INTERNATIONAL STANDARD

ISO/IEC 19772

First edition
2009-02-15

Information technology — Security techniques — Authenticated encryption

Technologies de l'information — Techniques de sécurité — Chiffrage authentifié

Reference number
ISO/IEC 19772:2009(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) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national 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 and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19772 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

When data is sent from one place to another, it is often necessary to protect it in some way whilst it is in transit, e.g. against eavesdropping or unauthorised modification. Similarly, when data is stored in an environment to which unauthorized parties may have access, it may be necessary to protect it.

If the confidentiality of the data needs to be protected, e.g. against eavesdropping, then one solution is to use encryption, as specified in ISO/IEC 18033 and ISO/IEC 10116. Alternatively, if it is necessary to protect the data against modification, i.e. integrity protection, then Message Authentication Codes (MACs), as specified in ISO/IEC 9797, or digital signatures, as specified in ISO/IEC 9796 and ISO/IEC 14888, can be used. If both confidentiality and integrity protection are required, then one possibility is to use both encryption and a MAC or signature. Whilst these operations can be combined in many ways, not all combinations of such mechanisms provide the same security guarantees. As a result it is desirable to define in detail exactly how integrity and confidentiality mechanisms should be combined to provide the optimum level of security. Moreover, in some cases significant efficiency gains can be obtained by defining a single method of processing the data with the objective of providing both confidentiality and integrity protection.

In this standard, *authenticated encryption mechanisms* are defined. These are methods for processing data to provide both integrity and confidentiality protection. They typically involve either a specified combination of a MAC computation and data encryption, or the use of an encryption algorithm in a special way such that both integrity and confidentiality protection are provided.

The methods specified in this standard have been designed to maximise the level of security and provide efficient processing of data. Some of the techniques defined here have mathematical 'proofs of security', i.e. rigorous arguments supporting their soundness.

Information technology — Security techniques — Authenticated encryption

1 Scope

This International Standard specifies six methods for authenticated encryption, i.e. defined ways of processing a data string with the following security objectives:

— data confidentiality, i.e. protection against unauthorized disclosure of data,

— data integrity, i.e. protection that enables the recipient of data to verify that it has not been modified,

— data origin authentication, i.e. protection that enables the recipient of data to verify the identity of the data originator.

All six methods specified in this International Standard are based on a block cipher algorithm, and require the originator and the recipient of the protected data to share a secret key for this block cipher. Key management is outside the scope of this standard; key management techniques are defined in ISO/IEC 11770.

Four of the mechanisms in this standard, namely mechanisms 1, 3, 4 and 6, allow data to be authenticated which is not encrypted. That is, these mechanisms allow a data string that is to be protected to be divided into two parts, *D*, the data string that is to be encrypted and integrity-protected, and *A* (the additional authenticated data) that is integrity-protected but not encrypted. In all cases, the string *A* may be empty.

NOTE Examples of types of data that may need to be sent in unencrypted form, but whose integrity should be protected, include addresses, port numbers, sequence numbers, protocol version numbers, and other network protocol fields that indicate how the plaintext should be handled, forwarded, or processed.

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:—[1)], *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

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

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

1) To be published. (Revision of ISO/IEC 9797-1:1999)

3.1
authenticated encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext that cannot be altered by an unauthorized entity without detection, i.e. it provides data confidentiality, data integrity, and data origin authentication

3.2
authenticated encryption mechanism
cryptographic technique used to protect the confidentiality and guarantee the origin and integrity of data, and which consists of two component processes: an encryption algorithm and a decryption algorithm

3.3
block cipher
symmetric encryption system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext [ISO/IEC 18033-1]

3.4
ciphertext
data which has been transformed to hide its information content [ISO/IEC 10116]

3.5
data integrity
the property that data has not been altered or destroyed in an unauthorized manner [ISO/IEC 9797-1]

3.6
decryption
reversal of a corresponding encryption [ISO/IEC 18033-1]

3.7
encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data [ISO/IEC 18033-1]

3.8
encryption system
cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys [ISO/IEC 18033-1]

3.9
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment) [ISO/IEC 18033-1]

3.10
message authentication code (MAC)
string of bits which is the output of a MAC algorithm [ISO/IEC 9797-1]

3.11
partition
process of dividing a string of bits of arbitrary length into a sequence of blocks, where the length of each block shall be n bits, except for the final block which shall contain r bits, $0 < r \leq n$

3.12
plaintext
unencrypted information [ISO/IEC 10116]

3.13
secret key
key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC 18033-1]

3.14
symmetric encryption system
encryption system based on symmetric cryptographic techniques that uses the same secret key for both the encryption and decryption algorithms [ISO/IEC 18033-1]

4 Symbols (and abbreviated terms)

For the purposes of this document, the following symbols and notation apply:

A Additional authenticated data.

C Authenticated-encrypted data string.

D Data string to which an authenticated encryption mechanism is to be applied.

d Block cipher decryption algorithm; $d_K(Y)$ denotes the result of block cipher decrypting the n-bit block Y using the secret key K.

e Block cipher encryption algorithm; $e_K(X)$ denotes the result of block cipher encrypting the n-bit block X using the secret key K.

K Secret block cipher key shared by the originator and recipient of the data to which the authenticated encryption mechanism is to be applied.

m Number of blocks in the partitioned version of D.

n Block length (in bits) for a block cipher.

t Tag length (in bits).

0^i Block of i zero bits.

1^i Block of i one bits.

$\oplus$ Bit-wise exclusive-or of strings of bits (of the same bit-length).

$||$ Concatenation of bit strings, i.e. if A and B are blocks of bits, then $A||B$ is the block of bits obtained by concatenating A and B in the order specified.

$\#$ Function converting a number into an a-bit block of bits; if k is an integer ($0 \leq k < 2^a$) then $\#_a(k)$ is the a-bit block which, when regarded as the binary representation of a number with the most significant bit on the left, equals k.

$\#^{-1}$ Function converting a block of bits to a number; if A is a block of bits, then $\#^{-1}(A)$ is the unique non-negative integer whose binary representation is A. Hence, if A has n bits, then $\#_n(\#^{-1}(A)) = A$.

$X|_s$ Left-truncation of the block of bits X: if X has bit-length greater than or equal to s, then $X|_s$ is the s-bit block consisting of the left-most s bits of X.

