TECHNICAL REPORT

ISO/TR 14742

First edition
2010-07-01

Financial services — Recommendations on cryptographic algorithms and their use

Services financiers — Recommandations sur les algorithmes cryptographiques et leur utilisation

Reference number
ISO/TR 14742:2010(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 14742 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

Introduction

The financial services industry has a clear need for cryptographic algorithms for a number of different applications. ISO standards 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 it was felt that there was 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. It was also felt that there was a need for appropriate guidance on migration from one algorithm or key length to another.

The ISO standards that define cryptographic algorithms for the financial services industry do not contain such guidance, and by the evolving nature of the field, it would be difficult for them to do so. Hence, the need was recognized for a document that could contain such guidance, and be updated more frequently than the five year review cycle for ISO standards. This Technical Report is intended to be that document. The intention is to update this Technical Report when the need arises, or at least every other year.

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 Technical Report are considered to be general purpose recommendations. Although it is accepted that there may exist low-risk applications that do not warrant the level of cryptographic strength recommended in this Technical Report, it is advisable that deviation from the recommendations only be made after appropriate analysis of the risks and in the context of any rules and policies that might apply.

A special case of the above 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 this may be 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 must be good for that duration, even if the keys are no longer in active use.

Financial services — Recommendations on cryptographic algorithms and their use

1 Scope

This Technical Report provides a list of recommended cryptographic algorithms for use within applicable financial services standards prepared by ISO/TC 68. It also provides strategic guidance on key lengths and associated parameters and usage dates.

The focus is on algorithms rather than protocols, and protocols are in general not included in this Technical Report. However, in some cases, for example for some key agreement and some authentication protocols, there is no “underlying” algorithm, and in a sense it is the protocol that constitutes the algorithm. In this case, the mechanisms are included, in particular where they have security parameters that can be adjusted for higher or lower security.

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 caused by algorithmic vulnerabilities are more systemic and harder to recover from than other kinds of compromises.

This Technical Report deals primarily with recommendations regarding algorithms and key lengths.

NOTE Key management is covered in ISO 11568-1, ISO 11568-2 and ISO 11568-4.

The categories of algorithms covered in this Technical Report are:

- block ciphers;
- stream ciphers;
- hash functions;
- message authentication codes (MACs);
- asymmetric algorithms:
  - digital signature schemes giving message recovery,
  - digital signatures with appendix,
  - asymmetric ciphers;
- authentication mechanisms;
- key establishment and agreement mechanisms;
- key transport mechanisms.

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

2 Measuring bits of security

For both block ciphers (Clause 4) and hash algorithms (Clause 6) the notion of “n bits of security” is introduced (e.g. see NIST SP 800-57, 2007, 5.6.1). For a block cipher to have n bits of security means that an estimated 2^n operations are needed to break the block cipher. Given a few plaintext blocks and corresponding ciphertext, a block cipher with n bits of security would then require an average of $2^{n-1}T$ of time to recover the encryption key, where T is the amount of time needed 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 means that an estimated 2^n calls to the hash function are necessary to find a hash collision, that is, two messages that when hashed yield the same hash result.

Table 1 below reflects recommendations for when an algorithm with n bits of security can be used. The dates coincide, where applicable, with the recommendations in NIST SP 800-57.

Table 1 — Recommended usage periods for algorithms of varying bit-strength

Bits of security	Recommended usage period
80	until end 2010
96	until end 2020
112	until end 2030
$\geqslant$ 128	as from 2030

The recommendations from Table 1 reflect that it is estimated that there is an overwhelming likelihood that an algorithm of the indicated bit strength will remain secure (that is, unbroken) until at least the year indicated.

For other categories of algorithms, such as message authentication codes and asymmetric algorithms, the concept of n bits of security is more difficult to define because of the nature of compromises and the measurement of the work or cost required to accomplish a compromise. However, for each category of algorithm, their security is still expressed in terms of bits of security. The intended interpretation is that if an algorithm is listed as having n bits of security, then it is estimated that it will remain secure until the same year as a symmetric cipher with n bits of security.

The efforts of breaking ciphers of different categories may have very different “profiles”. One algorithm may require a large amount of computing power and little storage, while another may use a large amount of storage and less computing power. One effort may be parallelizable, so that the main limitation is the number of computers that can be recruited to participate, whereas another may require a single computer with a very large amount of RAM. Lenstra and Verheul in Reference [52] estimate 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 MIPS years are the same. See also Reference [19] for comparisons of cryptographic strengths of symmetric and asymmetric algorithms.

For algorithms with an estimated security of 128 bits or more, a recommendation of “past 2030” is given, reflecting the view that any estimate beyond 2030 is so far into the future that it seems unwise to make the estimate any more precise at this time.

