American National Standard

(ISO/IEC 19790:2012,
Corrected 2015-12-15, IDT)

Information technology - Security techniques - Security requirements for cryptographic modules

Developed by

incits SM

Where IT all begins

Approved American National Standard

ANSI

Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.

Date of ANSI Approval: 6/25/2014

Published by American National Standards Institute,
25 West 43rd Street, New York, New York 10036

INTERNATIONAL **ISO/IEC**

Second edition
2012-08-15

Corrected version
2015-12-15

Information technology — Security techniques — Security requirements for cryptographic modules

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

Reference number
ISO/IEC 19790:2012(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

Page

1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviated terms 15
5 Cryptographic module security levels 15
5.1 Security Level 1 15
5.2 Security Level 2 16
5.3 Security Level 3 16
5.4 Security Level 4 17
6 Functional security objectives 17
7 Security requirements 18
7.1 General 18
7.2 Cryptographic module specification 20
7.2.1 Cryptographic module specification general requirements 20
7.2.2 Types of cryptographic modules 20
7.2.3 Cryptographic boundary 21
7.2.4 Modes of operations 22
7.3 Cryptographic module interfaces 23
7.3.1 Cryptographic module interfaces general requirements 23
7.3.2 Types of interfaces 24
7.3.3 Definition of interfaces 24
7.3.4 Trusted channel 25
7.4 Roles, services, and authentication 25
7.4.1 Roles, services, and authentication general requirements 25
7.4.2 Roles 26
7.4.3 Services 26
7.4.4 Authentication 28
7.5 Software/Firmware security 29
7.6 Operational environment 31
7.6.1 Operational environment general requirements 31
7.6.2 Operating system requirements for limited or non-modifiable operational environments 33
7.6.3 Operating system requirements for modifiable operational environments 33
7.7 Physical security 35
7.7.1 Physical security embodiments 35
7.7.2 Physical security general requirements 37
7.7.3 Physical security requirements for each physical security embodiment 39
7.7.4 Environmental failure protection/testing 42
7.8 Non-invasive security 43
7.9 Sensitive security parameter management 44
7.9.1 Sensitive security parameter management general requirements 44
7.9.2 Random bit generators 44
7.9.3 Sensitive security parameter generation 44
7.9.4 Sensitive security parameter establishment 45
7.9.5 Sensitive security parameter entry and output 45
7.9.6 Sensitive security parameter storage 46

7.9.7 Sensitive security parameter zeroisation 46
7.10 Self-tests 47
7.10.1 Self-test general requirements 47
7.10.2 Pre-operational self-tests 47
7.10.3 Conditional self-tests 48
7.11 Life-cycle assurance 50
7.11.1 Life-cycle assurance general requirements 50
7.11.2 Configuration management 51
7.11.3 Design 51
7.11.4 Finite state model 51
7.11.5 Development 52
7.11.6 Vendor testing 53
7.11.7 Delivery and operation 54
7.11.8 End of life 54
7.11.9 Guidance documents 54
7.12 Mitigation of other attacks 55

Annex A (normative) Documentation requirements 56
A.1 Purpose 56
A.2 Items 56
A.2.1 General 56
A.2.2 Cryptographic module specification 56
A.2.3 Cryptographic module interfaces 57
A.2.4 Roles, services, and authentication 57
A.2.5 Software/Firmware security 57
A.2.6 Operational environment 58
A.2.7 Physical security 58
A.2.8 Non-invasive security 58
A.2.9 Sensitive security parameter management 58
A.2.10 Self-tests 59
A.2.11 Life-cycle assurance 60
A.2.12 Mitigation of other attacks 61

Annex B (normative) Cryptographic module security policy 62
B.1 General 62
B.2 Items 62
B.2.1 General 62
B.2.2 Cryptographic module specification 62
B.2.3 Cryptographic module interfaces 63
B.2.4 Roles, services, and authentication 63
B.2.5 Software/Firmware security 64
B.2.6 Operational environment 64
B.2.7 Physical security 64
B.2.8 Non-invasive security 65
B.2.9 Sensitive security parameters management 65
B.2.10 Self-tests 66
B.2.11 Life-cycle assurance 66
B.2.12 Mitigation of other attacks 66