$X|^s$ Right-truncation of the block of bits X: if X has bit-length greater than or equal to s, then $X|^s$ is the s-bit block consisting of the right-most s bits of X.

$X<<1$ Left shift of a block of bits X by one position: the rightmost bit of $Y = X<<1$ will always be set to zero.

X>>1 Right shift of a block of bits X by one position: the leftmost bit of $Y = X$>>1 will always be set to zero.

len Function taking a bit-string X as input, and which gives as output the number of bits in X.

mod If a and $b > 0$ are integers, then a mod b denotes the unique integer c such that:

i) $0 \leq c < b$, and

ii) a-c is an integer multiple of b.

5 Requirements

The authenticated encryption mechanisms specified in this document have the following requirements.

The originator and recipient of the data to which the authenticated encryption mechanism is to be applied, must:

a) agree on the use of a particular mechanism from those specified in this document;

b) agree on the use of a particular block cipher to be used with the mechanism (one of the block ciphers standardised in ISO/IEC 18033-3 shall be used);

c) share a secret key K: in all mechanisms except for authenticated encryption mechanism 5, this shall be a key for the selected block cipher, and in mechanism 5 it shall be a key used as input to a key derivation procedure.

In addition, each mechanism has specific requirements listed immediately prior to the mechanism description.

6 Authenticated encryption mechanism 1 (OCB 2.0)

6.1 Introduction

In this clause an authenticated encryption mechanism commonly known as OCB 2.0 (for *Offset Codebook* version 2) is defined.

NOTE OCB 2.0 is due to Krovetz and Rogaway [7]. OCB 2.0 possesses a proof of security on the assumption that the block cipher used possesses certain 'ideal properties'.

6.2 Specific notation

For the purposes of the specification of this mechanism, the following symbols and notation apply:

B Block of bits used in the definition of function J.

$B_1, B_2, \ldots, B_w$ Sequence of blocks of bits (each of n bits, with the possible exception of B_w) used in the definition of function J.

$C_1, C_2, \ldots, C_m$ Sequence of blocks of bits (each of n bits, with the possible exception of C_m) obtained as part of the output of the authenticated encryption process.

$D_1, D_2, \ldots, D_m$ Sequence of blocks of bits (each of n bits, with the possible exception of D_m) obtained by partitioning D.

F n-bit block used in the encryption and decryption processes.

H n-bit block used in the encryption and decryption processes.

J	Function used in the encryption and decryption processes.
k	Variable used in the definition of function J.
m	The number of n-bit blocks in the message to be encrypted (where the final block may contain less than n bits), i.e. the message contains $(m\text{-}1)n+r$ bits.
M_2	Function used in the encryption and decryption processes.
M_3	Function used in the encryption and decryption processes.
P	n-bit block used in the definition of M_2.
r	The number ($0 < r \leq n$) of bits in the final block of the message to be encrypted, after it has been divided into n-bit blocks, i.e. $\text{len}(D) = (m\text{-}1)n+r$.
S	Starting Variable (n bits).
T	Tag (t bits), adjoined to an encrypted message to provide integrity protection.
T'	Recomputed tag value, generated during the decryption process.
w	Variable used in the definition of function J.
Z	n-bit block used in the encryption and decryption processes.

6.3 Specific requirements

In advance of any use of the mechanism, the originator and recipient of the data to which the authenticated encryption mechanism is to be applied must agree on the tag length t in bits, where $0 < t \leq n$.

6.4 Definition of function M_2

Definition of the encryption and decryption procedures requires the definition of a function M_2 that takes an n-bit block as input and gives an n-bit block as output. The definition of this function depends on an n-bit block P. Since n must correspond to the bit length of a block cipher chosen from amongst those specified in ISO/IEC 18033-3, we only define P for n=64 and n=128.

a) If n=64, then $P = 0^{59}||11011$.

b) If n=128, then $P = 0^{120}||10000111$.

The function M_2 is defined as follows. If X is an n-bit block, then:

a) If the left-most (most significant) bit of X is zero, then $M_2(X) = X<<1$;

b) If the left-most (most significant) bit of X is one, then $M_2(X) = [X<<1] \oplus P$.

6.5 Definition of function M_3

Definition of the procedure for handling additional authenticated data requires the definition of a function M_3 that takes an n-bit block as input and gives an n-bit block as output. If X is an n-bit block, then:

$$M_3(X) = M_2(X) \oplus X.$$

6.6 Definition of function *J*

This function takes a block of bits B as input (where len(B) > 0), and gives an n-bit block $J(B)$ as output. The value $J(B)$ is computed as follows.

a) Partition B into a sequence of blocks: B_1, B_2, …, B_w, as follows. Let B_1 contain the first n bits of B, B_2 the next n bits, and so on, until B_w contains the final k bits, where $0 < k \leq n$. Thus, len(B) = (w-1)n+k.

b) Let $F = M_3(M_3(e_K(0^n)))$.

c) Let $C_0 = 0^n$.

d) For i = 1, 2, ..., w-1, perform the following two steps:

   1) Let $F = M_2(F)$;

   2) Let $C_i = C_{i-1} \oplus e_K(B_i \oplus F)$.

e) Let $F = M_3(M_2(F))$.

f) If $k<n$ then perform the following two steps:

   1) Let $F = M_3(F)$;

   2) Let $B_w = B_w \,||\, 1 \,||\, 0^{n-k-1}$.

g) $J(B) = e_K(C_{w-1} \oplus B_w \oplus F)$.

6.7 Encryption procedure

The originator shall perform the following steps to protect a data string D.

a) An n-bit Starting Variable S shall be selected. This variable shall be distinct for every message to be protected, and must be made available to the recipient of the message. However, it is not necessary that this value be unpredictable or secret.

   NOTE The value S could, for example, be generated using a counter maintained by the originator, and sent in cleartext along with the protected message.

b) Partition D into a sequence of blocks: D_1, D_2, …, D_m, as follows. Let D_1 contain the first n bits of D, D_2 the next n bits, and so on, until D_m contains the final r bits, where $0 < r \leq n$. Thus, len(D) = (m-1)n+r.

c) Let $F = e_K(S)$ and let $H = 0^n$.

d) For i = 1, 2, ..., m-1, perform the following three steps:

   1) Let $F = M_2(F)$;

   2) Let $H = H \oplus D_i$;

   3) Let $C_i = F \oplus e_K(D_i \oplus F)$.

e) Let $F = M_2(F)$.

f) Let $Z = e_K(\#_n(r) \oplus F)$.

g) Let $C_m = D_m \oplus Z|_r$.

h) Let $H = H \oplus [D_m \,||\, (Z|^{n-r})]$.

i) Let $T = [e_K(H \oplus M_3(F))]|_t$.

j) If len(A) > 0, then let $T = T \oplus J(A)|_t$.

