



BSI Standards Publication

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

National foreword

This Published Document is the UK implementation of ISO/TS 14742:2025. It supersedes PD ISO/TR 14742:2010, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 22993 6

ICS 03.060; 35.240.40

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2025.

Amendments/corrigenda issued since publication

Date	Text affected



Technical Specification

ISO/TS 14742

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

*Services financiers — Recommandations et exigences relatives
aux algorithmes cryptographiques et leur utilisation*

**First edition
2025-11**



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

This first edition of ISO/TS 14742 cancels and replaces ISO/TR 14742:2010, which has been technically revised.

The main changes are as follows:

- the status of the document has changed from Technical Report (TR) to Technical Specification (TS);
- guidance has been updated in many areas;
- key wrap coverage has been enhanced;
- post quantum cryptographic algorithms have been considered.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The financial services industry has a clear need for cryptographic algorithms for a number of different applications. ISO standards (such as the ISO 18033 series) provide definitions for an extensive and comprehensive set of such algorithms. However, as the state of the art of cryptology progresses and the power of computers increases, cryptographic algorithms as well as cryptographic keys of a particular length all have a limited window of time in which they can be considered secure. Furthermore, as neither the development of cryptology nor the increase in computing power are entirely predictable, the collective wisdom of the cryptographic community as to which algorithms and key lengths are secure is constantly evolving. For this reason, there is an equally clear need in the financial services industry for guidance regarding the current and up-to-date view in the cryptographic community about the security of cryptographic algorithms and their keys. There is also a need for appropriate guidance on migration from one algorithm or key length to another.

Algorithmic vulnerabilities or cryptographic keys of inadequate lengths are less often the cause of security compromises in the financial industry than are inadequate key management or other procedural flaws, or mistakes in the implementation of cryptographic algorithms or the protocols that use them. However, compromises arising from algorithmic vulnerabilities are more systemic and harder to recover from than other kinds of compromises.

The strength requirements of a security mechanism can vary depending on the application(s) in which the mechanism is being used and the way it is being used. The recommendations given in this document are considered to be general purpose recommendations. Although it is accepted that low-risk applications exist that do not warrant the level of cryptographic strength recommended in this document, deviation from the recommendations should only be made after appropriate analysis of the risks and in the context of any rules and policies that can apply.

A special case relates to the lifetime of protection required by the application and its data. For example, if protection requirements are ephemeral (e.g. confidentiality is required only for one day or authentication is one-time), then it is possible that this is cause for allowing a deviation from the recommendations. Conversely, if the data must remain protected for a very long period of time, then the keys and algorithms used to provide the protection are required to be kept secure for that duration also, even if the keys are no longer in active use.

This document is not intended to cover privacy issues related to secondary usages of payment data such as location, kinds of merchant, services or goods purchase.

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

1 Scope

This document provides a list of recommended ISO cryptographic algorithms for use within applicable ISO TC 68, *Financial services*, standards. It also provides strategic guidance on key lengths and associated parameters and usage dates.

This document focuses on core algorithms, key lengths and frequently used mechanisms. The included algorithms are considered to be fit for purpose for financial service use. For additional algorithms, see the body of standards produced by ISO/IEC JTC 1 SC 27, *Information security, cybersecurity and privacy protection*. For standards on key management, see ISO 11568.

The categories of algorithms covered are:

- a) block ciphers and modes of operation;
- b) stream ciphers;
- c) message authentication codes (MACs);
- d) authenticated encryption algorithms;
- e) format preserving encryption;
- f) hash functions;
- g) asymmetric algorithms:
 - 1) digital signature schemes giving message recovery;
 - 2) digital signatures with appendix;
 - 3) asymmetric ciphers.
- h) authentication mechanisms;
- i) key derivation, establishment and agreement mechanisms;
- j) key transport mechanisms:
 - 1) key wrapping.

