भारतीय मानक

Indian Standard

IS 15899 : 2023
ISO 16609 : 2022

वित्तीय सेवाएँ — सममित तकनीकों का प्रयोग करते हुए संदेश विश्वसनीयता की अपेक्षाएँ

(दूसरा पुनरीक्षण)

Financial Services — Requirements for Message Authentication Using Symmetric Techniques

(Second Revision)

ICS 35.240.40

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुर शाह ज़फर मार्ग, नई दिल्ली - 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI - 110002
www.bis.gov.in www.standardsbis.in

November 2023 **Price Group 8**

Banking and Financial Services Sectional Committee, SSD 03

NATIONAL FOREWORD

This Indian Standard (Second Revision) which is identical to ISO 16609 : 2022 ‘Financial services — Requirements for message authentication using symmetric techniques’ issued by International Organization for Standardization (ISO) was adopted by the Bureau of Indian Standards on the recommendations of Banking and Financial Services Sectional Committee and approval of the Service Sector Division Council.

This standard was first published in 2012 as an identical adoption of ISO 16609 : 2004 ‘Banking — Requirements for message authentication using symmetric techniques’ under dual numbering system and further revised in 2017. This second revision has been undertaken to align the Indian Standard with the latest version of ISO 16609 that is, ISO 16609 : 2022 ‘Financial services — Requirements for message authentication using symmetric techniques’.

This revision cancels and replaces the previous edition, of which it constitutes a minor revision. The main changes to the previous edition are as follows:

a) Updated to include newer hash functions specified in updated versions of the ISO/IEC 9797 series.

The text of ISO standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words ‘International Standard’ appear referring to this standard, they should be read as ‘Indian Standard’; and
b) Comma (,) has been used as a decimal marker while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

In this standard, references appear to the following International Standards for which Indian Standards also exist. The corresponding Indian Standards which are to be substituted in their place are listed below along with their degree of equivalence for the editions indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO 8583-1 Financial transaction card originated messages — Interchange message specifications — Part 1: Messages, data elements and code values	IS 14943 (Part 1) : 2014/ISO 8583 -1 : 2003 Financial transaction card originated messages — Interchange message specifications: Part 1 Message, data elements and code values	Identical
ISO 11568-1 Banking — Key management (retail) — Part 1: Principles	IS 15256 (Part 1) : 2011/ ISO 11568-1 : 2005 Banking — Key management (retail): Part 1 Principles (*first revision*)	Identical
ISO 11568-2 Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle	IS 15256 (Part 2) : 2016/ ISO 11568- 2 : 2012 Financial services — Key management (retail): Part 2 Symmetric ciphers, their key management and life cycle (*first revision*)	Identical

Annexes A and B of this standard are for information only.

Contents

Page

Introduction

A message authentication code (MAC) is a data field used to verify the authenticity of a message, generated by the sender of the message using a key shared with the recipient. The message and the MAC are transmitted together. The recipient recalculates the MAC using the transmitted message and compares it with the transmitted MAC, which allows detection of an altered message. While non-keyed message integrity methods, such as checksums, only provide a method to detect *accidental* alteration of the message, MACs additionally detect deliberate alteration, as the adversary would not have access to the key used to generate the MAC.

A MAC can also be used as a means to confirm integrity of stored data.

This document 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 document identifies ciphers, hash functions and algorithms from the ISO/IEC 9797 series that are specifically approved for secure banking purposes.

General tutorial information can be found in Annex B.

Indian Standard

FINANCIAL SERVICES — REQUIREMENTS FOR MESSAGE AUTHENTICATION USING SYMMETRIC TECHNIQUES

(Second Revision)

1 Scope

This document specifies procedures, independent of the transmission process, for protecting the integrity of transmitted financial-service-related messages and for verifying that a message has originated from an authorized source, or that stored data has retained integrity. A list of block ciphers approved for the calculation of a message authentication code (MAC) is also provided. The authentication methods defined in this document are applicable to stored data and to messages formatted and transmitted both as coded character sets or as binary data.

This document 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. 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 documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 8583-1, *Financial transaction card originated messages — Interchange message specifications — Part 1: Messages, data elements and code values*

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 terms and definitions given in ISO 8583-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

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

3.2
authentication key
cryptographic key used for authentication

3.3
beneficiary
ultimate party to be credited or paid as a result of a transfer

Note 1 to entry: There can be more than one beneficiary.

