INTERNATIONAL STANDARD

ISO/IEC 19790

Second edition
2012-08-15

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)

COPYRIGHT PROTECTED DOCUMENT

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) 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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/IEC 19790 was prepared by Technical Committee ISO/TC 2, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 19790:2006), which has been technically revised. It also revises ISO/IEC 19790:2006/Cor 1:2008.

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.

Information technology — Security techniques — Security requirements for cryptographic modules

1 Scope

This International Standard specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems. This International Standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location). This International Standard specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level.

This International Standard specifies security requirements specified intended to maintain the security provided by a cryptographic module and compliance to this International Standard is not sufficient to ensure that a particular module is secure or that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected.

2 Normative references

The following referenced documents are indispensable for the application 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.

The documents listed in Annexes C, D, E and F of this International Standard

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
access control list
ACL
list of permissions to grant access to an object

3.2
administrator guidance
written material that is used by the Crypto Officer and/or other administrative roles for the correct configuration, maintenance, and administration of the cryptographic module

3.3
automated
without manual intervention or input (e.g. electronic means such as through a computer network)

3.4
approval authority
any national or international organisation/authority mandated to approve and/or evaluate security functions

NOTE An approval authority in the context of this definition evaluates and approves security functions based on their cryptographic or mathematical merits but is not the testing entity which would test for conformance to this International Standard.

3.5
approved data authentication technique
approved method that may include the use of a digital signature, message authentication code or keyed hash (e.g. HMAC)

3.6
approved integrity technique
approved hash, message authentication code or a digital signature algorithm

3.7
approved mode of operation
set of services which includes at least one service that utilises an approved security function or process and can include non-security relevant services

NOTE 1 Not to be confused with a specific mode of an approved security function, e.g. Cipher Block Chaining (CBC) mode

NOTE 2 Non-approved security functions or processes are excluded.

3.8
approved security function
security function (e.g. cryptographic algorithm) that is referenced in Annex C

3.9
asymmetric cryptographic technique
cryptographic technique that uses two related transformations: a public transformation (defined by the public key) and a private transformation (defined by the private key)

NOTE The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation in a given limited time and with given computational resources.

3.10
biometric
measurable, physical characteristic or personal behavioral trait used to recognise the identity, or verify the claimed identity, of an operator

3.11
bypass capability
ability of a service to partially or wholly circumvent a cryptographic function

3.12
certificate
entity's data rendered unforgeable with the private or secret key of a certification authority

NOTE Not to be confused with a modules validation certificate issued by a validation authority.

3.13
compromise
unauthorised disclosure, modification, substitution, or use of critical security parameters or the unauthorised modification or substitution of public security parameters

3.14
conditional self-test
test performed by a cryptographic module when the conditions specified for the test occur

3.15
confidentiality
property that information is not made available or disclosed to unauthorised entities

3.16
configuration management system
CMS
management of security features and assurances through control of changes made to hardware, software and documentation of a cryptographic module

3.17
control information
information that is entered into a cryptographic module for the purposes of directing the operation of the module

3.18
critical security parameter
CSP
security-related information whose disclosure or modification can compromise the security of a cryptographic module

EXAMPLE Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors.

NOTE A CSP can be plaintext or encrypted.

3.19
crypto officer
role taken by an individual or a process (i.e. subject) acting on behalf of an individual that accesses a cryptographic module in order to perform cryptographic initialisation or management functions of a cryptographic module

3.20
cryptographic algorithm
well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output

3.21
cryptographic boundary
explicitly defined continuous perimeter that establishes the physical and/or logical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module

3.22
cryptographic hash function
computationally efficient function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally infeasible to find two distinct values that hash into a common value

3.23
cryptographic key
key
sequence of symbols that controls the operation of a cryptographic transformation

EXAMPLE A cryptographic transformation can include but is not limited to encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification.

3.24
cryptographic key component
key component
parameter used in conjunction with other key components in an approved security function to form a plaintext CSP or perform a cryptographic function