This document does not define any cryptographic algorithms. However, the standards to which this document refers contain necessary implementation information as well as more detailed guidance regarding choice of security parameters, security analysis and other implementation considerations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9796-2:1997¹⁾, *Information technology — Security techniques – Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO/IEC 18033-3:2010, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

3 Terms and definitions

No terms and definitions are listed in this document.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

4 Algorithm strength and key cryptoperiod

4.1 Measuring bits of security

For both block ciphers (Clause 5) and hash algorithms (Clause 10), the notion of " n bits of security" is introduced (see NIST SP 800-57 Part 1:2020, Clause 5.6.1). For a block cipher to have n bits of security, an estimated 2^n operations are necessary to break the block cipher. Given a few plaintext blocks and corresponding ciphertext, a block cipher with n bits of security requires an average of $2^{n-1}T$ of time to recover the encryption key, where T is the amount of time it takes to perform one encryption of a plaintext value and a comparison of the result against the corresponding ciphertext value. For a hash algorithm to have n bits of security with respect to collision resistance, an estimated 2^n calls to the hash function are necessary to find a hash collision, i.e. two messages that when hashed yield the same hash result.

Table 1 — Status of bits of security for symmetric algorithms

Algorithm	Attacks	Maximum bits of security
2-key Triple Data Encryption Algorithm (TDEA)	Known plain/ciphertext pairs $2^8/2^{40}/2^{56}$	112/80/64
3-key TDEA	Meet in the middle	112
Advanced Encryption Standard (AES)-128	No practical attack known	128
AES-192	No practical attack known	192
AES-256	No practical attack known	256

Algorithms with 112 bits of security are allowed for legacy use, but new implementations should use keys with at least 128 bits of security and the corresponding 16-byte block ciphers.

Refer to NIST SP 800-57 part 1 for analysis of the likelihood that an algorithm of a given bit strength remains secure (that is, unbroken) until at least the year indicated.

See also section 2 of NIST SP 800-131A REV. 2.^[98]

See also 2016 NIST PQC Competition call for proposals for an overview of algorithmic strength.^[102]

It is important to understand the context in which the identified weaknesses are relevant. If a single key is to be used to encrypt large volumes of data (of the order of 2^{40} bytes), Triple Data Encryption Algorithm (TDEA) is a poor choice. However, in EMV 4.4 Book 2^[103], session keys are specified to form a single cryptogram for the purposes of a one-off real-time authorization. It can be argued that the weaknesses therefore do not apply for this use case and there is no immediate danger driving a migration to AES and that the industry should migrate as the opportunity arises.

1) Cancelled and replaced by ISO/IEC 9796-2:2010.

The efforts of breaking ciphers of different categories can have very different requirements. One algorithm can require a large amount of computing power and little storage, while another can use a large amount of storage and less computing power. One effort can be parallelizable, so that the main limitation is the number of computers that can be recruited to participate. Another can require a single computer with a very large amount of RAM. Lenstra and Verheul (see Reference [24]) estimated in 1999 that the financial costs associated with breaking an asymmetric cipher are 2 500 times larger than those associated with breaking a symmetric cipher, if the computational efforts measured in microprocessor without interlocked pipelined stages (MIPS) years are the same. See also Reference [18] for comparisons of cryptographic strengths of symmetric and asymmetric algorithms.

As pertains to the threat due to quantum computers, according to Grover's algorithm (Reference [15]), when a cryptanalytically relevant quantum computer (CRQC) is built, the number of queries to break a symmetric cipher with key size n drops from 2^n trial encryptions to $2^{n/2}$ evaluations of the encryption function in superposition and as many Grover steps.

Further analysis of the small print of Grover's algorithm reveals that pre-quantum security can be maintained with less effort than doubling key lengths (Reference [14]):

- a) Grover's algorithm does not benefit from linear speed-up through parallelisation. To obtain a thousand-fold speed-up when using Grover's algorithm, a million quantum computers are necessary.
- b) The quantum attack work function on AES-128 is estimated to be 2^{101} where 2^{64} operations are performed on a single quantum machine.

This indicates AES-128 can remain fit for purpose in many contexts.

All the conventional asymmetric algorithms mentioned in this document are vulnerable to quantum computing algorithms (see Reference [35]), and hence any leaps in progress in the area of implementing quantum computers can void the recommendations in Table 7. However, the commonly established wisdom is currently that quantum computing on the scale necessary, say, to factor a 1 024-bit Rivest, Shamir Adelman (RSA) modulus, is likely years away. The largest publicly known quantum computers in 2023 were at the scale of 1 000 qubits. However, in order to implement Shor's algorithm [attacking RSA and elliptic curve cryptography (ECC)] or Grover's algorithm (attacking symmetric keys), a quantum computer requires millions of qubits able to sustain the necessary level of qubit coherence and fault-tolerance throughout the attack.