3.4
block cipher
algorithm (3.1) 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

3.5
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

3.6
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

3.7
date MAC computed
DMC
date on which the sender computed the *message authentication code (MAC)* (3.10)

Note 1 to entry: The DMC can be used to synchronize the authentication process through selection of the proper key.

3.8
encipherment
(reversible) transformation of data by a cryptographic *algorithm* (3.1) with a cryptographic key in order to produce ciphertext, i.e. to hide the information content of the data

3.9
identifier for authentication key
IDA
field that identifies the key to be used in authenticating the message

3.10
message authentication code
MAC
cryptographic check sum on data that uses a symmetric key to detect both accidental and intentional modification of data

3.11
MAC algorithm
keyed cryptographic *algorithm* (3.1) that produces a fixed-length string of bits – the *message authentication code (MAC)* (3.10) – from a message of arbitrary length, such that it is not feasible to compute the MAC without knowledge of the key

3.12
message authentication element
element that is to be protected by authentication

3.13
message element
contiguous group of bytes designated for a specific purpose

3.14
message identifier
MID
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. date MAC computed (DMC)]

Note 1 to entry: In ISO 8583-1, the MID is referred to as the systems trace audit number (STAN), which it supersedes.

3.15
receiver
party intended to receive the message

3.16
sender
party responsible for, and authorized to, send a message

3.17
universal hash function
function mapping strings of bits to fixed-length strings of bits, indexed by a parameter called the key, satisfying the property that for all distinct inputs, the probability over all keys that the outputs collide is small

[SOURCE: ISO/IEC 9797-3:2011, 3.6, modified — Note 1 to entry removed.]

3.18
value date
date on which funds are to be at the disposal of the beneficiary

4 Principles

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

4.2 Message authentication elements

The MAC calculation shall include those data elements which require protection against fraudulent alteration. For messages, this is agreed between sender and receiver. Subject to bilateral agreement, the MAC calculation may also cover data elements not transmitted in a 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, 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 (MID);

f) date and time;

g) indication as to the disposition of the transaction.

NOTE Integrity protection applies only to the selected message 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 can 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. Examples of methods to achieve this include the following:

a) Incorporate 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 with 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) Incorporate in the MAC calculation an MID, i.e. a value that does not repeat before either:

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

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

   The MID can consist of a unique sending bank's transaction reference number in a fixed format message as an MID. A method of protection is described in Annex A. The MID can 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[1)]).

d) Use a unique key per transaction where the key of each transaction is derived from a unique transaction reference that does not repeat within the lifetime of the base key.

e) Combine the above techniques.

5 Procedures for message authentication

5.1 MAC generation

A MAC shall be generated by processing in an agreed order (e.g. the sequence in which they appear in a message) those elements to be authenticated (see 4.2). The generation mechanism shall use an authentication key, which is a secret between the two correspondents. This process creates the MAC, which shall then be included with the original text. To retain integrity of stored data the MAC is unambiguously associated with the respective data.

[1)] Under preparation. Stage at the time of publication: ISO/FDIS 11568:2022.

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;

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

c) retained in unambiguous association with the data requiring integrity protection.

5.3 MAC verification

A reference MAC is that which is received in the message to be verified, or that which is associated with the stored data.

When verifying a MAC it shall be recomputed using the message authentication elements, an identical authentication key and an identical algorithm. The result is then compared with the reference MAC. Authenticity of the elements to be authenticated (and the message source if applicable) shall be considered to have been confirmed when the computed MAC agrees with the reference MAC.

A MAC is not included in the algorithm computation.

Verification of the MAC is sensitive to the sequence in which the message authentication elements are processed (i.e. a change in the sequence of message authentication elements after the MAC is generated will result in a failure to authenticate).

5.4 Approved authentication mechanisms based on the ISO/IEC 9797 series

5.4.1 General

This document approves MAC algorithms specified in 5.4.2, 5.4.3 and 5.4.4, which shall be used for message authentication.

5.4.2 Approved message authentication mechanisms based on ISO/IEC 9797-1

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 is a variant of algorithm 1, using a final iteration with a separate key, so doubling the MAC algorithm key length.