The output of the above process, i.e. the authenticated-encrypted version of D, shall be the bit-string:

$$C = C_1 \,||\, C_2 \,||\, \ldots \,||\, C_m \,||\, T$$

i.e. a string of $(m\text{-}1)n+r+t$ bits, that is C contains precisely t bits more than D (although it is also necessary to convey the n-bit Starting Variable S and the variable length additional authenticated data bit string A to the recipient).

6.8 Decryption procedure

The recipient shall perform the following steps to decrypt and verify an authenticated-encrypted string C.

a) If the length of C is less than t then halt and output INVALID.

b) Let m and r be the unique integers defined so that C contains a total of $(m\text{-}1)n + r + t$ bits, where $0 < r \leq n$. Partition C into a sequence of blocks: $C_1, C_2, \ldots, C_m, T$ as follows. Let C_1 contain the first n bits of C, C_2 the next n bits of C, and so on, until C_m contains the next r bits of C. Finally, let T be the final t bits of C.

c) Let $F = e_K(S)$ and let $H = 0^n$.

d) For i = 1, 2, ..., m-1, perform the following three steps:

   1) Let $F = M_2(F)$;

   2) Let $D_i = F \oplus d_K(C_i \oplus F)$;

   3) Let $H = H \oplus D_i$.

e) Let $F = M_2(F)$.

f) Let $Z = e_K(\#_n(r) \oplus F)$.

g) Let $D_m = C_m \oplus Z|_r$.

h) Let $H = H \oplus [D_m \,||\, (Z|^{n-r})]$.

i) Let $T' = [e_K(H \oplus M_3(F))]|_t$.

j) If len(A) > 0, then let $T' = T' \oplus J(A)|_t$.

k) If $T = T'$, then output D and the additional authenticated data A. Otherwise output INVALID.

7 Authenticated encryption mechanism 2 (Key Wrap)

7.1 Introduction

In this clause an authenticated encryption mechanism commonly known as Key Wrap is defined.

NOTE 1 This scheme was originally designed for authenticated-encryption of keys and associated information. That is, it is designed for use with short data strings. However, the scheme can be used with arbitrary length data strings (up to a maximum of around 2^{67} bits), although it is not efficient for protecting long messages.

NOTE 2 This mode is known as AES Key Wrap when the AES block cipher is used, where AES stands for Advanced Encryption Standard, a block cipher algorithm specified in ISO/IEC 18033-3. AES Key Wrap is also specified in [9] and [11].

7.2 Specific notation

For the purposes of the specification of this mechanism, the following symbols and notation apply:

$C_0, C_1, \ldots, C_m$	Sequence of (m+1) 64-bit blocks obtained as the output of the authenticated encryption process.
$D_1, D_2, \ldots, D_m$	Sequence of m 64-bit blocks obtained by partitioning D, i.e. $64m$ = len(D).
$R_1, R_2, \ldots, R_m$	Sequence of m 64-bit blocks computed during the encryption and decryption processes.
Y	64-bit block used during the encryption and decryption processes.
Z	128-bit block computed during the encryption and decryption processes.

7.3 Specific requirements

The block cipher to be used with this mechanism must be a 128-bit block cipher, i.e. it must have n=128.

The data string D to be protected using this mechanism must contain at least 128 bits and must contain a multiple of 64 bits (i.e. the bit-length of D must be $64m$ for some integer $m > 1$).

7.4 Encryption procedure

The originator shall perform the following steps to protect a data string D.

a) Partition D into a sequence of m 64-bit blocks $D_1, D_2, \ldots, D_m$, so that D_1 contains the first 64 bits of D, D_2 the next 64 bits, and so on.

b) Let Y be the 64-bit block having hexadecimal representation A6A6A6A6A6A6A6A6, i.e. in binary it equals (10100110 10100110 … 10100110).

c) For $i = 1, 2, \ldots, m$:

   let $R_i = D_i$.

d) For $i = 1, 2, \ldots, 6m$, perform the following four steps:

   1) Let $Z = e_K(Y \,||\, R_1)$;

   2) Let $Y = Z|_{64} \oplus \#_{64}(i)$;

   3) For $j = 1, 2, \ldots, m$-1:

      let $R_j = R_{j+1}$;

   4) Let $R_m = Z|^{64}$.

e) Let $C_0 = Y$.

f) For $i = 1, 2, \ldots, m$:

let $C_i = R_i$.

The output of the above process, i.e. the authenticated-encrypted version of D, shall be the bit-string:

$C = C_0 \,||\, C_1 \,||\, \ldots \,||\, C_m$

i.e. a string of $64(m+1)$ bits, that is C contains precisely 64 bits more than D.

7.5 Decryption procedure

The recipient shall perform the following steps to decrypt and verify an authenticated-encrypted string C.

a) If len(C) is not a multiple of 64 or is less than 192, then halt and output INVALID.

b) Partition C into a sequence of $m+1$ 64-bit blocks $C_0, C_1, \ldots, C_m$, so that C_0 contains the first 64 bits of C, C_1 the next 64 bits, and so on.

c) Let $Y = C_0$.

d) For $i = 1, 2, \ldots, m$:

let $R_i = C_i$.

e) For $i = 6m, 6m\text{-}1$, down to 1, perform the following four steps:

1) Let $Z = d_K([Y \oplus \#_{64}(i)] \,||\, R_m)$;

2) Let $Y = Z|_{64}$;

3) For $j = m, m\text{-}1, \ldots, 2$:

let $R_j = R_{j-1}$;

4) Let $R_1 = Z|^{64}$.

f) If Y = (10100110 10100110 … 10100110), then output $D = R_1 \,||\, R_2 \,||\, \ldots \,||\, R_m$. Otherwise output INVALID.

8 Authenticated encryption mechanism 3 (CCM)

8.1 Introduction

In this clause an authenticated encryption mechanism commonly known as CCM (for *Counter with CBC-MAC*) is defined.

NOTE CCM is due to Whiting, Housley and Ferguson [12]. The version of CCM defined here is a special case of CCM as defined in [10] and [12].