For symmetric algorithms, Grover's algorithm (see Reference [17]) means that if a quantum computer were to be implemented, key sizes should be roughly doubled to maintain the same level of security. All the asymmetric algorithms mentioned in this Technical Report are vulnerable to quantum computing algorithms (see Reference [69]), and hence any leaps in progress in the area of implementing quantum computers could render the recommendations in Table 1 void. However, the commonly established wisdom is currently that quantum computing on the scale necessary, say to factor a 1 024-bit RSA modulus, is at least 20 to 25 years away. On the other hand, if and when quantum computers are realized, it would be expected that increases in key lengths would be much less a barrier to compromise than now, so that the mentioned asymmetric algorithms would quickly become obsolete.

3 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 may no longer be so. For algorithms that have 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 is mostly less onerous than migration where the cryptographic algorithm itself changes, and although performance in general would be expected to deteriorate with a more secure choice of security parameters, improvements in computer performance may make up for such a deterioration.

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

It must further be assumed that no cryptographic algorithm will continue forever to provide adequate and cost-efficient security, regardless of the choice of security parameters. Hence it must be assumed that although increasing the security parameters for an existing algorithm may buy some time, eventually any application of a cryptographic algorithm will face a migration from that algorithm to a newer one.

Any such migration will be 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 should be a faster, more secure and more cost-effective solution.

Experience gained in migrating from DES to TDEA has highlighted that the financial industry must establish a long-term and holistic (as opposed to piecemeal) approach to cryptographic algorithms. Lying as they do at the heart of all data security systems, changes to such algorithms are difficult, sensitive and expensive, and they take a long time to implement.

Thus, apart from identifying and preparing the financial industry for migration to other algorithms and longer key lengths with associated changes in key management, there is also a need to ensure that

- the structure of stored and transmitted data is suitable to be processed by generic cryptographic algorithms, and

- systems are designed to be sufficiently flexible to enable the negotiation of cryptographic algorithms and associated parameters.

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. A good example of this is the adoption by ISO/TC 68 (e.g. see ISO 16609) of ISO/IEC 10116 in place of ISO 8372.

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

a) development of flexible data structures;

b) agreement on algorithms and APIs;

c) development of plans to ensure interoperability through migration phase;

d) product development and test;

e) product implementation;

f) phased migration, including stopping the use of old algorithms;

g) protected data lifetime: this is the period after any new use of the old algorithms has ceased, but while data must still remain protected by the old algorithms.

See Figure 1.

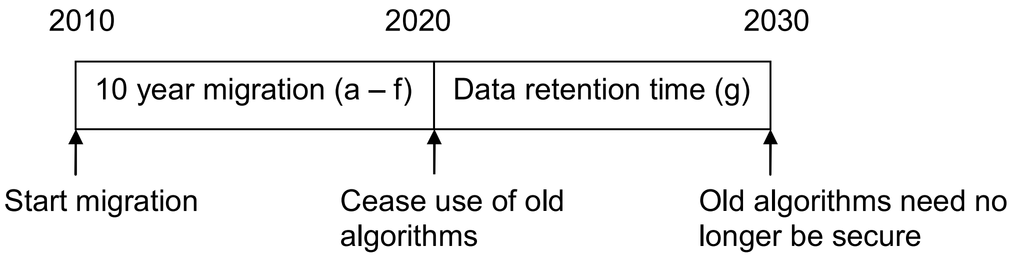
2010
2020
2030
10 year migration (a – f)
Data retention time (g)
Start migration
Cease use of old algorithms
Old algorithms need no longer be secure

Figure 1 — Example of migration from old to new algorithms

The individual clauses below will highlight any particular migration issues there may be for the algorithms they discuss.

4 Block ciphers

4.1 General

This clause lists block ciphers that may be used within applicable ISO/TC 68 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 below are defined in ISO/IEC 18033-3.

Table 2 — Block ciphers

Block length	Algorithm name	Key length
64 bits	TDEA	128 or 192 bits
	MISTY1	128 bits
	CAST-128	
128 bits	AES	128, 192 or 256 bits
	Camellia	
	SEED	128 bits

4.2 Keying options

4.2.1 Keying options for TDEA

Keying option 1, also known as 2-key Triple DES: 128-bit key represented as two 64-bit DEA keys, where for each DEA key 56 bits can be chosen arbitrarily and the rest can be used for error detection.

Keying option 2, also known as 3-key Triple DES: 192-bit key represented as three 64-bit DEA keys, where for each DEA key 56 bits can be chosen arbitrarily and the rest can be used for error detection.

4.2.2 Keying options for AES

Keying option 1: 128-bit, where all 128 bits can be chosen arbitrarily.

Keying option 2: 192-bit, where all 192 bits can be chosen arbitrarily.

Keying option 3: 256-bit, where all 256 bits can be chosen arbitrarily.

4.2.3 Keying options for Camellia

Keying option 1: 128-bit, where all 128 bits can be chosen arbitrarily.

Keying option 2: 192-bit, where all 192 bits can be chosen arbitrarily.

Keying option 3: 256-bit, where all 256 bits can be chosen arbitrarily.

4.3 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 References [13] and NIST SP 800-57).

Table 3 — Security of block ciphers

Algorithm	Keying option	Key length	Security in bits
TDEA	1	128 bits	80 – 112
	2	192 bits	112
AES	1	128 bits	128
	2	192 bits	192
	3	256 bits	256

Note that:

— 2-key Triple DES (TDEA with keying option 1) has effective strength $2^{\min (112,\ 120-t)}$ where 2^t is the number of plaintext ciphertext pairs available to an attacker.