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

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

ISO/IEC 9797-1 MAC algorithm	ISO/IEC 18033-3 cipher	Key length bits	ISO/IEC 9797-1 padding method	MAC length bits	Applicable uses
1	AES or SM4	128, 192, 256[b]	1	32 to 128	The length of the message needs to be known to the receiver in order to prevent message forgeries.
1	TDEA	112,168	1	32 to 64	The length of the message needs to be known to the receiver in order to prevent message forgeries.
1	TDEA	112,168	3	32 to 64	The message length is needed prior to starting MAC calculation.
1	AES or SM4	128, 192, 256[b]	3	32 to 128	
1	TDEA	112,168	2	32 to 64	The recipient need not have prior knowledge of the message length.
1	AES or SM4	128, 192, 256[b]	2	32 to 128	
3	DEA	56 + 56[a]	1	32 to 64	The length of the message needs to be known to the receiver in order to prevent message forgeries.
3	DEA	56 + 56[a]	2	32 to 64	The recipient need not have prior knowledge of the message length.
3	DEA	56 + 56[a]	3	32 to 64	The message length is needed prior to starting MAC calculation.
5	AES or SM4	128, 192, 256[b]	4	32 to 128	The recipient need not have prior knowledge of the message length.
5	TDEA	112,168	4	32 to 64	

[a] ISO/IEC 9797-1 algorithm 3 uses two independent DEA keys.

[b] For SM4, only 128-bit key length is allowed.

Consideration should be given to the selection of MAC length. Short MAC lengths increase the likelihood of successful collision attacks, while full-length MACs calculated over single blocks are potentially susceptible to key recovery attacks if a large number of MACs can be calculated. See ISO/TR 14742 and ISO/IEC 9797-1 for additional information.

The security analysis in ISO/IEC 9797-1:2011, Annex C, provides implementation recommendations for protecting against forgery and key recovery attacks.

For new implementations MAC algorithm 1 is not recommended. If algorithm 1 is used, then steps should be taken to prevent XOR forgery attacks as described in ISO/IEC 9797-1:2011, Annex C. An adequate precaution is to use padding method 3.

If algorithm 3 is used, then the number of MACs generated using the same key should be restricted to a maximum of 256 uses. In order not to reduce the lifetime of the MAC-generating device, the use of session keys is recommended.

Trivial forgery: if padding method 1 is used, then an adversary can typically add to, or delete from, the data string a number of trailing “0” bits without changing the MAC. This implies that padding method 1 should only be used in environments where the length of the data string is known to the parties beforehand, or where data strings with a different number of trailing “0” bits have the same semantics.

5.4.3 Approved message authentication mechanisms based on ISO/IEC 9797-2

The only allowable MAC algorithms from ISO/IEC 9797-2 are those under the heading of MAC algorithm 2, as defined in that document, and otherwise known as HMAC. As specified in ISO/IEC 9797-2, HMAC uses a secret key and a hash function (or its round function) with an *n*-bit result to calculate an *m*-bit MAC.

Table 2 shows the authentication mechanisms based on ISO/IEC 9797-2 approved for the generation of MACs for financial services.

Table 2 — Approved MAC algorithms from ISO/IEC 9797-2

ISO/IEC 9797-2 MAC algorithm	ISO/IEC 10118-3 hash function	Key length *k* bits	Maximum MAC length *m* bits
2	RIPEMD-160	112 - 512	160
	SHA-1	112 - 512	160
	SHA-224	112 - 512	224
	SHA-256	112 - 512	256
	SHA-384	112 - 1 024	384
	SHA-512	112 - 1 024	512
	SHA-512/224	112 - 1 024	224
	SHA-512/256	112 - 1 024	256
	SHA3–224	112 - 1 152	224
	SHA3–256	112 - 1 088	256
	SHA3–384	112 - 832	384
	SHA3–512	112 - 576	512
	SM3	112 - 512	256

NOTE 1 RIPEMD-160 and SHA-1 are still permitted for use, as known collision attacks are not applicable to HMAC construction.

NOTE 2 The lower bound on the key length in this table reflects that the effective strength of the HMAC mechanism is the minimum of the key length and twice the (internal) hash code, as well as 112 bits being the minimum supported strength. For more information, see NIST SP 800-107 Rev. 1, 5.3.

The security analysis in ISO/IEC 9797-2:2021, Annex C, provides implementation recommendations for protecting against forgery and key recovery attacks.

5.4.4 Approved message authentication mechanisms based on ISO/IEC 9797-3

MACs based on universal hash functions have the special property that their security can be proven under the assumption that the encryption algorithm is secure.

