INTERNATIONAL STANDARD

ISO/IEC 19790

FIrst edition
2006-03-01

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 19790:2006(E)

© ISO/IEC 2006

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2006

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

;;
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2006 – All rights reserved

Not for Resale

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 9

5 Cryptographic module security levels 9
5.1 Security Level 1 10
5.2 Security Level 2 10
5.3 Security Level 3 10
5.4 Security Level 4 11

6 Functional security objectives 11

7 Security requirements 12
7.1 Cryptographic module specification 14
7.2 Cryptographic module ports and interfaces 15
7.3 Roles, services, and authentication 16
7.4 Finite state model 18
7.5 Physical security 19
7.6 Operational environment 26
7.7 Cryptographic key management 29
7.8 Self-tests 31
7.9 Design assurance 34
7.10 Mitigation of other attacks 36

Annex A (normative) **Documentation requirements** 38

Annex B (normative) **Cryptographic module security policy** 42

Annex C (normative) **Approved protection profiles** 44

Annex D (informative) **Approved security functions** 45

Annex E (informative) **Approved key establishment methods** 47

Annex F (informative) **Recommended software development practices** 48

Annex G (informative) **Examples of mitigation of other attacks** 50

Bibliography 51

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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*.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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]).

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2005 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.47
passivation
process in the construction of semiconductor devices in which junctions, surfaces of components and integrated circuits are afforded a means of protection, which may modify circuit behaviour

NOTE 1 Silicon dioxide or phosphorus glass can be used for this purpose.

NOTE 2 Passivation material is technology dependent.

3.48
password
string of characters used to authenticate an identity or to verify access authorisation

EXAMPLE Letters, numbers, and other symbols.

3.49
personal identification number
PIN
numeric code used to authenticate an identity

3.50
physical protection
safeguarding of a cryptographic module, CSPs and PSPs using physical means

3.51
plaintext key
unencrypted cryptographic key

3.52
port
physical/logical input or output point of a cryptographic module that provides access to the module

3.53
private key
that key of an entity's asymmetric key pair which should only be used by that entity

NOTE In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation.

3.54
production-grade
product, component or software that has been tested to meet operational specifications

3.55
protection profile
implementation-independent set of security requirements for a category of TOE that meet specific consumer needs

3.56
public key
that key of an entity's asymmetric key pair which can be made public

NOTE In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

3.57
public key certificate
public key information of an entity signed by an appropriate certification authority and thereby rendered unforgeable

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.58
public security parameter
PSP
security related public information whose modification can compromise the security of a cryptographic module

EXAMPLE Public cryptographic keys, public key certificates, self-signed certificates, trust anchors, and one time passwords associated with a counter.

3.59
random bit generator
RBG
device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased

3.60
removable cover
physical means which permits access to the physical contents of a cryptographic module

3.61
role
security attribute associated with a user defining the user access rights or limitations to services of a cryptographic module

NOTE One or more services may be associated with a role. A role may be associated with one or more users and a user may assume one or more roles.

3.62
secret key
cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public

3.63
security function
cryptographic algorithms together with modes of operation, such as block ciphers, stream ciphers, asymmetric key, message authentication codes, hash functions, or other security functions, random bit generators, entity authentication and key establishment all approved either by ISO/IEC or an approval authority

NOTE See Annex D.

3.64
seed key
secret value used to initialise a cryptographic function or operation

3.65
simple power analysis
SPA
direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys

3.66
software
programs and data components within the cryptographic boundary and usually stored on erasable media which can be dynamically written and modified during execution

EXAMPLE Erasable media may include but are not limited to hard drives.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.67
split knowledge
process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key

3.68
status information
information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module

3.69
symmetric cryptographic technique
cryptographic technique that uses the same secret key for both the encryption and the decryption transformations

3.70
system software
general purpose software within the cryptographic boundary designed to facilitate the operation of the cryptographic module

EXAMPLES Operating system, compilers and utility programs.

3.71
tamper detection
automatic determination by a cryptographic module that an attempt has been made to compromise the security of the module

3.72
tamper evidence
external indication that an attempt has been made to compromise the security of a cryptographic module

NOTE The evidence of the tamper attempt should be observable.

3.73
tamper response
automatic action taken by a cryptographic module when tamper detection has occurred

3.74
target of evaluation
TOE
information technology product or system and associated administrator and user guidance documentation that is the subject of a CC evaluation

3.75
TOE security functions
TSF
subset of the TOE consisting of all hardware, software, and firmware that must be relied upon for the correct enforcement of the TOE security policy

3.76
TOE security policy
TSP
set of rules that regulate how assets are managed, protected, and distributed within a TOE

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.77
trust anchor
trusted information, which includes a public key algorithm, a public key value, an issuer name, and optionally, other parameters

NOTE 1 Other parameters may include but are not limited to a validity period.

NOTE 2 A trust anchor may be provided in the form of a self-signed certificate.

3.78
trusted path
means by which a user and a TSF can communicate with necessary confidence to support the TSP

3.79
user
individual or process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services

3.80
zeroisation
method of destruction of stored data and CSPs to prevent retrieval and reuse

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

API	Application Program Interface
CAPP	Controlled Access Protection Profile
CBC	Cipher Block Chaining
EAL	Evaluation Assurance Level
EDC	Error Detection Code
HDL	Hardware Description Language
IC	Integrated Circuit
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
ROM	Read-Only Memory

5 Cryptographic module security levels

The following sub-clauses provide an overview of the four security levels. Common examples, given to illustrate how the requirements might be met, are not intended to be restrictive or exhaustive. Within this document, references to a *module* shall be interpreted as a *cryptographic module*.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.1 Security Level 1

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one approved algorithm or approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

Security Level 1 allows the software and firmware components of a cryptographic module to be executed on a general purpose computer system using an unevaluated operating system. Such implementations may be appropriate for some low-level security applications when other controls, such as physical security, network security, and administrative procedures are limited or nonexistent. The implementation of cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements.

5.2 Security Level 2

Security Level 2 enhances the physical security mechanisms of Security Level 1 by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or pick-resistant locks on removable covers or doors.

Tamper-evident coatings or seals are placed on a module so that the coating or seal must be broken to attain physical access to Critical Security Parameters (CSPs) and/or Public Security Parameters (PSPs) within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorised physical access.

Security Level 2 requires, at a minimum, role-based authentication in which a cryptographic module authenticates the authorisation of an operator to assume a specific role and perform a corresponding set of services.

Security Level 2 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that:

- meets the functional requirements specified in an approved protection profile (Annex C); and
- is evaluated at the ISO/IEC 15408 evaluation assurance level EAL2 (or higher).

An approved evaluated operating system may be used. It provides a level of trust so that cryptographic modules executing on general purpose computing platforms are comparable to cryptographic modules implemented using dedicated hardware systems.

5.3 Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs and/or PSPs held within the module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroise all CSPs when the removable covers/doors of the cryptographic module are opened.

Security Level 3 requires identity-based authentication mechanisms, enhancing the security provided by the role-based authentication mechanisms specified for Security Level 2. A cryptographic module authenticates the identity of an operator and verifies that the identified operator is authorised to assume a specific role and perform a corresponding set of services.

Security Level 3 requires the entry or output of CSPs (including the entry or output of CSPs using split-knowledge techniques) to be performed using ports that are physically separated from other ports, or interfaces that are logically separated using a trusted path from other interfaces. CSPs may be entered into or

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

output from the cryptographic module in encrypted form (in which case they may travel through enclosing or intervening systems).

Security Level 3 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that:

- meets the functional requirements specified in an approved protection profile (Annex C) with the additional functional requirement of a Trusted Path (FTP_TRP.1); and
- is evaluated at the ISO/IEC 15408 evaluation assurance level EAL3 (or higher) with the additional assurance requirement of an Informal Target of Evaluation (TOE) Security Policy Model (ADV_SPM.1).

An approved evaluated trusted operating system may be used. The implementation of a trusted path protects CSPs and the software and firmware components of the cryptographic module from other untrusted software or firmware that may be executing on the system.

5.4 Security Level 4

Security Level 4 provides the highest level of security defined in this International Standard. At this level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorised attempts at physical access when CSPs and/or PSPs are contained in the module whether external power is applied or not. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroisation of all CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defences. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and zeroise CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

Security Level 4 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that:

- meets the functional requirements specified for Security Level 3; and
- is evaluated at the ISO/IEC 15408 evaluation assurance level EAL4 (or higher).

An approved evaluated trusted operating system may be used.

