

ISO/TS 14742:2025-11 (E)

Financial services - Recommendations and requirements on cryptographic algorithms and their use

Contents		Page
Foreword		v
Introduction		vi
1 Scope		1
2 Normative references		1
3 Terms and definitions		2
4 Algorithm strength and key cryptoperiod		2
4.1 Measuring bits of security.....		2
4.2 Cryptographic algorithm migration.....		3
4.3 Key cryptoperiod.....		5
5 Block ciphers		5
5.1 General.....		5
5.2 Keying options.....		6
5.2.1 Keying options for TDEA.....		6
5.2.2 Keying options for AES.....		6
5.2.3 Keying options for Camellia.....		6
5.2.4 Keying options for SM4.....		6
5.3 Recommended block ciphers.....		6
5.4 Cipher block size and key use.....		7
5.5 Modes of operation.....		8
5.6 Enciphering small plaintexts.....		8
5.7 Migrating from TDEA to AES.....		8
6 Stream ciphers		8
7 Message authentication codes (MACs)		9
7.1 Recommended MAC algorithms.....		9
7.2 MAC algorithms based on block ciphers.....		9
7.3 MAC algorithms based on hash functions.....		9
7.4 Length of the MAC.....		10
7.5 Message span of the key.....		10
8 Authenticated encryption		10
8.1 Recommended authenticated encryption methods.....		10
8.2 Key wrap.....		11
8.3 CCM.....		12
8.4 EAX.....		12
8.5 Encrypt-then-MAC.....		12
8.6 Galois Counter Mode.....		12
9 Format preserving encryption		12
10 Hash functions		13
10.1 Hash functions and their properties.....		13
10.2 Hash functions based on block ciphers.....		13
10.3 Dedicated hash functions.....		13
10.4 Hash functions using modular arithmetic.....		14
10.5 Migrating from one hash function to another.....		14
11 Asymmetric algorithms		15
11.1 General.....		15
11.2 Factorization-based security mechanisms.....		18

11.3	Integer discrete logarithm-based security mechanisms.....	19
11.4	Elliptic curve discrete logarithm-based security mechanisms.....	19
11.5	Algorithm or key expiry.....	20
11.6	Digital signature schemes giving message recovery.....	20
11.7	Digital signatures with appendix.....	20
11.8	Post-quantum algorithms.....	21
11.9	Blind digital signatures.....	21
11.10	Asymmetric ciphers.....	21
	11.10.1 Overview.....	21
	11.10.2 Hybrid ciphers.....	22
	11.10.3 RSAES.....	23
	11.10.4 HIME(R).....	23
12	Random number generation.....	24
Annex A (informative) Entity authentication and key management mechanisms.....		25
Bibliography.....		32