International Standard

ISO 20038

Banking and related financial services — Key wrap using advanced encryption standard (AES)

Banque et autres services financiers — Enveloppe de clé utilisant AES (norme de chiffrement avancé)

Second edition
2026-08

Reference number
ISO 20038:2026(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO 20038:2017), which has been technically revised.

The main changes are as follows:

— updated for compatibility with ANSI X9.143-2022.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The secure management of cryptographic keys requires that their values and usage constraints be protected for both confidentiality and integrity.

This document provides a method of wrapping cryptographic keys in order to provide confidentiality and integrity protection for the keys when being transmitted or stored. The mechanism is designed to use advanced encryption standard (AES) specified in FIPS 197 as the wrapping cipher.

Banking and related financial services — Key wrap using advanced encryption standard (AES)

1 Scope

This document defines a method for packaging cryptographic keys for transport. This method can also be used for the storage of keys under an advanced encryption standard (AES) key. The method uses the block cipher AES as the wrapping cipher algorithm.

Other methods for wrapping keys are outside the scope of this document but can use the authenticated encryption algorithms specified in ISO/IEC 19772.

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 8601-1, *Date and time — Representations for information interchange — Part 1: Basic rules*

ISO 9564-5, *Financial services — Personal identification number (PIN) management and security — Part 5: Methods for the generation, change, and verification of PINs*

ISO 11568, *Financial services — Key management (retail)*

ANSI X9.24-1-2017, *Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques*

ANSI X9.24-2-2021, *Retail Financial Services Symmetric Key Management - Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys*

ANSI X9.24-3-2017, *Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction*

ANSI X9.102-2020, *Symmetric Key Cryptography For the Financial Services Industry – Wrapping of Keys and Associated Data*

ANSI X9.132-xxx, *Issuer PIN Generation, Verification, and Storage Methodologies Using AES*

ANSI X9.143-2022, *Retail Financial Services Interoperable Secure Key Block Specification*

ANSI X9.139, *Retail Financial Services Interoperable Secure Key Block using Asymmetric Techniques*

ANS X9 TR-31, *Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms*

ANS X9 TR-34, *Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport*

IETF RFC 4648, *The Base16, Base32, and Base64 Data Encodings, October 2006*

NIST SP 800-57, *Recommendation for Key Management: Part 1 – General*

NIST SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*

PKCS #1 v2.1:2023, *RSA Cryptography Standard*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms, definitions and abbreviated terms 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/

3.1.1
active
attribute setting for a *directed key* (3.1.9) that allows starting a cryptographic interaction

EXAMPLE MAC generate, cipher encrypt, PIN encryption, key encryption (key export).

3.1.2
advanced encryption standard
AES
16-byte block cipher

Note 1 to entry: This is defined in ISO/IEC 18033-3.

[SOURCE: ISO 11568:2023, 3.2]

3.1.3
ASCII
American Standard Code for Information Interchange
binary encoding of 7-bit characters defined by ISO/IEC 646

[SOURCE: ISO/IEC 18477-4:2017, 3.1.2, modified — The term "American Standard Code for Information Interchange", has been added as an admitted term.]

3.1.4
authentication value
cryptographically generated value *message authentication code* (3.1.29) derived from the key block header and confidential data that can be used to validate the integrity of the data contained in the key block

3.1.5
CBC
cipher block chaining
confidentiality mode whose encryption process features the combining (i.e. "chaining") of the plaintext blocks with the previous ciphertext blocks

[SOURCE: NIST SP 800-38A:2001]

3.1.6
cryptographic domain
set of one or more *secure cryptographic devices (SCDs)* (3.1.32) that contain or can use the same set of keys

Note 1 to entry: All *SCDs* (3.1.32) in the domain are considered to be "equivalent" in that a key that can be used in one *SCD* (3.1.32) in the domain is also available for use by any other *SCD* (3.1.32) in the domain.

Note 2 to entry: A cryptographic domain is often defined for host processing to provide load balancing of hardware security modules (HSMs).

Note 3 to entry: The keys are typically structured in a hierarchy where higher-level keys are used to provide protection for lower-level keys.

3.1.7
CTR
counter mode of encryption
confidentiality mode that features the application of the forward cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa

[SOURCE: NIST SP 800-38A:2001, modified — The admitted term “counter mode” has been changed to “counter mode of encryption”.]

3.1.8
DEA
data encryption algorithm
cryptographic algorithm, previously specified in FIPS 46 which became effective July 1977, now withdrawn.

