INTERNATIONAL STANDARD

ISO/IEC 24759

Third edition
2017-03

Information technology — Security techniques — Test requirements for cryptographic modules

Technologies de l'information — Techniques de sécurité — Exigences d'essai pour modules cryptographiques

Reference number
ISO/IEC 24759:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 24759:2014), of which it constitutes a minor revision. It also incorporates the Technical Corrigendum ISO/IEC 24759:2014/Cor.1:2015.

The main changes compared to the previous edition (plus other minor editorial modifications) are as follows:

- References to ISO/IEC 19790:2012 have been corrected throughout:
- 6.2.3.2: AS02.15, AS02.16, AS02.17 and AS02.18 modified;
- 6.3.3: AS03.04, AS03.07, AS03.10 and AS03.15 modified;
- 6.3.4: AS03.19 modified;
- 6.4.1: AS04.02 modified;
- 6.4.2; AS04.05, AS04.06 and AS04.07 modified;
- 6.4.3.1: AS04.11, AS04.13 and AS04.14;
- 6.4.3.2 and AS04.20;
- 6.4.4: AS04.39, AS04.40 and AS04.42 modified;
- 6.5: AS05.05, AS05.06, AS05.07, AS05.08, AS05.13, AS05.17 and AS05.18 modified;
- 6.8: AS08.04 modified;
- 6.10.1: AS10.17 modified.

Information technology — Security techniques — Test requirements for cryptographic modules

1 Scope

This document specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.

This document also specifies the requirements for information that vendors provide to testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790:2012.

Vendors can use this document as guidance in trying to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:2012 before they apply to the testing laboratory for testing.

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 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19790:2012 apply.

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

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

4 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 19790:2012 apply.

5 Document organization

5.1 General

Clause 6 specifies the methods that shall be used by testing laboratories and the requirements for information that vendors shall provide to testing laboratories. Clause 6, besides a general subclause, 6.1, includes eleven subclauses corresponding to the eleven areas of security requirements and six subclauses corresponding to the six annexes, Annex A to Annex F, of ISO/IEC 19790:2012.