For discussion of cryptographic strength and preparation of systems for the threat of CRQCs, see References [44], [45] and [46].

On the other hand, when large scale quantum computers are realized, it is expected that increases in key lengths are much less a barrier to compromise than now, so that the mentioned asymmetric algorithms quickly become obsolete.

4.2 Cryptographic algorithm migration

As the state of the art of cryptology progresses and the power of computers increases, cryptographic algorithms and key lengths that once were secure can no longer be so. For algorithms that have variable security parameters, security can be improved by adjusting the security parameters rather than migrating to a new algorithm. Examples include RSA-based crypto systems, where the RSA key length can be increased, and AES, where the choice is between key lengths of 128, 192 and 256 bits.

Migration where only the security parameters are changed are simpler than migration where the cryptographic algorithm itself changes. Although performance in general is expected to decrease with a more secure choice of security parameters, improvements in computer performance can make up for such a deterioration.

However, specific applications, implementations, data formats or indeed performance considerations can impose limits on the values of certain security parameters such that at some point it becomes impossible, infeasible or uneconomical to maintain adequate security by only adjusting the security parameters.

It can further be assumed that no cryptographic algorithm can continue to provide adequate and cost-efficient security forever, regardless of the choice of security parameters. Hence it can be assumed that,

although increasing the security parameters for an existing algorithm can buy some time, eventually any application of a cryptographic algorithm can face a migration from that algorithm to a newer one.

Any such migration is likely to incur both cost and disruption, but it is also an opportunity to take advantage of cryptographic and technical progress in modernizing the use of cryptographic algorithms, to what is expected to be a faster, more secure and more cost-effective solution.

Experience gained in migrating from single DES to TDEA has highlighted that the financial industry must establish a long-term and holistic (as opposed to piecemeal) approach to cryptographic algorithms. These algorithms are fundamental to all data security systems, which means changes to them are difficult, sensitive and expensive and take a long time to implement.

Attacks on Triple DES have led to pressure to deprecate its use and replace it with AES. However, it is important to understand the context in which the identified weaknesses are relevant. Similarly, it is problematic for multi-target attacks to have short keys when there is a fixed plaintext and the key is used for confidentiality. The general principle is that the choice of cryptographic algorithm depends greatly on the strength of the algorithm as deployed in a specific use case, for which the minimum agreed level currently in industry is 128 bits of effective strength for new deployments.

Thus, apart from identifying and preparing the financial industry for migration to other cryptographic algorithms and longer key lengths with associated changes in key management, it is also necessary to ensure that:

- the structure of stored and transmitted data is suitable to be processed by generic cryptographic algorithms;
- systems are designed to be sufficiently flexible to enable the configuration of cryptographic algorithms and associated parameters from a lower strength to a higher strength or from a compromised algorithm or mechanism to one that is not compromised.

For this reason, in order to create systems that are sufficiently flexible to withstand algorithm migration in the future, it is important to first start migrating to more flexible data structures and methods for processing such data structures. For example, ISO 8372 was withdrawn and replaced with ISO/IEC 10116. Also, see ISO 16609.

Because of the complexity of the task and the lifetime of relevant system components, a migration time of 10 to 15 years can well be realistic. Example steps that should be completed are:

- a) decision to update a cryptographic algorithm or mechanism;
- b) inventory of systems and applications to determine what should change;
- c) agreement on algorithms and protocols;
- d) development of flexible data structures and APIs;
- e) development of plans to ensure interoperability through migration phase;
- f) product development and test;
- g) product implementation;
- h) phased migration, including stopping the use of old algorithms;
- i) protected data lifetime. This is the period after any new use of the old algorithms has ceased, but while data must remain protected by the old algorithms.