6 Functional security objectives

The security requirements specified in this International Standard relate to the secure design and implementation of a cryptographic module. The requirements are derived from the following high-level functional security objectives for a cryptographic module to:

- employ and correctly implement the approved security functions for the protection of sensitive information;
- protect a cryptographic module from unauthorised operation or use;
- prevent the unauthorised disclosure of the contents of the cryptographic module, including CSPs;

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- prevent the unauthorised and undetected modification of the cryptographic module and cryptographic algorithms, including the unauthorised modification, substitution, insertion, and deletion of CSPs and/or PSPs;
- provide indications of the operational state of the cryptographic module;
- ensure that the cryptographic module performs properly when operating in an approved mode of operation; and
- detect errors in the operation of the module and to prevent the compromise of CSPs and/or PSPs resulting from these errors.

7 Security requirements

This clause specifies the security requirements that shall be satisfied by cryptographic module's compliance to this International Standard. The security requirements cover areas related to the design and implementation of a cryptographic module. These areas include cryptographic module specification; module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; self-tests; and design assurance.

An additional area concerned with the mitigation of other attacks is currently not tested except at Security Level 4, but it is required to document implemented controls (e.g., DPA). Table 1 summarizes the security requirements in each of these areas.

A module shall be tested against the requirements of each area addressed in this clause. The cryptographic module shall be independently rated in each area. Several areas provide for increasing levels of security with cumulative security requirements for each security level. In these areas, the cryptographic module will receive a rating that reflects the maximum-security level for which the module fulfils all of the requirements of that area. In areas that do not provide for different levels of security (i.e., standard set of requirements), the cryptographic module will receive a rating commensurate with the overall level of security.

In addition to receiving independent ratings for each of the security areas, a cryptographic module will also receive an overall rating. The overall rating will indicate the minimum of the independent ratings received in the areas.

Many of the security requirements of this International Standard include specific documentation requirements that are summarized at Annex A. All documentation, including copies of the user and installation manuals, shall be provided for evaluation.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 1 — Summary of security requirements

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved algorithms, and approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for critical security parameters logically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production-grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modelling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random bit and key generation, key establishment, key distribution key entry/output, key storage and key zeroisation.			
	Secret and private keys transported using manual transport methods may be entered or output in plaintext form.		Secret and private keys transported using manual transport methods shall be entered or output either encrypted or using split knowledge procedures.	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, and critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and post conditions.
Mitigation of other attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			Specification of mitigation of attacks with testable requirements.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.1 Cryptographic module specification

A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, and is contained within a defined cryptographic boundary. A cryptographic module shall implement at least one approved security function used in an approved mode of operation. Non-approved security functions may also be included for use in non-approved mode of operation (i.e., not security relevant within the scope of the module). The operator shall be able to determine when an approved mode of operation is selected. For Security Levels 1 and 2, the cryptographic module security policy may specify when a cryptographic module is performing in an approved mode of operation. For Security Levels 3 and 4, a cryptographic module shall indicate when an approved mode of operation is selected. Approved security functions are listed at Annex D.

A cryptographic boundary shall consist of an explicitly defined perimeter that establishes the physical and/or logical bounds of a cryptographic module. If a cryptographic module consists of software or firmware components, the cryptographic boundary shall contain the processor(s) and other hardware components that store and protect the software and firmware components. Hardware, software, and firmware components of a cryptographic module can be excluded from the requirements of this International Standard if shown that these components do not affect the security of the module.

The following documentation requirements shall apply to all security-specific hardware, software, and firmware contained within a cryptographic module. These requirements do not apply to microcode or system software whose source code is not available or to any hardware, software, or firmware components that can be shown not to affect the security of the cryptographic module.

1. Documentation shall specify the hardware, software, and firmware components of a cryptographic module, specify the cryptographic boundary surrounding these components, and describe the physical configuration of the module (see clause 7.5).

2. Documentation shall specify any hardware, software, or firmware components of a cryptographic module that are excluded from the security requirements of this International Standard and explain the rationale for the exclusion.

3. Documentation shall specify the physical ports and logical interfaces and all defined input and output data paths of a cryptographic module.

4. Documentation shall specify the manual or logical controls of a cryptographic module, physical or logical status indicators, and relevant physical, logical, and electrical characteristics.

5. Documentation shall list all security functions, both approved and non-approved, that are employed by a cryptographic module and shall specify all modes of operation, both approved and non-approved.

6. Documentation shall specify:

    a. a block diagram depicting all of the major hardware components of a cryptographic module and component interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory; and

    b. the design of the hardware, software, and firmware components of a cryptographic module. High-level specification languages for software/firmware or schematics for hardware shall be used to document the design.

7. Documentation shall specify all security-related information, including CSPs, PSPs, and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8. Documentation shall specify a cryptographic module security policy. The security policy shall include the rules derived from the requirements of this International Standard and the rules derived from any additional requirements imposed through product development (see Annex B).

7.2 Cryptographic module ports and interfaces

A cryptographic module shall restrict all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module. The cryptographic module logical interfaces shall be distinctly defined from each other although they may share one physical port (e.g., input data may enter and output data may exit via the same port) or may be distributed over one or more physical ports (e.g., input data may enter via both a serial and a parallel port). An Application Program Interface (API) of a software component of a cryptographic module may be defined as one or more logical interfaces(s).

A cryptographic module shall have the following four distinctly defined logical interfaces ("input" and "output" are indicated from the perspective of the module).

1. *Data input interface*. All data (except control data entered via the control input interface) that is input to and processed by a cryptographic module (including plaintext data, ciphertext data, CSPs, PSPs, and status information from another module) shall enter via the "data input" interface.

2. *Data output interface*. All data (except status data output via the status output interface) that is output from a cryptographic module (including plaintext data, ciphertext data, CSPs, PSPs, and control information for another module) shall exit via the "data output" interface. All data output via the data output interface shall be inhibited when an error state exists and during self-tests (see clause 7.8).

3. *Control input interface.* All input commands, signals, and control data (including function calls and manual controls such as switches, buttons, and keyboards) used to control the operation of a cryptographic module shall enter via the "control input" interface.

4. *Status output interface*. All output signals, indicators, and status data (including return codes and physical indicators such as Light Emitting Diodes and displays) used to indicate the status of a cryptographic module shall exit via the "status output" interface.

All external electrical power that is input to a cryptographic module (including power from an external power source or batteries) shall enter via a power port. A power port is not required when all power is provided or maintained internally to the cryptographic boundary of the cryptographic module (e.g., an internal battery).

The cryptographic module shall distinguish between data and control data for input and on other hand data and status for output. All input data entering the cryptographic module via the "data input" interface shall only pass through the input data path. All output data exiting the cryptographic module via the "data output" interface shall only pass through the output data path. The output data path shall be logically disconnected from the circuitry and processes while performing key generation, manual key entry, or key zeroisation. To prevent the inadvertent output of sensitive information, two independent internal actions (e.g., two different software flags are set, one of which may be user initiated; or two hardware gates are set serially from two separate actions) shall be required to output plaintext CSPs or sensitive data via any output interface.

SECURITY LEVELS 1 AND 2

The physical port(s) and logical interface(s) used for the input and output of data may be shared physically and logically with other ports and interfaces of the cryptographic module.

SECURITY LEVELS 3 AND 4

Additional requirements include:

- the physical port(s) used for the input and output of plaintext CSPs shall be physically separated from all other ports of the cryptographic module;

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

or

- the logical interfaces used for the input and output of plaintext CSPs shall be logically separated from all other interfaces using a trusted path;

and that

- plaintext CSPs shall be entered into the cryptographic module either via a trusted path or directly without travelling through any enclosing or intervening systems where the key components may inadvertently be stored, combined, or otherwise processed. (See clause 7.7.4.)

7.3 Roles, services, and authentication

A cryptographic module shall support authorised roles for operators and corresponding services within each role. A single operator may assume multiple roles. If a cryptographic module supports concurrent operators, then the module shall internally maintain the separation of the roles assumed by each operator and the corresponding services. An operator is not required to assume an authorised role to perform services where CSPs and PSPs are not modified, disclosed, or substituted (e.g., *show status, self-tests,* or other services that do not affect the security of the module).

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module, and to verify that the operator is authorised to assume the requested role and perform the services within the role.

7.3.1 Roles

A cryptographic module shall support the following authorised roles for operators.

1. *User Role.* The role assumed to perform general security services, including cryptographic operations and other approved security functions.