8.2 Specific notation

For the purposes of the specification of this mechanism, the following symbols and notation apply:

B	Block of bits used in computing the tag value.
$B_1, B_2, \ldots, B_v$	Sequence of blocks of bits (each of n bits) used in computing the tag value.

$C_1, C_2, \ldots, C_m$	Sequence of m 128-bit blocks obtained as part of the output of the authenticated encryption process.
$D_1, D_2, \ldots, D_m$	Sequence of m 128-bit blocks obtained by partitioning a padded version of D.
F	Flag octet.
L	Length of D (in octets), excluding padding and the length block D_0.
r	The number of octets of D in the block D_m.
S	Starting Variable (of 120-8w bits).
T	Plaintext tag value (of t bits).
T'	Recomputed tag value, generated during the decryption process.
U	Encrypted tag value (of t bits).
v	Variable used in computing the tag value.
w	Length of message length field in octets.
X	128-bit block computed during the encryption and decryption processes.
Y	128-bit block computed during the encryption and decryption processes.

8.3 Specific requirements

In advance of any use of the mechanism, the originator and recipient of the data to which the authenticated encryption mechanism is to be applied, must agree on:

a) t, the bit-length of the tag; t must be chosen from the set {32, 48, 64, 80, 96, 112, 128}, and

b) w, the octet-length of the message length field; w must be chosen from the set {2, 3, 4, 5, 6, 7, 8}.

NOTE The choice of w affects the maximum message length which can be protected. The maximum message length is 2^{8w+3} bits, i.e. 2^{8w} octets.

The block cipher to be used with this mechanism must be a 128-bit block cipher, i.e. it must have n=128.

The data string D to be protected using this mechanism, and the additional authenticated data string A, must contain a whole number of octets, i.e. their lengths must be a multiple of 8 bits (i.e. len(D) and len(A) must both be an integer multiple of 8).

8.4 Encryption procedure

The originator shall perform the following steps to protect a data string D. Let L =len(D)/8, i.e. L is the number of octets in D.

a) A Starting Variable S containing 15-w octets (i.e. 120-8w bits) shall be selected. This variable shall be distinct for every message to be protected, and must be made available to the recipient of the message. However, it is not necessary that this value is unpredictable or secret.

NOTE The value S could, for example, be generated using a counter maintained by the originator, and sent in cleartext along with the protected message.

b) Right pad the data string D with 16-r zero octets (i.e. between 0 and 120 zero bits) so that the padded version of D contains a multiple of 128 bits. Then partition the padded version of D into a sequence of m 128-bit blocks D_1, D_2, …, D_m, so that D_1 contains the first 128 bits of D, D_2 the next 128 bits, and so on.

NOTE The value m must satisfy $16(m\text{-}1) < L \leq 16m$.

c) If len(A) = 0 then let the flag octet $F = 0^2 \,||\, \#_3((t\text{-}16)/16) \,||\, \#_3(w\text{-}1)$.

d) If len(A) > 0 then let the flag octet $F = 0 \,||\, 1 \,||\, \#_3((t\text{-}16)/16) \,||\, \#_3(w\text{-}1)$.

NOTE The most significant (left-most) bit of F is a 'reserved' bit, i.e. it is set to zero for the version of the mechanism specified here, but may be used in the future in other (as yet unspecified) versions of the mechanism. The next to the most significant bit of F is set to zero to indicate that all the data being protected by the mechanism is encrypted.

e) Let $X = e_K(F \,||\, S \,||\, \#_{8w}(L))$.

f) If len(A) > 0, then perform the following six steps:

1) If $0 <$ len(A) < 65280 then let $B = \#_{16}(\text{len}(A)/8) \,||\, A$;

2) If $65280 \leq$ len(A) $< 2^{32}$ then let $B = 1^{15} \,||\, 0 \,||\, \#_{32}(\text{len}(A)/8) \,||\, A$;

3) If $2^{32} \leq$ len(A) $< 2^{64}$ then let $B = 1^{16} \,||\, \#_{64}(\text{len}(A)/8) \,||\, A$;

4) Partition B into a sequence of blocks: B_1, B_2, …, B_v, as follows: let B_1 contain the first n bits of B, B_2 the next n bits, and so on, until B_v contains the final k bits, where $0 < k \leq n$; thus, len(B) = $(v\text{-}1)n+k$;

5) Right pad B_v with n-k zeros, i.e. let $B_v = B_v \,||\, 0^{n-k}$;

6) For i = 1, 2, …, v:

let $X = e_K(\, X \oplus B_i \,)$.

g) For i = 1, 2, …, m:

let $X = e_K(\, X \oplus D_i \,)$.

h) Let $T = X|_t$.

NOTE The plaintext tag T is equal to a MAC computed on the data string B_1, B_2, ..., B_v, D_1, D_2, …, D_m using a slight modification of MAC algorithm 1 specified in ISO/IEC 9797-1.

i) Let the flag octet $F = (\, 0^5 \,||\, \#_3(w\text{-}1) \,)$, and let $Y = (\, F \,||\, S \,||\, 0^{8w} \,)$.

NOTE The two most significant (left-most) bits of F are 'reserved' bits, i.e. they are set to zero for the version of the mechanism specified here, but may be used in the future in other (as yet unspecified) versions of the mechanism. The next three most significant bits of F are set to zero to ensure that this octet is distinct from the flag octet used in step c above.

j) Let $U = T \oplus [e_K(Y)]|_t$.

k) For i = 1, 2, …, m-1, perform the following two steps:

1) Let $Y = (\, F \,||\, S \,||\, \#_{8w}(i) \,)$;

2) Let $C_i = D_i \oplus e_K(Y)$.

l) Let $Y = (\, F \,||\, S \,||\, \#_{8w}(m) \,)$, and let $C_m = [D_m \oplus e_K(Y)\,]|_{8r}$.

The output of the above process, i.e. the authenticated-encrypted version of D, shall be the bit-string:

$$C = C_1 \,||\, C_2 \,||\, \ldots \,||\, C_{m-1} \,||\, C_m \,||\, U$$

i.e. a string of $8L+t$ bits, that is C contains precisely t bits more than the original data string D (although it is also necessary to convey the (120-8w)-bit Starting Variable S and the variable length additional authenticated data A to the recipient).

