

ISO 20038:2026-08 (E)

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

Contents	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	2
3.1 Terms and definitions	2
3.2 Abbreviated terms	6
4 Notation	8
5 Key block elements	8
6 Key block format	9
6.1 General	9
6.2 Key block header (KBH)	10
6.2.1 General	10
6.2.2 Changing key headers	13
6.3 Defined values for key block headers	14
6.3.1 Key usage	14
6.3.2 Algorithm	19
6.3.3 Mode of use	20
6.3.4 Key version number	21
6.3.5 Exportability	21
6.3.6 Optional block ID	22
6.4 Encoding	47
6.4.1 General	47
6.4.2 RSA key pairs	48
6.4.3 Elliptic curve cryptography (ECC) key pairs	49
7 Key block binding and validation methods	49
7.1 General	49
7.2 Key block binding method using key derivation	50
7.2.1 Key block binding and encryption	50
7.2.2 Key derivation	51
7.2.3 Key derivation binding validation method --AES	54
8 Examples	55
8.1 AES key block example	55
8.1.1 General	55
8.1.2 Constructing the key block header	55
8.2 AES key block with optional blocks	61
8.2.1 General	61
8.2.2 Keys used in the example	61
8.2.3 Constructing the key block header	62
8.3 RSA key block example with CT optional block	64
8.3.1 General	64
8.3.2 Keys used in the example	64

8.3.3	Constructing the key block header	65
8.3.4	Constructing the binary key data	67
8.3.5	Constructing the complete key block	68
8.4	ECC key block example with CT certificate chain optional block	70
8.4.1	General	70
8.4.2	Keys used in the example	70
8.4.3	Constructing the key block header	71
8.4.4	Constructing the binary key data	73
8.4.5	Constructing the complete key block	74
8.5	CTR mode without padding	75
Annex A (informative) GBIC scheme for directed key diversification		76
Annex B (informative) Operational challenges and examples with exportability		83
Bibliography		92