TECHNICAL **ISO/TR**

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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.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