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)

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

Page

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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.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