2. *Crypto Officer Role.* The role assumed to perform cryptographic initialisation or management functions (e.g., module initialisation, input/output of CSPs, PSPs, and audit functions).

If the cryptographic module allows operators to perform maintenance services, then the module shall support the following authorised role.

1. *Maintenance Role.* The role assumed to perform physical maintenance and/or logical maintenance services (e.g., hardware/software diagnostics). All CSPs shall be zeroised when entering or exiting the maintenance role.

A cryptographic module may support other roles or sub-roles in addition to the roles specified above.

7.3.2 Services

Services shall refer to all of the services, operations, or functions that can be performed by a module. *Service inputs* shall consist of all data or control inputs to the module that initiate or obtain specific services, operations, or functions. *Service outputs* shall consist of all data and status outputs that result from services, operations, or functions initiated or obtained by service inputs. Each service input shall result in a service output.

A cryptographic module shall provide the following services to operators.

1. *Show status.* Output the current status of the cryptographic module.

2. *Perform self-tests.* Initiate and run the self-tests as specified in clause 7.8.

3. *Perform approved security functions.* Perform at least one approved security function used in an approved mode of operation as specified in clause 7.1.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A cryptographic module may provide other services, operations, or functions, both approved and non-approved, in addition to the services specified above. Specific services may be provided in more than one role (e.g., key entry services may be provided in the user role and the crypto officer role).

If a cryptographic module implements a *bypass* capability, where services are provided without cryptographic processing (e.g., transferring plaintext through the module without encryption), then:

- two independent internal actions shall be required to activate the capability to prevent the inadvertent bypass of plaintext data due to a single error (e.g., two different software or hardware flags are set, one of which may be user-initiated), and

- the module shall show status to indicate whether the bypass capability:

    1. *is not* activated, and the module is exclusively providing services *with* cryptographic processing (e.g., plaintext data *is* encrypted);

    2. *is* activated and the module is exclusively providing services *without* cryptographic processing (e.g., plaintext data *is not* encrypted); or

    3. *is alternately* activated and deactivated and the module is providing some services *with* cryptographic processing and some services *without* cryptographic processing (e.g., for modules with multiple communication channels, plaintext data *is* or *is not* encrypted depending on each channel configuration).

7.3.3 Operator authentication

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorised to assume the requested role and perform services within that role. Depending on the security level, the module shall support at least one of the following mechanisms to control access to the module. It shall support either:

- *Role-Based Authentication*. If role-based authentication mechanisms are supported by a cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator and shall authenticate the assumption of the selected role (or set of roles). The cryptographic module is not required to authenticate the individual identity of the operator. The selection of roles and the authentication of the assumption of selected roles may be combined. If a cryptographic module permits an operator to change roles, then the module shall authenticate the assumption of any role that was not previously authenticated; or

- *Identity-Based Authentication*. If identity-based authentication mechanisms are supported by a cryptographic module, the module shall require that the operator be individually identified, shall require that one or more roles either be implicitly or explicitly selected by the operator, and shall authenticate the identity of the operator and the authorisation of the operator to assume the selected role (or set of roles). The authentication of the identity of the operator, selection of roles, and the authorisation of the assumption of the selected roles may be combined. If a cryptographic module permits an operator to change roles, then that module shall verify the authorisation of the identified operator to assume any role that was not previously authorised.

A cryptographic module may permit an authenticated operator to perform all of the services allowed within an authorised role, or may require separate authentication for each service or for different sets of services. When a module is powered off and subsequently powered on, the results of previous authentications shall not be retained and the module shall require the operator to be re-authenticated.

Various types of authentication data may be required by a cryptographic module to implement the supported authentication mechanisms, including (but not limited to) the knowledge or possession of a password, PIN, cryptographic key or equivalent; possession of a physical key, token, or equivalent; or verification of personal characteristics. Authentication data within the module shall be protected against unauthorised disclosure, modification, and substitution.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The initialisation of authentication mechanisms may warrant special treatment. If a cryptographic module does not contain the authentication data required to authenticate the operator for the first time the module is accessed, then other authorised methods (e.g., procedural controls or use of factory-set or default authentication data) shall be used to control access to the module and initialise the authentication mechanisms.

The strength of the authentication mechanism shall conform to the following specifications.

1. For each attempt to use the authentication mechanism, the probability shall meet the strength of the authentication objective. For example, less than one in 1,000,000 that a random attempt shall succeed (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination thereof).

2. For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall meet the strength of the authentication objective. For example, be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.

3. Feedback of authentication data to an operator shall be obscured during authentication (e.g., no visible display of characters when entering a password).

4. Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism by providing more information than the fact that the authentication passed or failed.

Authentication requirements as they apply to each security level are as follows.

SECURITY LEVEL 1

A cryptographic module is not required to employ authentication mechanisms to control access to the module. If a module does not support authentication mechanisms, the module shall require that the operator either implicitly or explicitly select one or more roles.

SECURITY LEVEL 2

A cryptographic module shall employ *role-based* authentication to control access to the module.

SECURITY LEVELS 3 AND 4

A cryptographic module shall employ *identity-based* authentication mechanisms to control access to the module.

7.4 Finite state model

The operation of a cryptographic module shall be specified using a finite state model (or equivalent) represented by a state transition diagram and/or a state transition table.

The state transition diagram and/or state transition table includes:

- all operational and error states of a cryptographic module;
- the corresponding transitions from one state to another;
- the input events that cause transitions from one state to another; and
- the output events resulting from transitions from one state to another.

A cryptographic module shall include the following operational and error states.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

1. *Power on/off states*. States for primary, secondary, or backup power. These states may distinguish between power sources being applied to a cryptographic module.

2. *Crypto officer states*. States in which the crypto officer services are performed (e.g., cryptographic initialisation and key management).

3. *CSP/PSP entry states*. States for entering CSPs and PSPs into the cryptographic module.

4. *User states*. States in which authorised users obtain security services, perform cryptographic operations, or perform other approved or non-approved functions.

5. *Self-test states*. States in which the cryptographic module is performing self-tests.

6. *Error states*. States when the cryptographic module has encountered an error. Error states may include "hard" errors that indicate an equipment malfunction and that may require maintenance, service or repair of the cryptographic module, or recoverable "soft" errors that may require initialisation or resetting of the module. Recovery from error states shall be possible except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.

A cryptographic module may contain other states including, but not limited to, the following:

1. *Bypass states*. States in which a bypass capability is activated and services are provided without cryptographic processing (e.g., transferring plaintext through the cryptographic module).

2. *Maintenance states*. States for maintaining and servicing a cryptographic module, including physical and logical maintenance testing. If a cryptographic module contains a maintenance role, then a maintenance state shall be included.

7.5 Physical security

A cryptographic module shall employ physical security mechanisms in order to restrict unauthorised physical access to the contents of the module and to deter unauthorised use or modification of the module (including substitution of the entire module) when installed. All hardware, software, firmware, and data components within the cryptographic boundary shall be protected.

A cryptographic module that is implemented completely in software such that the physical security is provided solely by the host platform is not subject to the physical security requirements of this International Standard.

Physical security requirements are specified for three defined physical embodiments of a cryptographic module.

1. ***Single-chip cryptographic modules*** are physical embodiments in which a single integrated circuit (IC) chip may be used as a standalone device or may be embedded within an enclosure or a product that may not be physically protected. Examples of single-chip cryptographic modules include single IC chips or smart cards with a single IC chip.

2. ***Multiple-chip embedded cryptographic modules*** are physical embodiments in which two or more IC chips are interconnected and are embedded within an enclosure or a product that may not be physically protected. Examples of multiple-chip embedded cryptographic modules include adapters and expansion boards.

3. ***Multiple-chip standalone cryptographic modules*** are physical embodiments in which two or more IC chips are interconnected and the entire enclosure is physically protected. Examples of multiple-chip, standalone cryptographic modules include encrypting routers or secure radios.

Depending on the physical security mechanisms of a cryptographic module, unauthorised attempts at physical access, use, or modification shall have a high probability of being detected:

- subsequent to an attempt by leaving visible signs (i.e., tamper evidence)

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

and/or

- during an access attempt so that appropriate immediate actions can be taken by the cryptographic module to protect CSPs and PSPs (i.e., tamper response). *Immediate actions* shall be taken to mean that retrieval of CSPs and PSPs are not possible.

Table 2 summarizes the physical security requirements, both the general and the three specific embodiments for each of the four security levels. The embodiment-specific physical security requirements at each security level enhance the general requirements at the same level, and the embodiment-specific requirements of the previous level.

