

INTERNATIONAL STANDARD

**ISO
20038**

First edition
2017-11

Banking and related financial services — Key wrap using AES

Banque et autres services financiers — Enveloppe de clé utilisant AES





COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	3
5 Key wrap method characteristics	3
6 Key Block Binding key wrap method	3
6.1 General.....	3
6.2 Key block binding and encryption	4
6.3 Key derivation.....	5
6.4 Key Block Decryption and MAC Validation.....	7
Annex A (normative) Key Block with Optional Block	8
Annex B (informative) Numerical example	19
Bibliography	22

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

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

Introduction

The secure management of cryptographic keys requires that their values and usage constraints be protected for both confidentiality and integrity. This is especially true for keys used with the 64-bit block cipher triple data encryption algorithm (TDEA) and the 128-bit block cipher advanced encryption standard (AES) because these block ciphers allow the use of key sizes that are larger than the block size.

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 AES as the wrapping cipher.

Banking and related financial services — Key wrap using 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 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 11568-2, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO/IEC 9797-1, *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*

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

3 Terms and definitions

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

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

— ISO Online browsing platform: available at <http://www.iso.org/obp>

— IEC Electropedia: available at <http://www.electropedia.org/>

3.1

advanced encryption standard

AES

algorithm specified in ISO/IEC 18033-3

3.2

bit

binary digit

3.3

byte

sequence of 8 *bits* ([3.2](#))

3.4

ciphertext

encrypted (enciphered) data

3.5

cryptographic key

key

sequence of symbols that controls the operation of a cryptographic transformation (e.g. *encryption* (3.7), *decryption* (3.6), cryptographic check function computation, signature generation, or signature verification)

3.6

decryption

process of transforming *ciphertext* (3.4) into *plaintext* (3.13)

3.7

encryption

process of transforming *plaintext* (3.13) into *ciphertext* (3.4)

3.8

exclusive-OR

bit-by-bit modulo-2 addition of binary vectors of equal length

3.9

initialization vector

binary vector used as the input to initialize the algorithm for the *encryption* (3.7) of a plaintext block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment

Note 1 to entry: See ISO/IEC 10116.

3.10

key block

block containing a protected key, its usage constrains and other data, that is wrapped (encrypted) using a key wrapping mechanism

3.11

key wrap

symmetric *encryption* (3.7) algorithm designed to encapsulate (encrypt) cryptographic key material

3.12

nibble

half a *byte* (3.3), which can be represented by a single hexadecimal digit

3.13

plaintext

intelligible data that has meaning and can be read or acted upon without the application of *decryption* (3.6)

Note 1 to entry: Also known as cleartext. In the context of this document, the plaintext is the key being wrapped.

3.14

secure cryptographic device

SCD

device that provides secure storage for secret information, such as keys, and provides security services based on this secret information

3.15

triple data encryption algorithm

TDEA

algorithm specified in ISO/IEC 18033-3

4 Symbols and abbreviated terms

AES	advanced encryption standard
CBC	cipher block chaining (mode of encryption)
CMAC	cipher-based MAC
CTR	counter (mode of encryption)
IV	initialization vector for CBC mode or starting value for CTR mode
K	cryptographic key
MAC	message authentication code
TDEA	triple data encryption algorithm
SCD	secure cryptographic device
$\oplus$	exclusive-OR

5 Key wrap method characteristics

Key management according to ISO 11568-2 requires that symmetric keys be protected by physical protection, by splitting the key into components, or by cryptographic protection. Cryptographic protection can be achieved using an authenticated encryption algorithm such as one standardized in ISO/IEC 19772. However, most of the authenticated encryption algorithms in ISO/IEC 19772 are designed for protecting generic payloads such as long messages or large databases rather than symmetric keys that are short and have high entropy. A clear exception to this is mechanism 2 of ISO/IEC 19772:2009 which is called Key Wrap. As stated in ISO/IEC 19772, “This scheme was originally designed for authenticated-encryption of keys and associated information. This mode is known as AES Key Wrap when the AES block cipher is used”. It is also noted in ISO/IEC 19772 that AES Key Wrap is also specified in NIST, *AES Key Wrap Specification* and Reference [5].

The method defined in this document uses the MAC as IV (compared with Algorithm 5 in ISO/IEC 19772 which is an encrypt-then-MAC authenticated encryption algorithm) and as such it could theoretically support any symmetric encryption algorithm mode (e.g. taken from ISO/IEC 10116) or MAC algorithm (e.g. taken from ISO/IEC 9797-1). However, for the purposes of this document, the key wrap method supports only CBC or CTR mode encryption (as defined in ISO/IEC 10116) and CMAC (Method 5 in ISO/IEC 9797-1 and NIST/SP 800-38B) for MAC generation.

The key usage attributes from ANS/TR 31 shall be included in the wrapping process as defined in [Annex A](#). Other methods include but are not limited to authenticated encryption algorithms in ISO/IEC 19772, RFC 3394[5], ANSI CBC MAC[4] and TDEA Key Wrap[4].

6 Key Block Binding key wrap method

6.1 General

When a key is encrypted with a block cipher that has a block size less than the size of the key, this forces the key to be represented by several blocks resulting in a danger of substitution or misuse of a fragment of the overall key cryptogram. Binding the blocks of the encrypted key may be achieved through various methods.

The Key Block Binding method protects the secrecy of the key blocks and protects the integrity of the association between the key blocks and the key block header (see [Annex A](#) for a definition of a key block header). The method uses an AES Key Block Protection Key that was previously exchanged (using