8.5 Decryption procedure

The recipient shall perform the following steps to decrypt and verify an authenticated-encrypted string C.

a) If C does not contain a whole number of octets, then halt and output INVALID.

b) If the length of C is less than (t+8) bits, then halt and output INVALID.

c) Let m and r be the unique integers such that C contains a total of 128(m-1) + 8r + t bits, where $0 < r \leq 16$. Partition C into a sequence of blocks: C_1, C_2, …C_m, U as follows. Let C_1 contain the first 128 bits of C, C_2 the next 128 bits of C, and so on, until C_m contains the next 8r bits of C. Finally, let U be the final t bits of C.

d) Let the flag octet $F = (0^5 \,||\, \#_3(w\text{-}1))$, and let $Y = (F \,||\, S \,||\, 0^{8w})$.

e) Let $T = U \oplus [e_K(Y)]|_t$.

f) For i = 1, 2, …, m-1, perform the following two steps:

   1) Let $Y = (F \,||\, S \,||\, \#_{8w}(i))$;

   2) Let $D_i = C_i \oplus e_K(Y)$.

g) Let $Y = (F \,||\, S \,||\, \#_{8w}(m))$, and let $D_m = C_m \oplus [e_K(Y)]|_{8r}$.

h) Let $D = D_1 \,||\, D_2 \,||\, \ldots \,||\, D_m$, and let $L = 16m - 16 + r$.

i) Right pad D_m with 128-8r zeros, i.e. let $D_m = D_m \,||\, 0^{128-8r}$.

j) If len(A) = 0 then let the flag octet $F = 0^2 \,||\, \#_3((t\text{-}16)/16) \,||\, \#_3(w\text{-}1)$.

k) If len(A) > 0 then let the flag octet $F = 0 \,||\, 1 \,||\, \#_3((t\text{-}16)/16) \,||\, \#_3(w\text{-}1)$.

l) Let $X = e_K(F \,||\, S \,||\, \#_{8w}(L))$.

m) If len(A) > 0, then perform the following six steps:

   1) If $0 <$ len(A) < 65280 then let $B = \#_{16}(\text{len}(A)/8) \,||\, A$;

   2) If $65280 \leq$ len(A) $< 2^{32}$ then let $B = 1^{15} \,||\, 0 \,||\, \#_{32}(\text{len}(A)/8) \,||\, A$;

   3) If $2^{32} \leq$ len(A) $< 2^{64}$ then let $B = 1^{16} \,||\, \#_{64}(\text{len}(A)/8) \,||\, A$;

   4) Partition B into a sequence of blocks: B_1, B_2, …, B_v, as follows: let B_1 contain the first n bits of B, B_2 the next n bits, and so on, until B_v contains the final k bits, where $0 < k \leq n$; thus, len(B) = (v-1)n+k;

   5) Right pad B_v with n-k zeros, i.e. let $B_v = B_v \,||\, 0^{n-k}$;

   6) For i = 1, 2, …, v:

let $X = e_K(X \oplus B_i)$.

n) For $i = 1, 2, \ldots, m$:

let $X = e_K(X \oplus D_i)$.

o) Let $T' = X|_t$.

p) If $T = T'$, then output D as computed in step h) and A. Otherwise output INVALID.

9 Authenticated encryption mechanism 4 (EAX)

9.1 Introduction

In this clause an authenticated encryption mechanism commonly known as EAX is defined.

NOTE EAX is due to Bellare, Rogaway and Wagner [2]. The letters EAX do not appear to stand for anything in particular.

9.2 Specific notation

For the purposes of the specification of this mechanism, the following symbols and notation apply:

$C_1, C_2, \ldots, C_m$	Sequence of blocks of bits (each of n bits, with the possible exception of C_m) obtained as part of the output of the authenticated encryption process.
$D_1, D_2, \ldots, D_m$	Sequence of blocks of bits (each of n bits, with the possible exception of D_m) obtained by partitioning D.
E_0, E_1, E_2	n-bit blocks computed during the encryption and decryption processes.
M	Function used in the encryption and decryption processes.
S	Starting Variable (n bits).
T	Tag (t bits), adjoined to an encrypted message to provide integrity protection.
T'	Recomputed tag value, generated during the decryption process.
W	n-bit block computed during the encryption and decryption processes.

9.3 Specific requirements

In advance of any use of the mechanism, the originator and recipient of the data to which the authenticated encryption mechanism is to be applied, must agree on:

a) t, the length of the tag in bits, where $0<t\leq n$.

9.4 Definition of function *M*

Definition of the encryption and decryption procedures requires the definition of a function M that takes an arbitrary length string of bits and a block cipher key as input and gives an n-bit block as output. The definition of this function is as follows.

If X is a string of bits, and K is a key for the chosen block cipher, then $M_K(X)$ shall equal an (untruncated) message authentication code computed on the string X using key K using MAC algorithm 5 of ISO/IEC 9797-1

(fourth edition), where the block cipher used in the MAC algorithm shall be the same as the block cipher algorithm selected for the authenticated encryption process.

NOTE MAC algorithm 5 of ISO/IEC 9797-1 (4th edition) is also known as OMAC.

9.5 Encryption procedure

The originator shall perform the following steps to protect a data string D.

a) A Starting Variable S containing n bits shall be selected. This variable shall be distinct for every message to be protected, and must be made available to the recipient of the message. However, it is not necessary that this value is unpredictable or secret.

b) Let $E_0 = M_K(0^n||S)$.

c) Let $E_1 = M_K(0^{n-1}||1||A)$.

d) Let $W = E_0$.

e) Partition D into a sequence of blocks: $D_1, D_2, \ldots, D_m$, as follows. Let D_1 contain the first n bits of D, D_2 the next n bits, and so on, until D_m contains the final r bits, where $0 < r \leq n$. Thus len(D) = (m-1)n+r.

f) For i = 1, 2, ..., m-1, perform the following two steps:

   1) Let $C_i = D_i \oplus e_K(W)$;

   2) Let $W = \#_n(\#^{-1}(W) + 1 \bmod 2^n)$.

g) Let $C_m = D_m \oplus [e_K(W)]|_r$.

h) Let $E_2 = M_K(0^{n-2}||1||0||C_1||C_2||\ldots||C_m)$.

i) Let $T = [E_0 \oplus E_1 \oplus E_2]|_t$.