The allowable MAC algorithms from ISO/IEC 9797-3 are:

— UMAC with output length of 32, 64, 96 or 128 bits;

— Poly1305-AES with output length of 128 bits;

— GMAC with output length of m bits, where *m* is a multiple of 8 and satisfies $64 \leq m \leq 128$.

Table 3 shows the authentication mechanisms based on ISO/IEC 9797-3 approved for the generation of MACs for financial services.

Table 3 — Approved algorithms from ISO/IEC 9797-3

ISO/IEC 9797-3 algorithm	**ISO/IEC 18033-3 cipher**	**Key length** bits	**MAC length** *m* bits	**Remarks**
UMAC	AES or SM4	128, 192, 256[a]	32, 64, 96, 128	UMAC makes use of simple zero padding for messages having a bit length that is not a multiple of 8.
Poly1305-AES	AES	256 (with 22 bits set to zero)	128	AES 128 is used in a final step of the algorithm. The specially formatted key of length 256 bits is not used as AES key.
GMAC	AES or SM4	128, 192, 256[a]	$64 \leq m \leq 128$ and $m \equiv 0 \bmod 8$	

[a] For SM4, only 128-bit key length is allowed.

The security analysis in ISO/IEC 9797-3:2011, Annex C, provides implementation recommendations for protecting against forgery and key recovery attacks.

5.4.5 Implementation recommendations

One simple criterion for choosing between mechanisms in ISO/IEC 9797-1 or ISO/IEC 9797-3 and mechanisms in ISO/IEC 9797-2 is the availability of an implementation of the block cipher or hash function. As indicated in Table 1 and Table 2, other characteristics such as performance issues or data length will help the appropriate choice of parameters.

Annex A
(informative)

Protection against duplication and loss using MIDs

A.1 Purpose

Protection against duplication and loss can be accomplished, in accordance with predefined agreements, by using unique-per-transaction message elements, time-variant keys or other methods. This annex describes methods for detecting duplication and loss of transmitted messages using MIDs in accordance with 4.3. Other methods, including variations of those described in this annex, may also be devised.

A.2 Protection against duplication

A.2.1 Duplicated messages

Duplicated messages can be detected if, under normal operation, the MID from a given sender does not repeat for a given date and a given key. The receiver should check the MID to ensure that it did not appear in a previous message. This check can be performed in one of the following ways:

a) If MIDs are sent in no predetermined order, the receiver can compare the received MID against a list of the MIDs received on that day.

b) If the MIDs for messages authenticated under a particular key are always sent in increasing order, the receiver need only check that the identifiers are strictly increasing.

Other methods, including variations on a) or b), may also be devised.

A.2.2 Multi-party operation

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

A.2.3 Including identities

When the identities of both the sending and receiving parties are included as message authentication elements in each message, the receiving party need only check that it is the intended receiver and that the MID has not appeared previously in a message from the sending party. In this case, the entire range of MIDs can be used by each sending and receiving pair, and MIDs can repeat between different pairs.

A.3 Loss detection

Loss of a transmitted message can be detected if both the sending and receiving parties keep a list of all MIDs used at a given time. One party sends its list (via an authenticated message which has duplication protection) to the party wishing to detect any loss. A comparison of the two lists is then performed. Alternatively, if the MIDs are to be received in sequence, the receiver can detect a lost message as soon as an out-of-sequence MID is received. The last MID for a day can be sent to the loss detection party by way of an authenticated message which has duplication protection. Other methods, including variations of those just described, may also be devised.

If it is necessary to ensure that deletion of messages is detected quickly enough (i.e. that silence means that no messages were sent), then null messages or reconciliation messages can be requested or sent at appropriate times.

Annex B
(informative)

General tutorial information

The purpose of message authentication is to ensure that transaction messages are received exactly as originated by the legitimate originator. To accomplish this, message authentication detects both the fraudulent insertion of totally spurious transaction messages and the fraudulent modification of otherwise legitimate transaction messages.

Message authentication differs from message encipherment in that the latter does not inherently protect against modified transactions, whereas the former not only provides this protection, but provides it on the cleartext message, allowing the message to be comprehended, processed and journalled while still protected. Message authentication is needed to thwart active wiretapping and related fraud threats. These are relatively sophisticated threats in which transaction data are modified or inserted in real time, perhaps via a microcomputer system inserted into a communications line. For example, assume that a criminal cuts the communications line from an automatic teller machine (ATM) (which does not use any form of message authentication) to its host, and inserts a microcomputer system in series with this line. To the host, this system looks like an idle ATM. To the ATM, this system looks like the host. This fraudulently inserted system is programmed to intercept and discard every request-for-cash message originated by the ATM, and to send in response the approval indication. Thus, the criminal can readily drain the ATM of cash, yet no account will be debited in the process.

