ISO 20038:2017-11 (E)

Banking and related financial services - Key wrap using AES

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