be detected.

[2] In unique-key-per-transaction techniques it may be possible to exclude these elements from the MAC calculation.

Annex E
(informative)

Protection against duplication and loss

E.1 Purpose

Message authentication can be enhanced as part of an overall security process, to protect against

a) fraudulent replay, or duplication of messages;

b) fraudulent deletion or loss of messages.

This can be accomplished, in accordance with predefined agreements, with the use of unique-per-transaction message elements, time variant keys, or other methods. The following are examples of how duplication or loss of messages may be detected; they use unique-per-transaction system trace and audit numbers (STAN). Other methods, including variations of those described in this annex, may also be devised.

E.2 Protection against duplication

E.2.1 Duplicated messages may be detected if under normal conditions the STAN does not repeat for a given key. The receiving party must check the STAN to ensure that it did not appear in a previous message. This check may be performed in one of the following ways:

a) when STANs are not sent in any particular order, then the receiver may compare the received STAN against a list of the STANs previously received under the same key;

b) when the STANs for a particular key are always sent in increasing order the receiver need only check to ensure that any STAN received is greater than the STAN previously received.

E.2.2 When more than two parties share a common key (multi-party operation), duplication may be detected if each party uses a mutually exclusive portion of the possible STANs. The receiving party checks that the STAN is in the proper range and has not already been received.

E.2.3 If the identities of both the sending and the receiving parties are included as authentication elements in each message the receiving party need only check that the STAN has not appeared previously in a message from the sending party. In this case the entire range of STANs may be used by each sending and receiving pair and STANs may repeat between different pairs.

E.3 Loss protection

If the STANs are sent in sequence the receiver may detect a lost message as soon as an out-of-sequence STAN is received.

Annex F
(informative)

Pseudo-random key generator

F.1 Purpose

The purpose of this annex is to provide a method for the generation of a pseudo-random key, R.

F.2 Algorithm

Let e[X](Y) represent the DEA encipherment of Y under key X using the Electronic Code Book (ECB) mode. Let K be a DEA key reserved only for the generation of other keys. Let V be a 64-bit seed value which is also kept secret. + is the exclusive-or operator. Let DT be a date-time vector which is updated on each key generation. I is an intermediate value. Generate a 64-bit vector, R, as follows:

$$I = e[K]\ (DT)$$

$$R = e[K]\ (I + V)$$

and generate a new V as follows:

$$V = e[K]\ (R + I)$$

When the authentication algorithm uses DEA, obtain the key, when generated in the clear, by resetting every eighth bit to odd parity. For other algorithms obtain the key by iterating the process as many times (1, 2, ..., *n*) as necessary to obtain the required number of bits (less than or equal to 64, 128, ..., $n \times 64$).

Annex G
(informative)

Bibliography

G.1 Requirements for security in the retail banking environment

[1] ISO 9564-1:1991, *Banking — Personal Identification Number management and security — Part 1: PIN protection principles and techniques.*

[2] ISO 9564-2:1991, *Banking — Personal Identification Number management and security — Part 2: Approved algorithm(s) for PIN encipherment.*

G.2 Requirements for security in the wholesale banking environment

[3] ISO 8730:1990, *Banking — Requirements for message authentication (wholesale).*

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

[5] ISO 8731-2:1987, *Banking — Approved algorithm for message authentication — Part 2: Message authenticator algorithms.*

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

[7] ISO 10126-1:1991, *Banking — Procedures for message encipherment (wholesale) — Part 1: General principles.*

[8] ISO 10126-2:1991, *Banking — Procedures for message encipherment (wholesale) — Part 2: DEA algorithm.*

G.3 General reference

[9] ISO 8583:1987, *Bank card originated messages — Interchange message specifications — Content for financial transactions.*

[10] ISO 8908:—[3], *Banking and related financial services — Vocabulary and data elements.*

[3] To be published.