

# DRAFT INTERNATIONAL STANDARD

## ISO/DIS 20038

ISO/TC 68/SC 2

Secretariat: BSI

Voting begins on:  
2023-05-26

Voting terminates on:  
2023-08-18

---

---

## Banking and related financial services — Key wrap using AES

*Banque et autres services financiers — Enveloppe de clé utilisant AES*

ICS: 35.240.40

ISO/DIS 20038 - Preview only Copy via ILNAS e-Shop

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number  
ISO/DIS 20038:2023(E)

© ISO 2023



## **COPYRIGHT PROTECTED DOCUMENT**

© ISO 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword.....	iv
Introduction.....	v
<b>1 Scope.....</b>	<b>1</b>
<b>2 Normative references.....</b>	<b>1</b>
<b>3 Terms and definitions.....</b>	<b>1</b>
<b>4 Notations and Symbols.....</b>	<b>5</b>
<b>5 Key Block Elements.....</b>	<b>6</b>
<b>6 Key Block Format.....</b>	<b>7</b>
6.1 Introduction.....	7
6.2 Key Block Header (KBH).....	8
6.2.1 General.....	8
6.2.2 Changing Key Headers.....	11
6.3 Defined values for Key Block Headers.....	12
6.3.1 Key Usage.....	12
6.3.2 Algorithm.....	17
6.3.3 Mode of Use.....	17
6.3.4 Key Version Number.....	19
6.3.5 Exportability.....	19
6.3.6 Optional Block ID.....	19
6.4 Encoding.....	42
6.4.1 General.....	42
6.4.2 RSA Key Pairs.....	43
6.4.3 Elliptic Curve Cryptography (ECC) Key Pairs.....	43
<b>7 Key Block Binding and Validation Methods.....</b>	<b>44</b>
7.1 General.....	44
7.2 Key Block Binding Method Using Key Derivation.....	45
7.2.1 General.....	45
7.2.2 Key Derivation Binding Method – AES.....	45
7.2.3 Key Derivation Binding Validation Method - AES.....	49
<b>8 Examples.....</b>	<b>50</b>
8.1 AES Key Block Example.....	50
8.1.1 Introduction.....	50
8.1.2 Constructing the Key Block Header.....	50
8.2 AES Key Block with Optional Blocks.....	56
8.2.1 Using AES Key Derivation Binding Method for CBC mode.....	56
8.3 RSA Key Block Example with CT Optional Block.....	59
8.3.1 General.....	59
8.3.2 Keys used in the example.....	59
8.3.3 Constructing the Key Block Header.....	61
8.3.4 Constructing the Binary Key Data.....	62
8.3.5 Constructing the complete Key Block.....	63
8.4 ECC Key Block Example with CT Certificate Chain Optional Block.....	65
8.4.1 General.....	65
8.4.2 Keys used in the example.....	65
8.4.3 Constructing the Key Block Header.....	66
8.4.4 Constructing the Binary Key Data.....	68
8.4.5 Constructing the complete Key Block.....	68
8.5 CTR mode without padding.....	69
<b>Annex A (Informative) Operational Challenges and Examples with Exportability.....</b>	<b>71</b>
<b>Bibliography.....</b>	<b>80</b>