The output of the above process, i.e. the authenticated-encrypted version of D, shall be the bit-string:

$C = C_1 \,||\, C_2 \,||\, \ldots \,||\, C_m \,||\, T$

i.e. a string of (m-1)n+r+t bits, that is C contains precisely t bits more than D (although it is also necessary to convey the n-bit Starting Variable S and the variable length additional authenticated data A to the recipient).

9.6 Decryption procedure

The recipient shall perform the following steps to decrypt and verify an authenticated-encrypted string C.

a) If the length of C is less than t, then halt and output INVALID.

b) Let m and r be the unique integers defined so that C contains a total of (m-1)n + r + t bits, where $0 < r \leq n$. Partition C into a sequence of blocks: $C_1, C_2, \ldots C_m, T$ as follows. Let C_1 contain the first n bits of C, C_2 the next n bits of C, and so on, until C_m contains the next r bits of C. Finally, let T be the final t bits of C.

c) Let $E_0 = M_K(0^n||S)$.

d) Let $E_1 = M_K(0^{n-1}||1||A)$.

e) Let $E_2 = M_K(0^{n-2}||1||0||C_1||C_2||\ldots||C_m)$.

f) Let $T' = [E_0 \oplus E_1 \oplus E_2]|_t$.

g) If $T \neq T'$, then halt and output INVALID.

h) Let $W = E_0$.

i) For i = 1, 2, ..., m-1, perform the following two steps:

1) Let $D_i = C_i \oplus e_K(W)$;

2) Let $W = \#_n(\#^{-1}(W) + 1 \bmod 2^n)$.

j) Let $D_m = C_m \oplus [e_K(W)]|_r$.

k) Output D and A.

10 Authenticated encryption mechanism 5 (Encrypt-then-MAC)

10.1 Introduction

In this clause an authenticated encryption mechanism made up of the combination of any encryption mechanism and any MAC scheme is defined. This scheme involves first encrypting the data to be protected, and then computing a MAC on the resulting encrypted data.

NOTE The Encrypt-then-MAC approach has been analysed by Bellare and Namprempre [1], who provide a proof of security on the assumption that the method of encryption and the MAC technique possess certain security properties.

10.2 Specific notation

For the purposes of the specification of this mechanism, the following symbols and notation apply:

C'	Bit string obtained by encrypting the data string D.
δ	The decryption function, i.e. a function which takes as input a block cipher key K_1 and an encrypted data string C' and, using the selected mode of operation, outputs a decrypted data string: the output is written $\delta_{K_1}(C')$.
ε	The encryption function, i.e. a function which takes as input a block cipher key K_1 and a data string D and, using the selected mode of operation, outputs an encrypted data string: the output is written $\varepsilon_{K_1}(D)$.
f	The MAC function; if X is an input string, and K_2 is a MAC key, then the output MAC is written $f_{K_2}(X)$.
K_1	Secret key for the block cipher.
K_2	Secret key for the MAC function.
S	Starting Variable (n bits).
T	Tag (t bits), adjoined to an encrypted message to provide integrity protection.
T'	Recomputed tag value, generated during the decryption process.

10.3 Specific requirements

In advance of any use of the mechanism, the originator and recipient of the data to which the authenticated encryption mechanism is to be applied, must agree on:

a) a block cipher mode of operation from amongst those specified in ISO/IEC 10116 (the ECB mode shall not be used),

b) a method for MAC computation, which shall be selected from the techniques specified in ISO/IEC 9797 (we suppose that the chosen method generates a tag of length t bits), and

c) a method for deriving a pair of secret keys (K_1, K_2) from the secret key K, where K_1 is a key for the selected block cipher and K_2 is a key for the selected method of MAC computation.

NOTE 1 K shall be chosen so that the number of possible values for K is at least as large as the number of possible values for the block cipher key, and also at least as large as the number of possible values for the MAC key.

NOTE 2 Possible methods for deriving (K_1, K_2) from the secret key K include: (a) let $K = K_1||K_2$ (where K is chosen to be of the appropriate length), and (b) K_1 and K_2 are derived by taking (disjoint) bit strings from $h(K)$, where h is a hash-function chosen from amongst those specified in ISO/IEC 10118 giving a suitable length output.

10.4 Encryption procedure

The originator shall perform the following steps to protect a data string D.

a) A Starting Variable S appropriate for use with the selected block cipher mode of operation shall be selected. This variable shall be distinct for every message to be protected during the lifetime of a key, and must be made available to the recipient of the message. Further possible requirements for S are as described in the appropriate clauses of ISO/IEC 10116.

b) Let $C' = \varepsilon_{K_1}(D)$.

c) Let $T = f_{K_2}(C')$.

The output of the above process, i.e. the authenticated-encrypted version of D, shall be the bit-string:

$C = C' \,||\, T$.

10.5 Decryption procedure

The recipient shall perform the following steps to decrypt and verify an authenticated-encrypted string C.

a) If the length of C is less than t then halt and output INVALID.

b) Let T be the rightmost t bits of C, and let C' be equal to C with the rightmost t bits removed, i.e. $C = C' \,||\, T$.

c) Let $T' = f_{K_2}(C')$.

d) If $T \neq T'$, then halt and output INVALID.

e) Let $D = \delta_{K_1}(C')$.

f) Output D.

11 Authenticated encryption mechanism 6 (GCM)

11.1 Introduction

In this clause an authenticated encryption mechanism commonly known as GCM (for Galois/Counter Mode) is defined.

NOTE 1 GCM is due to McGrew and Viega[8].

11.2 Specific notation

For the purposes of the specification of this mechanism, the following symbols and notation apply:

$C_1, C_2, ..., C_m$	Sequence of m 128-bit blocks (with the possible exception of C_m, which may contain between 1 and 128 bits) obtained as part of the output of the authenticated encryption process.
$D_1, D_2, ..., D_m$	Sequence of m 128-bit blocks of bits (with the possible exception of D_m) obtained by partitioning D.
G	Function used in the encryption and decryption processes (defined in clause 11.4).
H	128-bit block used in the encryption and decryption processes.
inc	Function taking a 128-bit block as input and giving a 128-bit block as output, where, if X is a 128-bit block: $\text{inc}(X) = (X\|_{96}) \| \#_{32}(\#^{-1}(X\|^{32})+1 \bmod 2^{32})$.
r	The number of bits in the final block of the message to be encrypted, after it has been divided into n-bit blocks, i.e. the message contains $(m-1)n+r$ bits.
R	128-bit block used in the computation of a GF(2^{128}) multiplication.
S	Starting Variable (variable length).
T	Tag (t bits), adjoined to an encrypted message to provide integrity protection.
T'	Recomputed tag value, generated during the decryption process.
U, V, W, Z	128-bit blocks used in defining the computation of a GF(2^{128}) multiplication.
$X_0, X_1, ..., X_{k+l+1}$	128-bit blocks used in computing the function G.
$Y_0, Y_1, ..., Y_m$	Sequence of 128-bit blocks used in the encryption and decryption processes.
{ }	A bit-string with zero length.
•	Multiplication in the field GF(2^{128}). The polynomial to be used to determine the representation of GF(2^{128}) is $1+\alpha+\alpha^2+\alpha^7+\alpha^{128}$.