In general, Security Level 1 requires minimal physical protection. Security Level 2 requires the addition of tamper-evident mechanisms. Security Level 3 adds requirements for the use of strong enclosures with tamper detection and response mechanisms for removable covers and doors. Security Level 4 adds requirements for the use of strong enclosures with tamper detection and response mechanisms for the entire enclosure. Environmental failure protection (EFP) or environmental failure testing (EFT) is required at Security Level 4. Tamper detection and tamper response are not substitutes for tamper evidence.

Security requirements are specified for a maintenance access interface when a cryptographic module is designed to permit physical access (e.g., by the module vendor or other authorised individuals).

7.5.1 General physical security requirements

The following requirements shall apply to all physical embodiments.

- Documentation shall specify the physical embodiment and the security level for which the physical security mechanisms of a cryptographic module are implemented.

- If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g., by the module vendor or other authorised individual), then:

    1. a maintenance access interface shall be defined;

    2. the maintenance access interface shall include all physical access paths to the contents of the cryptographic module, including any removable covers or doors;

    3. any removable covers or doors included within the maintenance access interface shall be safeguarded using the appropriate physical security mechanisms; and

    4. all CSPs shall be zeroised when the maintenance access interface is accessed.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 2 — Summary of physical security requirements

	General Requirements for all Embodiments	Single-Chip Cryptographic Modules	Multiple-Chip Embedded Cryptographic Modules	Multiple-Chip Standalone Cryptographic Modules
Security Level 1	Production-grade components (with standard passivation). Automatic zeroisation when accessing the maintenance access interface	No additional requirements.	If applicable, production-grade enclosure or removable cover.	Production-grade enclosure.
Security Level 2	Evidence of tampering (e.g., cover, enclosure, or seal).	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Tamper response and zeroisation circuitry. Protected vents.	Hard opaque tamper-evident coating on chip or strong removal-resistant and penetration resistant enclosure.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-Chip Standalone Security Level 3 requirements.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong enclosure with removal/penetration attempts causing serious damage.
Security Level 4	EFP or EFT for temperature and voltage.	Hard opaque removal-resistant coating on chip.	Tamper detection envelope with tamper response and zeroisation capability.	Tamper detection/ response envelope with tamper response and zeroisation capability.

SECURITY LEVEL 1

The following requirements shall apply to all cryptographic modules for Security Level 1.

1. The cryptographic module shall consist of production-grade components that shall include standard passivation techniques (e.g., a conformal coating or a sealing coat applied over the module's circuitry to protect against environmental or other physical damage).

2. When performing physical maintenance, all CSPs contained in the cryptographic module shall be zeroised. Zeroisation shall either be performed procedurally by the operator or automatically by the cryptographic module.

SECURITY LEVEL 2

In addition to the general requirements for Security Level 1, the following requirement shall apply to all cryptographic modules for Security Level 2.

1. The cryptographic module shall provide evidence of tampering (e.g., on the cover, enclosure, and seal) when physical access to the module is attempted.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

SECURITY LEVEL 3

In addition to the general requirements for Security Levels 1 and 2, the following requirements shall apply to all cryptographic modules for Security Level 3.

1. If the cryptographic module contains any doors or removable covers or if a maintenance access interface is defined, then the module shall contain tamper response and zeroisation capability. The tamper response and zeroisation capability shall immediately zeroise all CSPs when a door is opened, a cover is removed, or when the maintenance access interface is accessed. The tamper response and zeroisation capability shall remain operational when CSPs are contained within the cryptographic module.

2. If the cryptographic module contains ventilation holes or slits, then the holes or slits shall be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g., require at least one 90 degree bend or obstruction with a substantial blocking material).

SECURITY LEVEL 4

In addition to the general requirements for Security Levels 1, 2, and 3, the module shall either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT) as specified in clause 7.5.2 for Security Level 4.

7.5.1.1 Single-chip cryptographic modules

In addition to the general security requirements specified in clause 7.5.1, the following requirements are specific to single-chip cryptographic modules.

SECURITY LEVEL 1

There are no additional Security Level 1 requirements for single-chip cryptographic modules.

SECURITY LEVEL 2

In addition to the requirements for Security Level 1, the following requirements shall apply to single-chip cryptographic modules for Security Level 2.

1. The cryptographic module shall be covered with a tamper-evident coating (e.g., a tamper-evident passivation material or a tamper-evident material covering the passivation) or contained in a tamper-evident enclosure to deter direct observation, probing, or manipulation of the module and to provide evidence of attempts to tamper with or remove the module.

2. The tamper-evident coating or tamper-evident enclosure shall be opaque within the visible spectrum (i.e., light of wavelength range of 400nm to 750nm).

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements shall apply to single-chip cryptographic modules for Security Level 3.

Either the:

1. module shall be covered with a hard opaque tamper-evident coating (e.g., a hard opaque epoxy covering the passivation);

or

2. enclosure shall be implemented so that attempts at removal or penetration of the enclosure shall have a high probability of causing serious damage to the cryptographic module (i.e., the module will not function).

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to single-chip cryptographic modules for Security Level 4.

1. The cryptographic module shall be covered with a hard, opaque removal-resistant coating with hardness and adhesion characteristics such that attempting to peel or pry the coating from the module will have a high probability of resulting in serious damage to the module (i.e., the module will not function).

2. The removal-resistant coating shall have solvency characteristics such that dissolving the coating will have a high probability of dissolving or seriously damaging the module (i.e., the module will not function).

7.5.1.2 Multiple-chip embedded cryptographic modules

In addition to the general security requirements specified in clause 7.5.1, the following requirements are specific to multiple-chip embedded cryptographic modules.

SECURITY LEVEL 1

If the cryptographic module is contained within an enclosure or removable cover, a production-grade enclosure or removable cover shall be used.

SECURITY LEVEL 2

In addition to the requirement for Security Level 1, the following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 2.

Either the:

1. module components shall be covered with a tamper-evident coating or potting material (e.g., etch-resistant coating or bleeding paint) to deter direct observation, probing, or manipulation of module components and to provide evidence of attempts to tamper with or remove module components; and

   tamper-evident coating or tamper-evident enclosure shall be opaque within the visible spectrum;

or

2. module shall be entirely contained within a metal or hard plastic production-grade enclosure that may include doors or removable covers;

   the enclosure shall be opaque within the visible spectrum; and

   if the enclosure includes any doors or removable covers, then the doors or covers shall be locked with pick-resistant mechanical locks employing physical or logical keys or shall be protected with tamper-evident seals (e.g., evidence tape or holographic seals).

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 3.

Either the:

1. multiple-chip embodiment of the circuitry within the cryptographic module shall be covered with a hard coating or potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum;

or

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2. applicable Security Level 3 requirements for multiple-chip standalone cryptographic modules shall apply. (clause 7.5.1.3).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 4.

1. The module components shall be covered by potting material or contained within an enclosure encapsulated by a tamper detection envelope (e.g., a flexible Mylar printed circuit with a serpentine geometric pattern of conductors or a wire-wound package or a non-flexible, brittle circuit or a strong enclosure) that shall detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure to an extent sufficient for accessing CSPs and/or PSPs.

2. The module shall contain tamper response and zeroisation circuitry that shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroise all CSPs. The tamper response circuitry shall remain operational when CSPs and/or PSPs are contained within the cryptographic module. The zeroisation capability shall remain operational when CSPs are contained within the cryptographic module.

7.5.1.3 Multiple-chip standalone cryptographic modules

In addition to the general security requirements specified in clause 7.5.1, the following requirements are specific to multiple-chip standalone cryptographic modules.

SECURITY LEVEL 1

For Security Level 1, the cryptographic module shall be entirely contained within a metal or hard plastic production-grade enclosure that may include doors or removable covers.

SECURITY LEVEL 2

In addition to the requirements for Security Level 1, the following requirements shall apply to multiple-chip standalone cryptographic modules for Security Level 2.

1. The enclosure of the cryptographic module shall be opaque within the visible spectrum.

2. If the enclosure of the cryptographic module includes any doors or removable covers, then the doors or covers shall be locked with pick-resistant mechanical locks employing physical or logical keys or shall be protected with tamper-evident seals (e.g., evidence tape or holographic seals).

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements shall apply to multiple-chip standalone cryptographic modules for Security Level 3.

Either the:

1. multiple-chip embodiment of the circuitry within the module shall be covered with a hard potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum;

or

2. module shall be contained within a strong enclosure such that attempts at removal or penetration of the enclosure will have a high probability of causing serious damage to the module (i.e., the module will not function).