[SOURCE: NIST SP 800-67 Rev. 2]

3.1.9
directed key
key K in a cryptographically bilateral protocol between two parties A and B for direction A to B, if and only if, there exist keys K_A, with key value of K and key attributes for *active* (3.1.1) on the cryptographic system of an entity A and K_B, with key value of K and the corresponding key attribute for *passive* (3.1.29) on the cryptographic system of an entity B

3.1.10
diversification data
derivation data for *key diversification* (3.1.20), containing information on the key attributes to be assigned to the derived key by the HSM

3.1.11
diversification scheme
cryptographic scheme implemented in an HSM that specifies how *diversification data* (3.1.10) is processed during *key diversification* (3.1.20), ensuring that different key attributes lead to cryptographically independent key values

3.1.12
diversification scheme for directed keys
diversification scheme (3.1.11) to obtain *directed keys* (3.1.9) for a cryptographically bilateral protocol between two parties identified as A and B, based on a common *key diversification key (KDK)* (3.1.21), which differs for the parties in the party identifier key attribute and on a tag in the *diversification data* (3.1.10), indicating the direction of the *directed key* (3.1.9) that determines whether the key derived from KDK party identifier type A has the *active* (3.1.1) role and the key derived from KDK party identifier type B has the *passive* (3.1.29) role or vice versa

3.1.13
hex-ASCII
number in base 16 expressed as *American Standard Code for Information Interchange* (*ASCII)* (3.1.3) characters

EXAMPLE The 32-bit *message authentication code* (3.1.28) result 0x12345678 (4 binary bytes) is encoded as eight hex-ASCII characters that reads “12345678” but is stored or transmitted as 0x3132333435363738.

3.1.14
initialization vector
IV
binary value used as a starting point for the encryption of a data sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment

3.1.15
key block
result of performing a cryptographic process over a key and its associated data to produce a key block header, ciphertext and *authentication value* (3.1.4) – the *message authentication code* (3.1.28)

[SOURCE: ANSI X9.143:2022, 3.15]

3.1.16
key block encryption key
KBEK
key that is derived from the *key block protection key* (3.1.18) and that is used solely for enciphering the *key block* (3.1.15)

[SOURCE: ANSI X9.143:2022, 3.16]

3.1.17
key block authentication key
KBAK
key that is derived from the *key block protection key* (3.1.18) and that is used solely for calculating the *message authentication code* (3.1.28) over the *key block* (3.1.15)

[SOURCE: ANSI X9.143:2022, 3.17]

3.1.18
key block protection key
KBPK
key wrapping key (KWK) (3.1.26) that is used as a derivation key from which the *key block encryption key* (3.1.16) and the *key block authentication key* (3.1.17) are derived

Note 1 to entry: This key is used for no other purpose.

[SOURCE: ANSI X9.143:2022, 3.18]

3.1.19
key derivation function
KDF
function to derive a key from a key generation key (KGK) using a *pseudorandom function* (3.1.31) with the KGK as seed and derivation or diversification data as input

3.1.20
key diversification
key derivation function (3.1.19) using *diversification data* (3.1.10) in a *diversification scheme* (3.1.11)

3.1.21
key diversification key
KDK
key used in a hardware security module (HSM) function implementing a diversification scheme for *key diversification* (3.1.20)

3.1.22
key encrypting key
KEK
key used exclusively to encrypt and decrypt other keys

[SOURCE: ANSI X9.143:2022, 3.19]

3.1.23
key export
secure cryptographic device (SCD) (3.1.32) operation that

a) unwraps a key and its attributes from a storage *key encrypting key* (3.1.22) or the *master file key (MFK)* (3.1.27) and re-encrypts that key under a *key wrapping key* (3.1.26) shared with another entity or internal system; or

b) wraps a clear key and its attributes that is stored within an *SCD* (3.1.32) using a *key wrapping key* (3.1.26) shared with another entity or internal system

[SOURCE: ANSI X9.143:2022, 3.20]

3.1.24
key import
secure cryptographic device (SCD) (3.1.32) operation that unwraps a key and its attributes using a *key wrapping key* (3.1.26) shared with another entity or system and then stores the key and its attributes from the key block within one or more related *SCDs* (3.1.32) or re-wraps the key and its attributes using a storage *key encrypting key* (3.1.22) or the *master file key (MFK)* (3.1.27)

[SOURCE: ANSI X9.143:2022, 3.21]

3.1.25
key type vector
KTV
set of attributes formatted according to the *diversification scheme* (3.1.11) used in the *diversification data* (3.1.10) for defining the attributes of a key derived from a *key diversification key (KDK)* (3.1.21)

3.1.26
key wrapping key
KWK
symmetric key that determines the *wrapping* (3.1.36) and *unwrapping* (3.1.35) functions of a symmetric key authenticated encryption mechanism that is intended for the protection of cryptographic keys and other specialized data

[SOURCE: ANSI X9.143:2022, 3.22]

3.1.27
master file key
MFK
key used to encrypt other keys for storage

Note 1 to entry: Storage can be internal to the *secure cryptographic device (SCD)* (3.1.32) housing the MFK or can pertain to external storage (e.g. on a host system).