11.3 Specific requirements

In advance of any use of the mechanism, the originator and recipient of the data to which the authenticated encryption mechanism is to be applied, must agree on:

a) The tag length t in bits, where t must be a multiple of 8 satisfying $96 \le t \le 128$ (t=32 and t=64 are also permitted for specialized applications).

The block cipher to be used with this mechanism must be a 128-bit block cipher, i.e. it must have n=128.

11.4 Definition of multiplication operation •

Suppose U and V are 128-bit blocks; then $W = U \bullet V$ is defined as follows, where W is also a 128-bit block. Note that, in the description below, v_i denotes the ith bit of V, i.e. $V = v_0||v_1||...||v_{127}$. Analogously, z_{127} denotes the rightmost bit of Z.

a) Let $R = 11100001 || 0^{120}$.

b) Let $W = 0^{128}$.

c) Let $Z = U$.

d) For $i = 0, 1, ..., 127$, perform the following two steps:

1) if $v_i = 1$ then let $W = W \oplus Z$;

2) if $z_{127} = 0$ then let $Z = Z>>1$; otherwise let $Z = (Z>>1) \oplus R$.

11.5 Definition of function *G*

The encryption and decryption procedures make use of a function G, that takes as input a 128-bit block and two arbitrary length strings of bits, and gives a 128-bit block as output. Let H be a 128-bit block, and W and Z be two arbitrary length (possible empty) strings of bits. Suppose that k and u are the unique integers such that $\text{len}(W) = 128(k-1)+u$ and $0 < u \leq 128$; similarly suppose that l and v are the unique integers such that $\text{len}(Z) = 128(l-1)+v$ and $0 < v \leq 128$. Let $W_1, W_2, ..., W_k$ be the sequence of 128-bit blocks (with the possible exception of W_k which contains the final u bits of W) obtained by partitioning W; similarly, let $Z_1, Z_2, ..., Z_l$ be the sequence of 128-bit blocks (with the possible exception of Z_l which contains the final v bits of Z) obtained by partitioning Z.

Then $G(H,W,Z)$ is the 128-bit value X_{k+l+1}, where X_i is recursively defined for $i = 0, 1, ..., k+l-1$, as follows:

a) $X_0 = 0^{128}$.

b) $X_i = (X_{i-1} \oplus W_i) \bullet H$, $\quad 1 \leq i \leq k-1$ (this step is omitted if $k \leq 1$).

c) $X_k = (X_{k-1} \oplus (W_k||0^{128-u})) \bullet H$ (this step is omitted if $k=0$).

d) $X_i = (X_{i-1} \oplus Z_{i-k}) \bullet H$, $\quad k+1 \leq i \leq k+l-1$ (this step is omitted if $l \leq 1$).

e) $X_{k+l} = (X_{k+l-1} \oplus (Z_l||0^{128-v})) \bullet H$ (this step is omitted if $l=0$).

f) $X_{k+l+1} = (X_{k+l} \oplus [\#_{64}(\text{len}(W)) || \#_{64}(\text{len}(Z))]) \bullet H$.

11.6 Encryption procedure

The originator shall perform the following steps to protect a data string D and ensure the integrity of an additional authenticated data string A.

a) A variable length Starting Variable S shall be selected. This value shall be distinct for every message to be protected, and must be made available to the recipient of the message. However, it is not necessary that this value be unpredictable or secret.

NOTE The value S could, for example, be generated using a counter maintained by the originator, and sent in clear text along with the protected message.

b) Partition D into a sequence of 128-bit blocks: $D_1, D_2, ..., D_m$, as follows. Let D_1 contain the first 128 bits of D, D_2 the next 128 bits, and so on, until D_m contains the final r bits, where $0 < r \leq 128$. Thus D contains a total of $(m-1)n+r$ bits.

c) Let $H = e_K(0^{128})$.

d) If len(S) = 96 then let $Y_0 = S \,||\, 0^{31} \,||\, 1$. Otherwise let $Y_0 = G(H, \{\}, S)$.

e) For i = 1, 2, ..., m-1, perform the following two steps:

1) let $Y_i = \text{inc}(Y_{i-1})$;

2) let $C_i = D_i \oplus e_K(Y_i)$.

f) Let $Y_m = \text{inc}(Y_{m-1})$.

g) Let $C_m = D_m \oplus (e_K(Y_m))|_r$.

h) Let $T = (G(H, A, C) \oplus e_K(Y_0))|_t$.

The output of the above process, i.e. the authenticated-encrypted version of *D,* shall be the bit-string:

$C = C_1 \,||\, C_2 \,||\, \ldots \,||\, C_m \,||\, T$

i.e. a string of $(m\text{-}1)n+r+t$ bits, that is C contains precisely t bits more than D (although it is also necessary to convey the variable length starting variable S and the variable length additional authenticated data A to the recipient).

11.7 Decryption procedure

The recipient shall perform the following steps to decrypt and verify an authenticated-encrypted string C and to verify the additional authenticated data A.

a) If the length of C is less than t then halt and output INVALID.

b) Let m and r be the unique integers defined so that len(C) = $(m\text{-}1)n+r+t$, where $0 < r \leq n$. Partition C into a sequence of blocks: $C_1, C_2, \ldots, C_m, T$ as follows. Let C_1 contain the first n bits of C, C_2 the next n bits of C, and so on, until C_m contains the next r bits of C. Finally, let T be the final t bits of C.

c) Let $H = e_K(0^{128})$.

d) If len(S) = 96 then let $Y_0 = S \,||\, 0^{31} \,||\, 1$. Otherwise let $Y_0 = G(H, \{\}, S)$.

e) Let $T' = (G(H, A, C) \oplus e_K(Y_0))|_t$.

f) If $T \neq T'$, then halt and output INVALID.

g) For i = 1, 2, ..., m-1, perform the following two steps:

1) let $Y_i = \text{inc}(Y_{i-1})$;

2) let $D_i = C_i \oplus e_K(Y_i)$.

h) Let $Y_m = \text{inc}(Y_{m-1})$.

i) Let $D_m = C_m \oplus (e_K(Y_m))|_r$.

j) Output D and the additional authenticated data A.