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to multiple-chip standalone cryptographic modules for Security Level 4.

1. The module shall be encapsulated by a tamper detection envelope, by the use of tamper detection mechanisms such as cover switches (e.g., micro switches, magnetic Hall effect switches, permanent magnetic actuators, etc.), motion detectors (e.g., ultrasonic, infrared, or microwave), or other tamper detection mechanisms as described above for multiple-chip embedded cryptographic modules. The tamper detection mechanisms shall detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure, to an extent sufficient for accessing CSPs and/or PSPs.

2. The cryptographic module shall contain tamper response and zeroisation capability that shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroise all CSPs. The tamper response capability shall remain operational when CSPs and/or PSPs are contained within the cryptographic module. The zeroisation capability shall remain operational when CSPs are contained within the cryptographic module.

7.5.2 Environmental failure protection/testing

The electronic devices and circuitry are designed to operate within a particular range of environmental conditions. Deliberate or accidental excursions outside the specified normal operating ranges of voltage and temperature can cause erratic operation or failure of the electronic devices or circuitry that can compromise the security of the cryptographic module. Reasonable assurance that the security of a cryptographic module cannot be compromised by extreme environmental conditions can be provided by having the module employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT).

For Security Levels 1, 2, and 3, a module is not required to employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT). At Security Level 4, a module shall either employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT).

7.5.2.1 Environmental failure protection features (alternative 1)

Environmental failure protection (EFP) features shall protect a cryptographic module against unusual environmental conditions or fluctuations (accidental or induced) outside of the module's normal operating range that can compromise the security of the module.

The module shall monitor and correctly respond to fluctuations in the operating *temperature* and *voltage* outside of the specified normal operating ranges.

The EFP features shall involve electronic capability or devices that continuously measure the operating temperature and voltage of a cryptographic module. If the temperature or voltage falls outside of the cryptographic module's normal operating range, the protection capability shall either:

1. shutdown the module to prevent further operation; or

2. immediately zeroise all CSPs.

Documentation shall specify the normal operating ranges of a cryptographic module and the environmental failure protection features employed by the module.

7.5.2.2 Environmental failure testing procedures (alternative 2)

Environmental failure testing (EFT) shall involve a combination of analysis, simulation, and testing of a cryptographic module to provide reasonable assurance that the environmental conditions or fluctuations (accidental or induced) outside the module's normal operating ranges for temperature and voltage will not compromise the security of the module.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

EFT shall demonstrate that, if the operating temperature or voltage falls outside the normal operating range of the module resulting in a failure , at no time shall the security of the cryptographic module be compromised.

The temperature range to be tested shall be from a temperature within the normal operating temperature range up to the largest negative temperature that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs; and from a temperature within the normal operating temperature range up to the largest positive temperature that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs. The temperature range to be tested shall be from - 100° to + 200° Celsius (- 150° to + 400° Fahrenheit), however, the test shall be interrupted as soon as either (1) the module is shutdown to prevent further operation, (2) all CSPs are immediately zeroised or (3) put the module in failure.

The voltage range to be tested shall be from the smallest negative voltage (with respect to ground) that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs to the smallest positive voltage (with respect to ground) that that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs, including reversing the polarity of the voltages.

Documentation shall specify the normal operating ranges of the cryptographic module and the environmental failure tests performed.

7.6 Operational environment

The *operational environment* of a cryptographic module refers to the management of the software, firmware, and/or hardware components required for the module to operate. The operational environment can be non-modifiable (e.g., firmware contained in ROM, or software contained in a computer with I/O devices disabled), or modifiable (e.g., firmware contained in RAM or software executed by a general purpose computer). An operating system is an important component of the operating environment of the module.

A *general-purpose operational environment* refers to the use of a commercially available general-purpose operating system (i.e., resource manager) that manages the software and firmware components within the cryptographic boundary, and also manages system and operator(s) processes/thread(s), including general-purpose application software such as word processors.

This clause specifies two specific operational environments. Each is distinct from the other and may or may not be required to comply with Clause 7.6.1.

1. A *limited operational environment* refers to a static non-modifiable virtual operational environment (e.g., JAVA virtual machine on a non-programmable PC card) with no underlying general-purpose operating system upon which the operational environment uniquely resides.

2. A *modifiable operational environment* refers to an operating environment that *may* be reconfigured to add/delete/modify functionality, and/or *may* include general-purpose operating system capabilities (e.g., use of a computer O/S, configurable smart card O/S, or programmable firmware). Operating systems are considered to be modifiable operational environments if software/firmware components can be modified by the operator and/or the operator can load and execute software or firmware (e.g., a word processor) that was not included as part of the validation of the module.

If the operational environment is a modifiable operational environment, the operating system requirements in clause 7.6.1 shall apply.

If the operational environment is non-modifiable or a limited operational environment, the operating system requirements in clause 7.6.1 do not apply.

Documentation shall specify the operational environment for a cryptographic module, including, if applicable, the operating system employed by the module, and for Security Levels 2, 3, and 4, the approved protection profile as listed in Annex C.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.6.1 Operating system requirements

SECURITY LEVEL 1

The following requirements shall apply to operating systems for Security Level 1.

1. For Security Level 1 only, the operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded).

2. For Security Level 1 only, the cryptographic module shall prevent access by other processes to CSPs and/or PSPs during the time the cryptographic module is executing/operational. Processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators. Non-cryptographic processes shall not interrupt a cryptographic module during execution.

3. All cryptographic software and firmware shall be installed in a form that protects the software and firmware source and executable code from unauthorised disclosure and modification.

4. A cryptographic mechanism using an approved integrity technique (e.g., an approved message authentication code or digital signature algorithm) shall be applied to all cryptographic software and firmware components within the cryptographic module. This cryptographic mechanism requirement may be incorporated as part of the Software/Firmware Integrity Test (clause 7.8.1) if an approved authentication technique is employed for that test.

SECURITY LEVEL 2

In addition to the applicable requirements for Security Level 1 (i.e. points 3 and 4), the following requirements shall also apply for Security Level 2.

1. All cryptographic software and firmware, CSPs, PSPs, and control and status information shall be under the control of:

   a. an operating system that meets the functional requirements specified in the Protection Profiles specified in Annex C and shall be evaluated at the ISO/IEC 15408 evaluation assurance level EAL2.

2. To protect plaintext data, cryptographic software and firmware, CSPs, PSPs, the discretionary access control mechanisms of the operating system shall be configured to specify the set of roles that can:

   a. *execute* stored cryptographic software and firmware;

   b. *modify* (i.e., write, replace, and delete) the following cryptographic module software or firmware components stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g., audit data), CSPs, PSPs, and plaintext data;

   c. *read* the following cryptographic software components stored within the cryptographic boundary: cryptographic data (e.g., audit data), CSPs, and plaintext data; and

   d. *enter* CSPs and/or PSPs.

3. The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not.

4. The operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5. The operating system shall provide an audit mechanism to record modifications, accesses, deletions, and additions of cryptographic data, CSPs and PSPs.

   a. The following events shall be recorded by the audit mechanism:

      - attempts to provide invalid input for crypto officer functions; and
      - the addition or deletion of an operator to/from a crypto officer role.

   b. The audit mechanism shall be capable of auditing the following events:

      - operations to process audit data stored in the audit trail;
      - requests to use authentication data management mechanisms;
      - use of a security-relevant crypto officer function;
      - requests to access user authentication data associated with the cryptographic module;
      - use of an authentication mechanism (e.g., login) associated with the cryptographic module;
      - explicit requests to assume a crypto officer role; and
      - the allocation of a function to a crypto officer role.

   c. The stored audit data shall be protected from unauthorised access.

SECURITY LEVEL 3

In addition to the applicable requirements for Security Levels 1 and 2, the following requirements shall apply for Security Level 3.

1. All cryptographic software and firmware, CSPs, PSPs, and control and status information shall be under the control of an operating system that meets the functional requirements specified in the Protection Profiles specified in Annex C. The operating system shall be evaluated at the ISO/IEC 15408 evaluation assurance level EAL3 and include the following additional requirements: Trusted Path (FTP_TRP.1) and Informal TOE Security Policy Model (ADV_SPM.1).

