

# ISO/TS 14742:2025-11 (E)

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

---

| <b>Contents</b>  |  | <b>Page</b> |
|--|--|-------------|
| <b>Foreword</b> .....                                  |  | <b>v</b>    |
| <b>Introduction</b> .....                              |  | <b>vi</b>   |
| <b>1 Scope</b> .....                                   |  | <b>1</b>    |
| <b>2 Normative references</b> .....                    |  | <b>1</b>    |
| <b>3 Terms and definitions</b> .....                   |  | <b>2</b>    |
| <b>4 Algorithm strength and key cryptoperiod</b> ..... |  | <b>2</b>    |
| 4.1 Measuring bits of security.....                    |  | 2           |
| 4.2 Cryptographic algorithm migration.....             |  | 3           |
| 4.3 Key cryptoperiod.....                              |  | 5           |
| <b>5 Block ciphers</b> .....                           |  | <b>5</b>    |
| 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           |
| <b>6 Stream ciphers</b> .....                          |  | <b>8</b>    |
| <b>7 Message authentication codes (MACs)</b> .....     |  | <b>9</b>    |
| 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          |
| <b>8 Authenticated encryption</b> .....                |  | <b>10</b>   |
| 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          |
| <b>9 Format preserving encryption</b> .....            |  | <b>12</b>   |
| <b>10 Hash functions</b> .....                         |  | <b>13</b>   |
| 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          |
| <b>11 Asymmetric algorithms</b> .....                  |  | <b>15</b>   |
| 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        |
| <b>12</b> | <b>Random number generation.....</b>  | <b>24</b> |
|           | <b>Annex A (informative) Entity authentication and key management mechanisms.....</b> | <b>25</b> |
|           | <b>Bibliography.....</b>  | <b>32</b> |