[SOURCE: ANSI X9.143:2022, 3.24]

3.1.28
message authentication code
MAC
cryptographic value, which is the result of passing a financial message through the message authentication algorithm using a specific key

[SOURCE: ANSI X9.143:2022, 3.25]

3.1.29
passive
attribute setting for a directed key that allows only reacting on a cryptographic interaction

EXAMPLE MAC verify only, cipher decrypt, PIN verify, key decryption (key import)

3.1.30
PIN
personal identification number
numeric code used to authenticate an identity or to verify access authorization

[SOURCE: ISO/IEC 19790:2025, modified — added “or to verify access authorization” to the definition.]

3.1.31
pseudorandom function
PRF
function that can be used to generate output from a random seed and a data variable such that the output is computationally indistinguishable from truly random output

Note 1 to entry: The PRF is specified in the NIST SP 800–108r1-upd1.

3.1.32
secure cryptographic device
SCD
device that provides physically and logically protected cryptographic services and storage (e.g. *personal identification number (PIN)* (3.1.30) entry device or hardware security module (HSM)), and which can be integrated into a larger system, such as an automated teller machine (ATM) or point of sale terminal

[SOURCE: ISO 13491-1:2024, 3.18, modified — the example "(e.g. *PIN* entry device or HSM)" has been merged with the definition.]

3.1.33
subkey
cryptographic key that is used internally in a cryptographic algorithm, such as cipher-based message authentication code (CMAC), and not chosen by or exposed to the user of the algorithm

3.1.34
TDEA
triple data encryption algorithm
symmetric algorithm

Note 1 to entry: The TDEA is specified in the ISO/IEC 18033 series.

[SOURCE: ISO 11568:2023, 3.87, modified — the term "triple data encryption algorithm" has been changed to an admitted term, and the abbreviated term "TDEA" has been changed to the preferred term.]

3.1.35
unwrapping
function in a key wrap mechanism that either produces the key data from the ciphertext or indicates that either the ciphertext or the associated data is invalid

[SOURCE: ANSI X9.143:2022, 3.32]

3.1.36
wrapping
function in a key wrap mechanism that produces the ciphertext from and creates a validity check for the key and associated data

[SOURCE: ANSI X9.143:2022, 3.33]

3.2 Abbreviated terms

AAC	application authentication cryptogram
ARQC	authorization request cryptogram
BDK	base derivation key
CMAC	cipher-based message authentication code
DAC	data authentication code
DD	derivation data

DER	distinguished encoding rules
ECC	elliptic curve cryptography
ECDSA	elliptic curve digital signature algorithm
ECIES	elliptic curve integrated encryption scheme
EMV	Europay, Mastercard, Visa
GBIC	German banking industry committee
HMAC	keyed-hash message authentication code
HSM	hardware security module
ID	identifier
IKID	initial key identifier
KBH	key block header
KCV	key check value
KDH	key distribution host
KLD	key loading device
KRD	key receiving device
KEK	key encryption key
KMS	key management system
KSI	key set identifier
KWK	key wrapping key
MFK	master file key
PAN	personal account number
PED	PIN encryption device
PVK	PIN verification key
PVV	PIN verification value
SHA	secure hash algorithm
RD	random data
RSA	Rivest, Shamir and Adleman
TC	transaction certificate
TLS	transport layer security

4 Notation

The following are used to indicate field encoding in the key block:

a) nA: *n*-digits of alphabetic ("A" to "Z", "a" to "z"), e.g. 6A means exactly six alphabetic characters in ASCII;

b) nAN: alphanumeric ("A" to "Z", "a" to "z", "0" to "9"), e.g. 6AN means exactly six alphanumeric characters in ASCII;

c) nH: hex-ASCII ("0" to "9", "A" to "F"), e.g. 6H means exactly six hex-ASCII characters;

d) nN: numeric-ASCII ("0"-"9"), e.g. 6N means exactly six decimal characters in ASCII;

e) nB: binary bytes (0x00 to 0xFF), e.g. 6B means exactly six bytes of binary data;

f) nPA: *n* printable ASCII characters. Printable ASCII characters are those with hexadecimal values in the range 20 to 7E, inclusive. 6PA means exactly six printable ASCII characters;