— 3-key Triple DES (TDEA with keying option 2) has effective strength exceeding 2^{100}. Typically, its strength is cited as 2^{112}, but in general its strength is best expressed as in Reference [55], Note 7.38, as a trade-off between memory and computation, where a “meet-in-the-middle” attack requires 2^{57-s} space and 2^{112+s} time, for $1 \leqslant s \leqslant 56$.

The recommended end date for use of 2-key Triple DES (TDEA with keying option 1) ranges from 2010 to 2030. Which date is appropriate for a given implementation depends on the way in which the keys are being used in that implementation. If the key usage provides a potential attacker with a large number of plaintext-ciphertext pairs for the same key (e.g. 1 000 000 000 000 ≈ 2^{40} pairs), the security of the key is approximately 80 bits and hence the recommended use is until 2010. If only a few (fewer than 256) pairs are available, it may be acceptable to continue use until 2030.

Interpolating, by way of example, if an estimated maximum of 16 million plaintext-ciphertext pairs might become available to an attacker, the estimated security of the key would be approximately 96 bits (since 2^{24} ≈ 16 million), and the recommended use would be until 2020. Hence, proper use of session keys will greatly extend the usable life of a 2-key Triple DES (TDEA with keying option 1) implementation, as will frequent change of keys. If it is not possible to estimate a limit on the number of plaintext-ciphertext pairs that may become available to an attacker, then the most conservative recommendation (to stop use by 2010) applies.

Notice also that in the absence of session keys, 64-bit MACs may provide an attacker with plaintext-ciphertext pairs (in particular for messages less than 8 bytes) and thus aid in reducing the security of the key used.

For example, consider PIN entry devices that use a fixed key versus those that use unique keys per transaction, such as DUKPT (Derived Unique Key Per Transaction, as specified in ANSI X9.24-1). Fixed-key devices could provide an attacker with a large number of plaintext-ciphertext pairs (one pair for each encryption), weakening the strength of the key, whereas devices that use a unique key per transaction provide at most one plaintext-ciphertext pair for each session key. Particular implementations or formats may also limit the availability of plaintexts to attackers (e.g. by including randomness in the encrypted values, such as in PIN block format 3), thereby protecting the strength of the encipherment key.

The other symmetric algorithms from Table 2 (MISTY1, CAST-128, Camellia and SEED) should only be used when legacy applications require it. In this case, the maximum strength of the algorithm would be expected to be similar to that of AES with the same keying option, and hence the recommendations from Table 3 can be carried over for those key lengths. Consideration should however be given to the fact that these algorithms have received significantly less scrutiny in the cryptographic community than TDEA and AES. Note that there are recent research papers which propose theoretical related-key attacks against AES using keying options 2 and 3 (192-bit and 256-bit keys respectively). See Reference [75].

When evaluating the suitability of a particular block cipher for a given implementation, it is important to take into account the length of time it is necessary to protect the data that the block cipher is used to encrypt. For example, if a 3-key Triple DES (TDEA with keying option 2) implementation is used to encrypt data which needs to be protected for 10 years after it is encrypted, then encipherment of new data should stop in 2020 [because in terms of years, 2020 + 10 = 2030, the last year where 3-key Triple DES (TDEA with keying option 2) is recommended].

4.4 Block size and key use

Besides key length, block size is an important security parameter, e.g. the French government IT Security Agency recommends against using 64-bit block ciphers for encryption or MAC-ing. The concern with small block size is mainly that text dictionary attacks and matching ciphertext attacks become feasible, as outlined in Reference [55], Note 7.8. A text dictionary attack builds a dictionary of known plaintext-ciphertext pairs (each 1 block), and a complete dictionary for a 64-bit block cipher can thus be built if 2^{64} plaintext-ciphertext pairs are available. Matching ciphertext attacks exploit that the birthday paradox implies that once the number of available ciphertexts for an n-bit block cipher reaches $2^{n/2}$, which for a 64-bit block cipher is approximately 4 290 000 000, one expects to find matching ciphertext blocks, which may reveal partial information about the plaintexts. For this reason it is recommended not to use the same key for more than $2^{n/2}$ times for an n-bit block cipher.

The use of session keys greatly reduces the risks of small block size.

4.5 Modes of operation

The modes of operation for block ciphers should follow ISO/IEC 10116. For TDEA, see also ISO/TR 19038. As stated in ISO/IEC 10116:2006, B.1.2, one property of the Electronic Code Book (ECB) mode is as follows:

> “(...) the same plaintext block always produces the same ciphertext block (for the same key) making it vulnerable to a “dictionary attack”, where a dictionary is built up with corresponding plaintext and ciphertext blocks. The ECB mode is, in general, not recommended for messages longer than one block. The use of ECB may only be specified in future International Standards for those special purposes where the repetition characteristic is acceptable, blocks have to be accessed individually, or blocks have to be accessed randomly”.