2. All CSPs, control inputs, and status outputs shall be communicated via a trusted mechanism (e.g., a dedicated I/O physical port or a trusted path). If a trusted path is used, the TOE Security Functions (TSF) shall support the trusted path between the TSF and the operator when a positive TSF-to-operator connection is required. Communications via this trusted path shall be activated exclusively by an operator or the TSF and shall be logically isolated from other paths.

3. In addition to the audit requirements of Security Level 2, the following events shall be recorded by the audit mechanism:

   a. attempts to use the trusted path function;

   b. identification of the initiator and target of a trusted path;

   c. unsuccessful self test operations; and

   d. notification of tamper detection.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

SECURITY LEVEL 4

In addition to the applicable requirements for Security Levels 1, 2, and 3, the following requirements shall also apply to operating systems for Security Level 4.

1. All cryptographic software, CSPs, PSPs, and control and status information shall be under the control of an operating system that meets the functional requirements specified in the Protection Profiles specified in Annex C. The operating system shall be evaluated at the ISO/IEC 15408 evaluation assurance level EAL4.

7.7 Cryptographic key management

The security requirements for cryptographic key management encompass the entire lifecycle of CSPs and PSPs, employed by the cryptographic module. Key management includes random bit and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroisation. A cryptographic module may also employ the key management mechanisms of another cryptographic module. Encrypted CSPs refer to CSPs that are encrypted using an approved algorithm or approved security function.

NOTE CSPs encrypted using a non-approved algorithm or proprietary algorithm or method is considered in plaintext form, within the scope of this International Standard.

CSPs shall be protected within the cryptographic module from unauthorised disclosure, modification, and substitution. PSPs shall be protected within the cryptographic module against unauthorised modification and substitution.

Documentation shall specify all CSPs, and PSPs employed by a cryptographic module.

7.7.1 Random bit generators (RBGs)

A cryptographic module may employ random bit generators (RBGs), a chain of RBGs, or may be solely an RBG. All RBGs and their usage shall be defined. If a cryptographic module employs an approved RBG, or chain of RBGs, in an approved mode of operation:

- RBG entropy source shall be subject to the RBG entropy test as specified in clause 7.8.1;
- deterministic components of an RBG shall be subject to the cryptographic algorithm test in clause 7.8.1; and
- data output from the RBG shall pass the continuous random bit generator test as specified in clause 7.8.2.

The RBG and its mode of operation shall be compliant with ISO/IEC 18031.

7.7.2 Key generation

A cryptographic module may generate cryptographic keys internally. Cryptographic keys generated by the cryptographic module for use by an approved algorithm or security function shall be generated using an approved RBG.

Compromising the security of the key generation method (e.g., guessing the seed value to initialise the deterministic RBG) shall require at least as many operations as determining the value of the generated key.

If a seed key is entered during the key generation process, entry of the key shall meet the key entry requirements specified in clause 7.7.4. If intermediate key generation values are output from the cryptographic module, the values shall be output either:

1. in encrypted form; or

2. under split knowledge techniques.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.7.3 Key establishment

Key establishment may be performed by approved methods (e.g., use of a public key algorithm), manual transport methods (use of a manually-transported key loading device), or a combination of electronic and manual transport methods. If a cryptographic module employs key establishment methods, only approved key establishment methods shall be used and defined. Examples of approved key establishment methods are listed at Annex E to this International Standard.

Compromising the security of the key establishment method (e.g., compromising the security of the algorithm used for key establishment) shall require at least as many operations as determining the key value being transported or agreed upon.

If a *key transport* method is used, the cryptographic key being transported shall meet the key entry/output requirements of clause 7.7.4. If a *key agreement* method is used (e.g., a cryptographic key is derived from shared intermediate values), the shared values are not required to meet the key entry/output requirements of clause 7.7.4.

7.7.4 Key entry and output

Cryptographic keys may be entered into or output from a cryptographic module. The entry or output of keys shall be performed and defined using either manual (e.g., via a keyboard) or electronic methods (e.g., smart cards/tokens, PC cards, or other electronic key loading devices or connections).

A seed key, if entered during key generation, shall be entered in the same manner as cryptographic keys.

All encrypted secret and private keys, entered into or output from a cryptographic module and used in an approved mode of operation, shall be encrypted using an approved algorithm (listed at Annex D) and may be integrity protected. Public keys may be entered into or output from a cryptographic module in plaintext form and may be integrity protected. A cryptographic module shall associate a key (secret, private, or public) entered into or output from the module with the name of the correct entity (i.e., person, group, or process) to which the key is assigned.

Manually-entered cryptographic keys shall be verified during entry into a cryptographic module for accuracy using the manual key entry test specified in clause 7.8.2. During key entry, the manually entered values may be temporarily displayed to allow visual verification and to improve accuracy. If encrypted cryptographic keys or key components are manually entered into the cryptographic module, then the plaintext values of the cryptographic keys or key components shall not be displayed.

SECURITY LEVELS 1 AND 2

Secret and private keys transported using *electronic methods* shall be entered into and output from a cryptographic module in encrypted form. Secret and private keys transported using *manual transport methods* may be entered into or output from a cryptographic module in plaintext form.

SECURITY LEVELS 3 AND 4

Key entry and output requirements for security levels 3 and 4 are as follows.

1. Secret and private keys transported using *electronic methods* shall be entered into and output from a cryptographic module in encrypted form.

2. Secret and private keys transported using *manual transport methods* shall be entered into or output from a cryptographic module either (1) in encrypted form or (2) using split knowledge techniques (i.e., as two or more plaintext cryptographic key components).

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3. If split knowledge procedures are used:

   a. the cryptographic module shall separately authenticate the operator entering or outputting each key component;

   b. plaintext cryptographic key components shall be entered into or output from the cryptographic module either via a trusted path or directly without travelling through any enclosing or intervening systems where the key components may inadvertently be stored, combined, or otherwise processed (see clause 7.2);

   c. at least two key components shall be required to reconstruct the original cryptographic key;

   d. documentation shall verify that if knowledge of *n* key components is required to reconstruct the original key, then knowledge of any *n*-1 key components provides no information about the original key other than the length; and

   e. the documentation shall specify the procedures employed by a cryptographic module.

7.7.5 Key storage

Cryptographic keys stored within a cryptographic module shall be stored either in plaintext form or encrypted form. Plaintext secret and private keys shall not be accessible from outside the cryptographic module to unauthorised operators.

A cryptographic module shall associate a cryptographic key (secret, private, or public) stored within the module with the name of the correct entity (e.g., person, group, or process) to which the key is assigned.

7.7.6 Key zeroisation

A cryptographic module shall provide methods to zeroise all CSPs. Zeroisation of encrypted CSPs or CSPs otherwise physically or logically protected within an additional embedded validated module (meeting the requirements of this International Standard) is not required.

CSPs need not meet these zeroisation requirements if they are used exclusively to reveal plain text data to processes that are authentication proxies.

NOTE An example of such a CSP is a module initialisation key.

7.8 Self-tests

A cryptographic module shall perform and define power-up self-tests and conditional self-tests to ensure that the module is functioning properly. *Power-up self-tests* shall be performed when the cryptographic module is powered up. *Conditional self-tests* shall be performed when an applicable security function or operation is invoked (i.e., security functions for which self-tests are required). A cryptographic module may perform other power-up or conditional self-tests in addition to the tests specified in this International Standard.

If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator. The error indicator may be explicitly output via the status output interface or implicitly by some other mechanism. The cryptographic module shall not perform any cryptographic operations while in an error state. All data output via the data output interface shall be inhibited when an error state exists.

Documentation shall specify:

- the self tests performed by the cryptographic module, including power-up and conditional tests;
- the error states that a cryptographic module can enter when a self-test fails; and
- the conditions and actions necessary to exit the error states and resume normal operation of a cryptographic module (i.e., this may include maintenance or repair of the module).

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.8.1 Power-up tests

Power-up tests shall be performed by a cryptographic module when it is powered up (after being powered off, reset, rebooted, etc.). The power-up tests shall be initiated automatically and shall not require operator intervention. When the power-up tests are completed, the results shall be output explicitly via the "status output" interface or implicitly. All data output via the data output interface shall be inhibited when the power-up tests are performed.

In addition to performing the power-up tests when powered up, the module shall permit operators to initiate the tests on demand for periodic testing of the module. Resetting, rebooting, and power cycling are acceptable means for the on-demand initiation of power-up tests.

The module shall perform the following power-up tests.