g) ||: used for concatenation of bitstrings, 30A4F || 0C1 is equal to 30A4F0C1;

h) $\oplus$: xor. Bit-wise, xor is defined as $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ and $1 \oplus 1 = 0$. $\oplus$ applied to longer strings is performed bitwise, e.g. 0x3FC4 $\oplus$ 0xED27 = 0xD2E3;

i) < < : left-shift. If M is a bit string, then M < < 1 means M shifted one bit to the left, e.g. the bit string 0101010 < < 1 is 1010100 and 1010100 < < 1 is 0101000. The length of M < < 1 is the same as the length of M. Left-shift can also be described as multiplying by 2, without carry;

j) 0x: notation indicating a hexadecimal number follows, e.g. 0x31 indicates 31-hexadecimal (49-decimal).

5 Key block elements

The key block shall contain three parts:

a) the key block header (KBH), which contains non-sensitive attribute information about the key and the key block;

b) the confidential data that is being exchanged or stored (i.e. the key and attributes formatted according to the key data format);

c) the authentication value, which consists of a MAC that binds the key block header and confidential data.

This general format of a key block is illustrated in Figure 1.

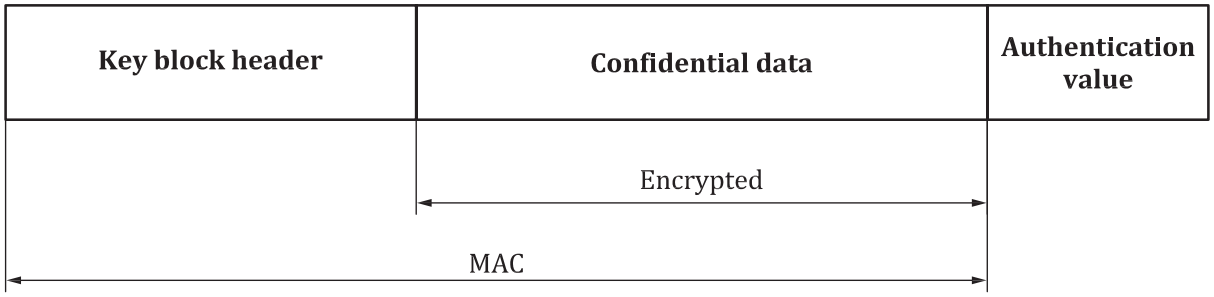

Figure 1 — Key block

For TDEA and AES keys, the confidential data should be padded to the maximum key length to hide its true length (key length obfuscation padding) from an external observer. When the confidential data are padded for key length obfuscation:

— TDEA keys less than 192 bits shall be padded to 192 bits.

— AES keys less than 256 bits shall be padded to 256 bits.

The key length obfuscation padding is determined by the size of the key being wrapped, but the block padding is determined by the algorithm being used to encrypt the confidential data. Because of the existence of the key length field in the information that is encrypted, additional padding is required to make the block consistent with the size of block the algorithm requires. For example, AES operates on 128 bits, so if the key is padded out to 256 bits, additional block padding characters are required because of the key length field.

For operational and compliance reasons (e.g. regulatory, contractual, industry and ecosystem standard), an entity may have SCD mechanisms to:

a) verify key length against the policies of an organization and the requirements of industry;

b) obtain key length information of stored keys.

Such SCD mechanisms should be managed with SCD administrative controls requiring dual-control execution.

6 Key block format

6.1 General

This clause defines a secure key block that uses the methods described in Clause 7.

Key blocks constructed according to this document shall conform to the relevant key wrapping requirements in ANSI X9.102.

The key block is a variable-length structure with a maximum length of 9999 bytes. The key block is composed of three sub-structures: a variable-length header, a variable-length confidential data field and an authentication value. The header may include optional fields.

The key block shall consist of three parts:

a) The KBH, which contains attribute information about the key and the key block and is not encrypted;

   1) The first section is 16 bytes with a fixed format defined in Table 1;

   2) The second section is of variable length and optional.

b) The confidential data, which will be encrypted;

   1) two bytes, indicating the key length (in bits) and excluding padding;

   2) the secret key and any confidential attributes;

   3) random padding to obfuscate the key length, if required;

   4) random cipher-block padding, if required.

c) The authentication value. The length of the authentication value shall be as follows:

   1) 128 bits, because the AES key derivation method is used (see 7.2.2).

TDEA and AES symmetric keys should be padded with random key length obfuscation padding to the maximum length for the algorithm, 192 bits for TDEA or 256 bits for AES. Other key types are not padded for key length obfuscation but are padded up to the cipher block of the wrapping method (e.g. HMAC, RSA and ECC keys). This format is illustrated in Figure 2.