



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**

Itch Standards
(standards.itch.ai)
Document Preview

[ISO/TS 14742:2025](https://standards.itch.ai/catalog/standards/iso/8bd3dc83-b523-4bf6-92e3-6ba5a76d9416/iso-ts-14742-2025)

<https://standards.itch.ai/catalog/standards/iso/8bd3dc83-b523-4bf6-92e3-6ba5a76d9416/iso-ts-14742-2025>

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO/TS 14742:2025](https://standards.itih.ai/catalog/standards/iso/8bd3dc83-b523-4bf6-92e3-6ba5a76d9416/iso-ts-14742-2025)

<https://standards.itih.ai/catalog/standards/iso/8bd3dc83-b523-4bf6-92e3-6ba5a76d9416/iso-ts-14742-2025>



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

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/TS 14742:2025](https://standards.iteh.ai/catalog/standards/iso/8bd3dc83-b523-4bf6-92e3-6ba5a76d9416/iso-ts-14742-2025)

<https://standards.iteh.ai/catalog/standards/iso/8bd3dc83-b523-4bf6-92e3-6ba5a76d9416/iso-ts-14742-2025>

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.