1. Cryptographic algorithm test. A cryptographic algorithm test using a known answer shall be conducted for all cryptographic functions (e.g., encryption, decryption, authentication) of each approved cryptographic algorithm implemented by a cryptographic module. A known-answer test involves operating the cryptographic algorithm on data for which the correct output is already known and comparing the calculated output with the previously generated output (the known answer). If the calculated output does not equal the known answer, the known answer test shall fail.

   Cryptographic algorithms whose outputs vary for a given set of inputs (e.g., the Digital Signature Algorithm) shall be tested using a known-answer test or shall be tested using a pair-wise consistency test (specified below). Message digest algorithms shall have an independent known-answer test or the known-answer test shall be included with the associated cryptographic algorithm test (e.g., the Digital Signature Standard).

   If a cryptographic module includes two independent implementations of the same cryptographic algorithm, then the known-answer test may be omitted but, shall be replaced having the outputs of two implementations shall be continuously compared. If the outputs of two implementations are not equal, the cryptographic algorithm test shall fail.

2. *RBG entropy test*. If a cryptographic module employs approved RBGs in an approved mode of operation, the module shall perform the cryptographic health tests on the RBG entropy sources found in ISO/IEC 18031.

3. *Software/firmware integrity test*. A software/firmware integrity test using an error detection code (EDC) or approved authentication technique (e.g., an approved message authentication code or digital signature algorithm) shall be applied to all validated software and firmware components within a cryptographic module when the module is powered up. The software/firmware integrity test is not required for any software and firmware components excluded from the security requirements of this International Standard (refer to clause 7.1). If the calculated result does not equal the previously generated result, the software/firmware test shall fail.

   If an Error Detection Code (EDC) is used, the EDC shall be at least 16 bits in length.

   NOTE The software/firmware integrity test does not apply to data stored in ROM.

4. *Critical functions test*. There may be other security functions critical to the secure operation of a cryptographic module that shall be tested when the module is powered up as part of the power-up tests. Critical security functions performed under specific conditions shall be tested as conditional tests.

Documentation shall specify all security functions critical to the secure operation of a cryptographic module and shall identify the applicable power-up tests and conditional tests performed by the module.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.8.2 Conditional tests

Conditional tests shall be performed as specified below.

7.8.2.1 Pair-wise consistency test

If a cryptographic module generates asymmetric keys, to be used for the approved functions key transport or generation and verification of digital signatures, then the pair-wise consistency of the keys shall be verified using a known answer test.

7.8.2.2 Manual key entry test

If cryptographic keys or key components are manually entered into a module, then the following manual key entry tests shall be performed:

1. The cryptographic key or key components shall have an EDC applied, or shall be entered using duplicate entries;

2. If an EDC is used, the EDC shall be at least 16 bits in length; and

3. If the EDC cannot be verified, or the duplicate entries do not match, the test shall fail.

7.8.2.3 Continuous random bit generator test

If a cryptographic module employs approved RBGs in an approved mode of operation, the module shall perform the following continuous random bit generator test on the RBG that tests for failure to a constant value.

1. If each call to a RBG produces blocks of *n* bits (where *n* > 15), the first *n*-bit block generated after power-up, initialisation, or reset shall not be used, but shall be saved for comparison with the next *n*-bit block to be generated. Each subsequent generation of an *n*-bit block shall be compared with the previously generated block. The test shall fail if any two compared *n*-bit blocks are equal.

2. If each call to a RBG produces fewer than 16 bits, the first *n* bits generated after power-up, initialisation, or reset (for some *n* > 15) shall not be used, but shall be saved for comparison with the next *n* generated bits. Each subsequent generation of *n* bits shall be compared with the previously generated *n* bits. The test fails if any two compared *n*-bit sequences are equal.

This test is only for purpose of minimum health test of the RBG and not addressing the quality of the random generation. All other tests on RBG will be done according to ISO/IEC 18031.

7.8.2.4 Bypass test

If a cryptographic module implements a *bypass* capability where the services may be provided without cryptographic processing (e.g., transferring plaintext through the module), then the following bypass tests shall be performed to ensure that a single point of failure of module components will not result in the unintentional output of plaintext.

A cryptographic module shall test for the correct operation of the services providing cryptographic processing when a switch takes place between an exclusive bypass service and an exclusive cryptographic service.

If a cryptographic module can automatically alternate between a bypass service and a cryptographic service, providing some services *with* cryptographic processing and some services *without* cryptographic processing, then the module shall test for the correct operation of the services providing cryptographic processing when the mechanism governing the switching procedure is modified (e.g., an IP address source/destination table).

The mechanism or logic governing the switching procedure shall be defined and documented.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.9 Design assurance

Design assurance refers to the use of best practices specifications applied to a cryptographic module during the design, deployment, and operation of a cryptographic module, providing assurance that the module is properly tested, configured, delivered, installed and developed, and that the proper operational guidance documentation is provided. Security requirements are specified for configuration, delivery and operation, development, and documents.

7.9.1 Configuration management

Configuration management specifies the security requirements for a configuration management system. It provides assurance that the functional requirements and specifications are realized in the implementation.

A configuration management system shall be implemented for a cryptographic module and module components within the cryptographic boundary, and for associated module documentation. Each version of each configuration item (e.g., cryptographic module, module components, user guidance, security policy, and operating system) that comprises the module and associated documentation shall be assigned and labelled with a unique identification number.

A configuration management system shall provide measures such that only authorised changes are made to the configuration items. A configuration management system shall support the generation of a cryptographic module**.** A configuration management system shall provide an automated means by which only authorised changes are made to a cryptographic module implementation representation. A configuration management system shall provide an automated means to support the generation of a cryptographic module. A configuration management system shall uniquely identify all configuration items. A configuration list shall uniquely identify all configuration items that comprise a cryptographic module. The evidence shall demonstrate that the configuration management system is operating in accordance with the configuration management plan and that all configuration items have been and are being effectively maintained under the configuration management system.

A list of configuration items shall include the information regarding previous security flaws and their resolution.

7.9.2 Delivery and operation

Delivery and operation specifies the security requirements for the secure delivery, installation, and start-up of a cryptographic module, providing assurance that the module is securely delivered to authorised operators, and is installed and initialised in a correct and secure manner.

SECURITY LEVEL 1

Documentation shall specify the procedures for secure installation, initialisation, and start-up of a cryptographic module.

SECURITY LEVELS 2, 3, AND 4

In addition to the requirements of Security Level 1, documentation shall specify the procedures required for maintaining security while distributing and delivering versions of a cryptographic module to authorised operators.

7.9.3 Development

Development specifies the security requirements for the representation of a cryptographic module's security functionality at various levels of abstraction from the functional interface to the implementation representation. Development provides assurance that the implementation of the module corresponds to the module security policy and functional specification.

Functional specification refers to a high-level description of the ports and interfaces visible to the operator and a high-level description of the behaviour of the cryptographic module.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of a cryptographic module design and implementation in its development environment. The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of a cryptographic module.

All development tools used for implementation shall be unambiguously identified. The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation. The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

SECURITY LEVEL 1

The following requirements shall apply to cryptographic modules for Security Level 1.

1. Documentation shall specify the correspondence between the design of the hardware, software, and firmware components of a cryptographic module and the cryptographic module security policy (see clause 7.1).

2. If a cryptographic module contains software or firmware components, documentation shall specify the source code for the software and firmware components, annotated with comments that clearly depict the correspondence of the components to the design of the module.

3. If a cryptographic module contains hardware components, documentation shall specify the schematics and/or Hardware Description Language (HDL) listings for the hardware components.

SECURITY LEVEL 2

In addition to the requirements for Security Level 1, the following requirement shall apply to cryptographic modules for Security Level 2.

Documentation shall specify a functional specification that informally describes a cryptographic module, the external ports and interfaces of the module, and the purpose of the interfaces.

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements shall apply to cryptographic modules for Security Level 3.

All software and firmware components within a cryptographic module shall be implemented using a high-level language, except that the limited use of a low-level language (e.g., assembly language or microcode) is allowed if essential to the performance of the module or when a high-level language is not available.

If HDL is used, all hardware components within a cryptographic module shall be implemented using a high-level specification language.

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to cryptographic modules for Security Level 4.

1. Documentation shall specify a formal model that describes the rules and characteristics of the cryptographic module security policy. The formal model shall be specified using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory.

2. Documentation shall specify a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module security policy.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3. Documentation shall specify an informal proof of the correspondence between the formal model and the functional specification.

4. For each cryptographic module hardware, software, and firmware component, the source code shall be annotated with comments that specify (1) the preconditions required upon entry into the module component, function, or procedure in order to execute correctly and (2) the post conditions expected to be true when execution of the module component, function, or procedure is complete. The preconditions and post conditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behaviour of the cryptographic module component, function, or procedure.

