Informationsteknik – Säkerhetstekniker – Säkerhetskrav för kryptomoduler
(ISO/IEC 19790:2006, IDT)

Information technology – Security techniques – Security requirements for cryptographic modules
(ISO/IEC 19790:2006, IDT)
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 and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19790 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.
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 security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; self-tests; design assurance; and mitigation of other attacks.

The overall security level 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 utilized 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 utilize 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;
- 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.

This International Standard will be revised later, if a new work item is approved, in order to improve the links with Common Criteria scheme (ISO/IEC 15408).

This International Standard is derived from NIST Federal Information Processing Standard (FIPS) PUB 140-2 (see Bibliography [1]).
Information technology — Security techniques — Security requirements for cryptographic modules

1 Scope

This International Standard specifies the security requirements for a cryptographic module utilized 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, and life protecting data) and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Four security levels are specified for each of 10 requirement areas. Each security level offers an increase in security over the preceding level.

While the security requirements specified in this International Standard are intended to maintain the security provided by a cryptographic module, 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.

ISO/IEC 15408 (all parts), Information technology — Security techniques — Evaluation criteria for IT security

ISO/IEC 18031, Information technology — Security techniques — Random bit generation

3 Terms and definitions

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

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

3.2 approved
ISO/IEC approved or approval authority approved

3.3 approved mode of operation
mode of the cryptographic module that employs only approved security functions

NOTE Not to be confused with a specific mode of an approved security function, e.g., Cipher Block Chaining (CBC) mode.
3.4 approved operating system
any operating system evaluated and approved by an approval authority

3.5 approved protection profile
any protection profile approved by an approval authority

3.6 ISO/IEC approved
security function that is either

- specified in an ISO/IEC standard or
- adopted/recommended in an ISO/IEC standard and specified either in an annex of the ISO/IEC standard or in a document referenced by the ISO/IEC standard

3.7 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) — which have the property that, given the public transformation, it is computationally infeasible to derive the private transformation in a given limited time and with a given limited computing power

3.8 authentication code
cryptographic checksum based on an approved security function

NOTE Also known as a Message Authentication Code (MAC).

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

3.10 compromise
unauthorised disclosure, modification, substitution, or use of CSPs or the unauthorised modification or substitution of PSPs

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

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

3.13 critical security parameter
CSP
secret or private 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.
3.14 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

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

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

3.16 cryptographic key component
key component
parameter(s) used in a security function to perform a cryptographic function

3.17 cryptographic module
module
set of hardware, software, and/or firmware that implements security functions and is contained within the cryptographic boundary

3.18 cryptographic module security policy
security policy
precise specification of the security rules under which a cryptographic module shall operate, including the rules derived from the requirements of this International Standard and additional rules imposed by the module

NOTE See Annex B.

3.19 crypto officer
role taken by an individual or a process (i.e., subject) acting on behalf of an individual allowing cryptographic initialisation or management functions of a cryptographic module to be performed

3.20 data path
physical or logical route over which data passes

NOTE A physical data path may be shared by multiple logical data paths.

3.21 differential power analysis
DPA
analysis of the variations of the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to cryptographic operation

3.22 digital signature
data appended to, or a cryptographic transformation of a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery (e.g., by the recipient)

3.23 electronic key entry
entry of cryptographic keys into a cryptographic module using electronic methods such key loader or on line means

NOTE The operator of the key may have no knowledge of the value of the key being entered.
3.24 electronic key transport
transfer of cryptographic keys, usually in encrypted form, using electronic means such as a computer network

3.25 encrypted key
cryptographic key that has been encrypted using an approved security function with a key encryption key

3.26 entity
person, a group, a device or a process

3.27 environmental failure protection
EFP
use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions or fluctuations outside of the module's normal operating range

3.28 environmental failure testing
EFT
use of specific methods to provide reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions or fluctuations outside of the module's normal operating range

3.29 error detection code
EDC
value computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data

3.30 finite state model
FSM
mathematical model of a sequential machine that is comprised of a finite set of input events, a finite set of output events, a finite set of states, a function that maps states and input to output, a function that maps states and inputs to states (a state transition function), and a specification that describes the initial state

3.31 firmware
programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution

EXAMPLE Storage hardware may include but is not limited to ROM, PROM, EEPROM, or FLASH.

3.32 hardware
physical equipment/components within the cryptographic boundary used to process programs and data

3.33 input data
information that is entered into a cryptographic module and may be used for the purposes of transformation or computation using an approved security function

3.34 integrity
property that sensitive data has not been modified or deleted in an unauthorised and undetected manner
3.35
interface
logical entry or exit point of a cryptographic module that provides access to the module for logical information flows

3.36
key encryption key
KEK
cryptographic key that is used for the encryption or decryption of other keys

3.37
key establishment
process of making available a shared secret key to one or more entities

NOTE Key establishment includes key agreement and key transport.

3.38
key loader
self-contained device that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module

3.39
key management
administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy

3.40
key transport
process of transferring a key from one entity to another entity

3.41
maintenance role
role assumed to perform physical maintenance and/or logical maintenance services

EXAMPLE Maintenance services may include but are not limited to hardware and/or software diagnostics.

3.42
manual key entry
entry of a cryptographic key into a cryptographic module, using a device such as a keyboard

3.43
manual key transport
out of band means of transporting cryptographic keys, such as a key loader

3.44
microcode
processor instructions that correspond to an executable program instruction

EXAMPLE Assembler code.

3.45
operator
individual or a process (subject) operating on behalf of the individual, authorised to assume one or more roles

3.46
output data
information produced by a cryptographic module