# ISO/TR 14742:2010-07 (E)

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

## Contents

Page


Foreword ..... iv

Introduction ..... v

1 Scope ..... 1

2 Measuring bits of security ..... 2

3 Algorithm migration ..... 3

4 Block ciphers ..... 4
4.1 General ..... 4
4.2 Keying options ..... 4
4.3 Recommended block ciphers ..... 5
4.4 Block size and key use ..... 6
4.5 Modes of operation ..... 6
4.6 Enciphering small plaintexts ..... 7
4.7 Migrating from TDEA to AES ..... 7

5 Stream ciphers ..... 7

6 Hash functions ..... 7
6.1 Hash functions and their properties ..... 7
6.2 Hash functions based on block ciphers ..... 8
6.3 Dedicated hash functions ..... 8
6.4 Hash functions using modular arithmetic ..... 10
6.5 Migrating from one hash function to another ..... 10

7 Message authentication codes ..... 11
7.1 Recommended MAC algorithms ..... 11
7.2 MAC algorithms based on block ciphers ..... 11
7.3 MAC algorithms based on hash functions ..... 11
7.4 Length of the MAC ..... 12
7.5 Message span of the key ..... 12

8 Asymmetric algorithms ..... 12
8.1 General ..... 12
8.2 Factorization-based security mechanisms ..... 14
8.3 Integer discrete logarithm-based security mechanisms ..... 14
8.4 Elliptic curve discrete logarithm-based security mechanisms ..... 15
8.5 Algorithm or key expiry ..... 15
8.6 Digital signature schemes giving message recovery ..... 15
8.7 Digital signatures with appendix ..... 16
8.8 Asymmetric ciphers ..... 16

9 Random number generation ..... 18

Annex A (informative) Entity authentication and key management mechanisms ..... 19

Bibliography ..... 28