Message authentication thwarts active wiretapping fraud scenarios by appending an MAC to each of the transaction messages. This code consists of a number of check digits, which are analogous to a parity check or cyclic redundancy check, except that they are generated via a cryptographic process. The MAC is generated by the originator of the message and is based on the entire message, or upon critical elements of the message, according to prior agreement between the originator and the recipient. (Elements not included in the message but known to both originator and recipient can, by predefined agreement such as this, be included in the MAC computation.) The MAC is included in the transmitted message, then verified by the recipient who holds the same secret key used in the generation process.

Should anyone attempt to modify the protected message elements between the time the MAC is generated and the time it is checked, his or her attempt would be detected. Without knowledge of the secret key, he or she would be unable to generate the correct MAC for the modified message. Similarly, no one can successfully introduce a spurious message because, without the secret key, the proper MAC for this message cannot be generated.

For message authentication to be effective, it is important to ensure the secrecy of the cryptographic key. Preferably, a unique key is used by each communicating pair so that, should the key be compromised, this only jeopardizes the transactions between the two parties and limits accountability to those two parties.

Although message authentication can detect spurious and modified transaction messages, it cannot inherently detect the fraudulent replay of a previously valid message nor the loss of a message. See Annex A for a discussion of these issues.

Message authentication cannot protect against errors in, nor subversion of, the message processing that takes place before the MAC is generated or after it has been verified. For example, it cannot protect against a dishonest merchant that modifies its terminal to indicate one value of the transaction to the customer, while causing the customer's account to be debited (and the merchant's account to be credited) by a higher value.

Message authentication can be used effectively by some participants in a retail electronic funds transfer (EFT) system, even if not used by all. Should an institution decide not to implement message authentication, but later becomes the victim of an active wiretapping fraud scenario, this institution could be made liable for the fraud loss, since transaction journals would indicate where the transaction was fraudulently modified. Thus, each institution participating in the retail EFT system should estimate the implementation cost for message authentication, and the fraud cost for no message authentication, and make its decision accordingly.

Bibliography

[1] ISO/IEC 9797 (all parts), *Information security — Message authentication codes (MACs)*

[2] ISO/IEC 10118-3, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

[3] ISO 11568,[2)]*Financial services — Key management (retail)*

[4] ISO/TR 14742, *Financial services — Recommendations on cryptographic algorithms and their use*

[5] ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

[6] NIST SP 800-107 Rev. 1, *Recommendation for Applications Using Approved Hash Algorithms*, August 2021

[2)] Under preparation. Stage at the time of publication: ISO/FDIS 11568:2022.

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the website- www.bis.gov.in or www.standardsbis.in

This Indian Standard has been developed from Doc No.: SSD 03 (22715).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices: *Telephones*

Central : 601/A, Konnectus Tower -1, 6th Floor,
DMRC Building, Bhavbhuti Marg, New
Delhi 110002 — 2323 7617

Eastern : 8th Floor, Plot No 7/7 & 7/8, CP Block, Sector V,
Salt Lake, Kolkata, West Bengal 700091 — 2367 0012, 2320 9474

Northern : Plot No. 4-A, Sector 27-B, Madhya Marg,
Chandigarh 160019 — 265 9930

Southern : C.I.T. Campus, IV Cross Road, Taramani, Chennai 600113 — 2254 1442, 2254 1216

Western : Plot No. E-9, Road No.-8, MIDC, Andheri
(East), Mumbai 400093 — 2821 8093

Branches : AHMEDABAD. BENGALURU. BHOPAL. BHUBANESHWAR. CHANDIGARH. CHENNAI. COIMBATORE. DEHRADUN. DELHI. FARIDABAD. GHAZIABAD. GUWAHATI. HIMACHAL PRADESH. HUBLI. HYDERABAD. JAIPUR. JAMMU & KASHMIR. JAMSHEDPUR. KOCHI. KOLKATA. LUCKNOW. MADURAI. MUMBAI. NAGPUR. NOIDA. PANIPAT. PATNA. PUNE. RAIPUR. RAJKOT. SURAT. VISAKHAPATNAM.

Published by BIS, New Delhi