Annex A (informative)

Guidance on use of the mechanisms

A.1 Introduction

The purpose of this annex is to provide guidance on the use of the mechanisms defined in this International Standard. Use of each mechanism requires the choice of mechanism-specific parameters, and recommendations regarding choices of parameters are provided in clauses A.3-A.8. In the remainder of this clause, recommendations are made with respect to the requirements applying to all mechanisms in this standard (see clause 5).

All mechanisms require the selection of a block cipher from amongst those standardized in ISO/IEC 18033-3. The block length n of the block cipher must be at least 64, and wherever possible use of a block cipher with n = 128 is recommended. The use of a block cipher with n = 128 is mandatory for mechanisms 2, 3 and 6.

All mechanisms also require that the originator and recipient of protected data share a secret key K. This key should be known only to these two parties and, possibly, by third parties trusted for this purpose by both originator and receiver. There are many ways in which this key could be established; however, the use of a key establishment mechanism specified in ISO/IEC 11770-2 or ISO/IEC 11770-3 is recommended.

All six mechanisms require the choice of a tag length. The choice of this parameter affects the degree of assurance provided to the recipient regarding the integrity and origin of a protected message. For further details see Annex C of ISO/IEC 9797-1.

A.2 Selection of mechanism

All the mechanisms specified in this standard are believed to provide a high level of security. However, some mechanisms are more suitable than others for particular applications. When selecting a mechanism for use, the facts given in Table 1 and those listed below should be taken into consideration.

Table 1 — Properties of mechanisms

Mechanism number	**1**	**2**	**3**	**4**	**5**	**6**
Approximate number of block cipher operations required to encrypt a q-bit message	q/n	$12\lceil q/n \rceil$	$2q/n$	$2q/n$	Depends on encryption and MAC methods used	q/n
Licence possibly required	Yes	No	No	No	Depends on encryption and MAC methods used	No
Specifically designed for use with short messages	No	Yes	No	No	No	No
Message length must be known prior to starting encryption	No	No	Yes	No	No	No
Starting value required	Yes	No	Yes	Yes	Yes	Yes
Previously standardised	No	Yes	Yes	No	No	Yes

a) Mechanisms 3 and 4 are methods for combining block cipher encryption in CTR mode (see ISO/IEC 10116) with a message authentication code.

b) Mechanism 5 provides a method for combining standardised methods for encryption and MAC computation. If implementations of such functions are already available, then mechanism 5 may have some implementation advantages.

c) Mechanism 6 is suitable for high-throughput hardware implementations, since it can be implemented without pipeline stalls.

A.3 Mechanism 1 (OCB 2.0)

This mechanism requires the selection of a tag length parameter t ($t \leq n$). The choice of the tag length t depends on the environment within which the mechanism is to be used; however, unless there are strong reasons to make a different choice, use of $t \geq 64$ is recommended.

A.4 Mechanism 2 (Key Wrap)

This mechanism requires the block cipher used to have $n = 128$. Use of one of the block ciphers with this property specified in ISO/IEC 18033-3 is mandated (see clause 5).

A.5 Mechanism 3 (CCM)

This mechanism requires the block cipher used to have $n = 128$. Use of one of the block ciphers with this property specified in ISO/IEC 18033-3 is mandated (see clause 5).

This mechanism requires the selection of a tag length parameter t (from the set {32, 48, 64, 80, 96, 112, 128}). The choice of the tag length t depends on the environment within which the mechanism is to be used; however, unless there are strong reasons to make a different choice, use of $t \geq 64$ is recommended.

This mechanism requires the selection of the length w (in octets) of the message field (from the set {2, 3, 4, 5, 6, 7, 8}). The choice of the octet-length of the message length field w also depends on the environment within which the mechanism is to be used. The choice of w does not affect the level of security provided by the mechanism. Larger values of w allow longer message lengths, although they also reduce the length of the remainder of the Starting Variable. Nevertheless, even if w is chosen to be the maximum possible value, i.e. w=8, 56 bits of the Starting Variable can be selected to ensure that a different Starting Variable is used for every message, which should be sufficient for most, if not all, practical applications. For the majority of applications a value of $w = 4$, i.e. giving a maximum message length of $2^{32} \approx 4 \times 10^9$ octets, is likely to be adequate.

A.6 Mechanism 4 (EAX)

This mechanism requires the selection of a tag length parameter t ($t \leq n$). The choice of the tag length t depends on the environment within which the mechanism is to be used; however, unless there are strong reasons to make a different choice, use of $t \geq 64$ is recommended.

A.7 Mechanism 5 (Encrypt-then-MAC)

This mechanism requires the choice of a mode of operation and a method for MAC computation. The security offered by the resulting authenticated encryption scheme will depend on the security of the two underlying primitives.

A.8 Mechanism 6 (GCM)

This mechanism requires the block cipher used to have n = 128. Use of one of the block ciphers with this property specified in ISO/IEC 18033-3 is mandated (see clause 5).

The variable length starting variable, S, shall be selected such that $1 \leq \text{len}(S) \leq 2^{64}$. The requirement that starting variables are never re-used during the lifetime of a key is critical to the security of this mechanism.

The tag length t shall be selected such that t is a multiple of 8 satisfying $96 \leq t \leq 128$ (t=32 and t=64 are also permitted for specialized applications, although these options should only be used with great care – detailed guidance on use of these tag lengths is provided in Appendix C of [8]).

The data string, D, to which the authenticated encryption mechanism is to be applied shall satisfy

$$\text{len}(D) \leq 2^{39}-256,$$

and the additional authenticated data string A shall satisfy $\text{len}(A) \leq 2^{64}$. The total number of data blocks and additional authenticated data blocks to which GCM shall be applied for a fixed key K shall be at most 2^{64}. In addition, the total number of invocations of the encryption procedure for any given key shall be at most 2^{32}, unless $\text{len}(S) = 96$ for every use of that key.