Annex C (normative) Approved security functions 67
C.1 Purpose 67
C.1.1 Block ciphers 67
C.1.2 Stream ciphers 67
C.1.3 Asymmetric algorithms and techniques 67
C.1.4 Message authentication codes 67
C.1.5 Hash functions 67
C.1.6 Entity authentication 68

C.1.7 Key management 68
C.1.8 Random bit generation 68

Annex D (normative) Approved sensitive security parameter generation and establishment methods 69
D.1 Purpose 69
D.1.1 Sensitive security parameter generation 69
D.1.2 Sensitive security parameter establishment methods 69

Annex E (normative) Approved authentication mechanisms 70
E.1 Purpose 70
E.1.1 Authentication mechanisms 70

Annex F (normative) Approved non-invasive attack mitigation test metrics 71
F.1 Purpose 71
F.1.1 Non-invasive attack mitigation test metrics 71

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 document 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 and IEC 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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

Technical corrigendum 1 to ISO/IEC 19790:2012 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This corrected version of Technical corrigendum 1 to ISO/IEC 19790:2012 cancels and replaces the first edition (ISO/IEC 19790:2012/Cor 1:2015), incorporating the same technical revisions and miscellaneous editorial corrections showing in **red** text instead of black underlining:

— 3.21: The term "cryptographic boundary" is corrected;

— 3.80: The term "non-security relevant" is corrected;

— 3.108: The term "self-test" is corrected;

— 7.2.2: The requirements **[02.04]**, **[02.05]** and **[02.06]** are corrected;

— 7.2.4.3: The requirement **[02.31]** is corrected;

— 7.3.3: The requirement **[03.14]** is corrected;

— 7.5: The requirements **[05.06]** and **[05.07]** are added. The requirements **[05.08]**, **[05.13]** and **[05.17]** through **[05.23]** are corrected;

— 7.6.3: The requirement **[06.06]** is corrected;

- 7.8: The requirement **[08.04]** is corrected;
- 7.9.1: The requirement **[09.04]** is corrected;
- 7.9.7: The requirement **[09.37]** is corrected;
- 7.10.2.2: The requirement **[10.17]** is corrected;
- 7.11.5: The requirement **[11.26]** is corrected;
- 7.11.7: The requirement **[11.35]** is corrected;
- 7.11.9: The requirement **[11.38]** is corrected;
- A.2.5: The requirements of the 1st and 2nd bullets are corrected;
- A.2.7: The requirement of the 3rd bullet is corrected;
- A.2.10: The requirement of the 4th bullet is corrected;
- B.2.4: The requirement of the 9th bullet is corrected;
- B.2.5: The requirement of the 1st bullet is corrected;
- B.2.7: The requirement of the 2nd level 6th bullet is corrected;
- D.1: Duplicate text is removed;
- D.1.2: The reference to ISO/IEC 15946-3 is removed;
- E.1: Duplicate text is removed; and
- F.1: Duplicate text is removed.

Introduction

In Information Technology there is an ever-increasing need to use cryptographic mechanisms such as the protection of data against unauthorised disclosure or manipulation, for entity authentication and for non-repudiation. The security and reliability of such mechanisms are directly dependent on the cryptographic modules in which they are implemented.

This International Standard provides for four increasing, qualitative levels of security requirements intended to cover a wide range of potential applications and environments. The cryptographic techniques are identical over the four security levels. The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operational environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks.

The overall security rating of a cryptographic module must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilised and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilise cryptographic modules provide an acceptable level of security for the given application and environment. Since each authority is responsible for selecting which approved security functions are appropriate for a given application, compliance with this International Standard does not imply either full interoperability or mutual acceptance of compliant products. The importance of security awareness and of making information security a management priority should be communicated to all concerned.

Information security requirements vary for different applications; organizations should identify their information resources and determine the sensitivity to and the potential impact of a loss by implementing appropriate controls. Controls include, but are not limited to:

— physical and environmental controls;

— access controls;

— software development;

— backup and contingency plans; and

— information and data controls.

These controls are only as effective as the administration of appropriate security policies and procedures within the operational environment.