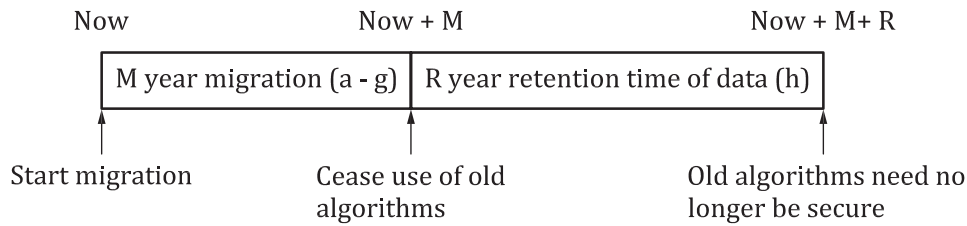


Figure 1 — Example of migration from old to new algorithms

Where necessary, this document specifies particular migration issues for the algorithms discussed.

4.3 Key cryptoperiod

The effective strength of a key for a given cryptographic algorithm is influenced by the management of the key during its lifecycle, which includes consideration of the cryptoperiod or usable life of the key.

Cryptoperiod is the length of time that an individual key can safely be reused. Properly defining a cryptoperiod is based on the:

- strength of the key;
- importance and amount of data protected by the key:
 - restricting the ability to subject a key to crypto analysis;
 - limiting the value of a key to a potential attacker.
- risk of compromise for the key.

The cryptoperiod of symmetric key-wrapping keys depends on their intended usage. NIST SP 800-57 part 1 recommends that the originator's duration of a symmetric key-wrapping key used to wrap a very large number of keys over a short period of time is one week. If a key-wrapping key protects only a small number of keys, the period can be up to two years. If a key-wrapping key is used for a single message or communications session, the cryptoperiod is limited to that session. The recipient's usage period should be no longer than three years more than the originator's usage period.

The risk of compromise includes factors such as how the key is stored, secure hardware storage verses software usage or insecure hardware, and others. See section 5.3 of NIST SP 800-57 part 1, revision 5 (May 2020).

5 Block ciphers

5.1 General

This clause lists block ciphers that can be used within applicable TC 68, *Financial services*, standards.

A block cipher maps a block of n plaintext bits to a block of n ciphertext bits using a key of k bits. The block ciphers listed in [Table 2](#) are defined in ISO/IEC 18033-3.

Table 2 — Block ciphers

Block length	Algorithm name	Key length
64 bits	TDEA	128 or 192 bits
128 bits	AES	128, 192 or 256 bits
	Camellia	
	SM4	128 bits

5.2 Keying options

5.2.1 Keying options for TDEA

Keying option 2, also known as 2-key Triple DES: 128-bit key represented as two 64-bit DEA keys, where one bit in each key byte is not used by the DEA and can be used for error detection.

Keying option 1, also known as 3-key Triple DES: 192-bit key represented as three 64-bit DEA keys, where one bit in each key byte is not used by the DEA and can be used for error detection.

5.2.2 Keying options for AES

Keying option 1: 128-bit.

Keying option 2: 192-bit.

Keying option 3: 256-bit.

5.2.3 Keying options for Camellia

Keying option 1: 128-bit.

Keying option 2: 192-bit.

Keying option 3: 256-bit.

5.2.4 Keying options for SM4

Keying option 1: 128-bit.

Keying option 2: 256-bit.

5.3 Recommended block ciphers

[Table 3](#) contains a list of recommended block ciphers and their current estimated security in bits. The recommendations are based on the analyses and recommendations provided in the ECRYPT yearly report on algorithms and key sizes (see Reference [\[12\]](#)) and NIST SP 800-57, Part 1.

The currently prevalent block cipher algorithm in the payment industry is TDEA, which is increasingly considered unsafe and should not be used in new implementations, although it remains permissible in legacy systems.

Table 3 — Security of block ciphers

Algorithm	Keying option	Key length	Security in bits
TDEA ^a	2	128 bits	80–112
	1	192 bits	112
AES	1	128 bits	128
	2	192 bits	192
	3	256 bits	256
SM4	1	128 bits	128
	2	256 bits	256
^a TDEA is deprecated.			

General considerations:

- Implementations of block cipher algorithms should be evaluated for susceptibility to side channel attacks, especially where shielding and counter-measures are not possible.