5. Documentation shall specify an informal proof of the correspondence between the design of the cryptographic module (as reflected by the precondition and post condition annotations) and the functional specification.

NOTE Implementation of software and firmware components within a cryptographic module using recommended development practices listed at Annex F will facilitate the analysis of the components for conformance to the requirements in this International Standard and will reduce the chance of design errors.

7.9.4 Guidance documents

Crypto officer guidance is concerned with the correct configuration, maintenance, and administration of the cryptographic module. *User guidance* describes the security functions of the cryptographic module along with instructions, guidelines, and warnings for the secure use of the module. If a cryptographic module supports a maintenance role, user/crypto officer guidance describes the physical and/or logical maintenance services for operators assuming the maintenance role.

Guidance for the crypto officer shall specify:

1. the administrative functions, security events, security parameters (and parameter values, as appropriate), physical ports, and logical interfaces of the cryptographic module available to the crypto officer;

2. procedures on how to administer the cryptographic module in a secure manner: and

3. assumptions regarding user behaviour that are relevant to the secure operation of the cryptographic module.

Guidance for the user shall specify:

1. the approved security functions, physical ports, and logical interfaces available to the users of a cryptographic module; and

2. all user responsibilities necessary for the secure operation of a cryptographic module.

7.10 Mitigation of other attacks

Susceptibility of a cryptographic module to such attacks depends on module type, implementation, and implementation environment. Such attacks may be of particular concern for cryptographic modules implemented in hostile environments (e.g., where the attackers may be the authorised operators of the module). Such types of attacks generally rely on the analysis of information obtained from sources physically external to the module. In all cases, the attacks attempt to determine some knowledge about the cryptographic keys and CSPs within the cryptographic module. Brief summaries of currently known attacks are provided at Annex G.

SECURITY LEVELS 1, 2, AND 3

The existence and proper functioning of the security mechanisms will be validated when requirements and associated tests are developed.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

SECURITY LEVEL 4

At Security Level 4, if mitigation of other attacks is claimed, documentation shall include the specification of the appropriate methods and means necessary to validate the additional security claimed. The specification of testing methods shall be used to test the mitigation methods employed.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(normative)

Documentation requirements

A.1 Purpose

This annex specifies the minimum documentation required for a cryptographic module that is to undergo an independent verification or evaluation scheme.

A.1.1 Cryptographic module specification

a. Specification of the hardware, software, and firmware components of a cryptographic module, specification of the cryptographic boundary surrounding these components, and description of the physical configuration of the module. *(Security Levels 1, 2, 3, and 4).*

b. Specification of any hardware, software, or firmware components of a cryptographic module that are excluded from the security requirements of this International Standard and an explanation of the rationale for the exclusion. *(Security Levels 1, 2, 3, and 4).*

c. Specification of the physical ports and logical interfaces of a cryptographic module. *(Security Levels 1, 2, 3, and 4).*

d. Specification of the manual or logical controls of a cryptographic module, physical or logical status indicators, and applicable physical, logical, and electrical characteristics. *(Security Levels 1, 2, 3, and 4).*

e. List of all security functions, both approved and non-approved, that are employed by a cryptographic module and specification of all modes of operation, both approved and non-approved. *(Security Levels 1, 2, 3 and 4).*

f. Block diagram depicting all of the major hardware components of a cryptographic module and component interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory. *(Security Levels 1, 2, 3, and 4).*

g. Specification of the design of the hardware, software, and firmware components of a cryptographic module. *(Security Levels 1, 2, 3, and 4).*

h. Specification of all security-related information, including CSPs, PSPs, and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module *(Security Levels 1, 2, 3, and 4)*.

i. Specification of a cryptographic module security policy including the rules derived from the requirements of this International Standard and the rules derived from any additional requirements imposed by the vendor). *(Security Levels 1, 2, 3, and 4).*

A.1.2 Cryptographic module ports and interfaces

Specification of the physical ports and logical interfaces of a cryptographic module and all defined input and output data paths. *(Security Levels 1, 2, 3, and 4).*

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.1.3 Roles, services, and authentication

Specification of all authorised roles supported by a cryptographic module. *(Security Levels 1, 2, 3, and 4).*

Specification of the services, operations, or functions provided by a cryptographic module, both approved and non-approved. For each service, specification of the service inputs, corresponding service outputs, and the authorised role(s) in which the service can be performed. *(Security Levels 1, 2, 3, and 4).*

Specification of any services provided by a cryptographic module for which the operator is not required to assume an authorised role, and how these services do not modify, disclose, or substitute CSPs and/or PSPs, or otherwise affect the security of the module *(Security Levels 1, 2, 3, and 4)*.

Specification of the authentication mechanisms supported by a cryptographic module, the types of authentication data required to implement supported authentication mechanisms, the authorised methods used to control access to the module for the first time and initialise the authentication mechanism, and the corresponding strength of the mechanisms supported by the module. *(Security Levels 2, 3, and 4).*

A.1.4 Finite state model

Representation of a finite state model (or equivalent) using the state transition diagram and/or state transition table that specifies all operational and error states, corresponding transitions from one state to another, input events (including data inputs and control inputs) that cause transitions from one state to another, and output events (including internal module conditions, data outputs, and status outputs) resulting from transitions from one state to another. *(Security Levels 1, 2, 3, and 4).*

A.1.5 Physical security

Specification of the physical embodiment and security level for which the physical security mechanisms of a cryptographic module are implemented. Specification of the physical security mechanisms that are employed by a module. *(Security Levels 1, 2, 3, and 4).*

If a cryptographic module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access, specification of the maintenance access interface and how CSPs are to be zeroised when the maintenance access interface is accessed. *(Security Levels 1, 2, 3, and 4).*

Specification of the normal operating ranges of a cryptographic module. Specification of the environmental failure protection features employed by a cryptographic module or specification of the environmental failure tests performed. *(Security Level 4).*

A.1.6 Operational Environment

Specification of the operational environment for the cryptographic module. *(Security Levels 1, 2, 3, and 4).*

Identification of the operating system employed by a cryptographic module, the applicable Protection Profile, and the ISO/IEC 15408 assurance level. *(Security Levels 2, 3, and 4).*

A.1.7 Cryptographic key management

Specification of all CSPs and PSPs employed by a cryptographic module *(Security Levels 1, 2, 3, and 4)*.

Specification of each RBG (approved and non-approved) employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4).*

Specification of each of the key generation methods (approved and non-approved) employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4).*

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Specification of the key establishment methods employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4).*

Specification of the key entry and output methods employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4).*

If split knowledge procedures are used, proof that if knowledge of *n* key components is required to reconstruct the original key, then knowledge that any *n*-1 key components provides no information about the original key other than length, and specification of the split-knowledge procedures employed by a cryptographic module. *(Security Levels 3 and 4).*

Specification of the key storage methods employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4).*

Specification of the key zeroisation methods employed by a cryptographic module. *(Security Levels 1, 2, 3, and 4).*

A.1.8 Self-tests

Specification of the self-tests performed by a cryptographic module including power-up and conditional tests. *(Security Levels 1, 2, 3, and 4).*

Specification of the error states that a cryptographic module can enter when a self-test fails, and the conditions and actions necessary to exit the error states and resume normal operation of a module. *(Security Levels 1, 2, 3, and 4).*

Specification of all security functions critical to the secure operation of a cryptographic module and identification of the applicable power-up tests and conditional tests performed by the module. *(Security Levels 1, 2, 3, and 4).*

If a cryptographic module implements a bypass capability, specification of the mechanism or logic governing the switching procedure. *(Security Levels 1, 2, 3, and 4).*

A.1.9 Design assurance

Specification of procedures for secure installation, generation, and start-up of a cryptographic module. *(Security Levels 1, 2, 3, and 4).*

Specification of the procedures for maintaining security while distributing and delivering versions of a cryptographic module to authorised operators. *(Security Level 2, 3, and 4).*

Specification of the correspondence between the design of the hardware, software, and firmware components of a cryptographic module and the cryptographic module security policy (i.e., the rules of operation). *(Security Levels 1, 2, 3, and 4).*

If a cryptographic module contains software or firmware components, specification of the source code for the software and firmware components, annotated with comments that clearly depict the correspondence of the components to the design of the module. *(Security Levels 1, 2, 3, and 4).*

If a cryptographic module contains hardware components, specification of the schematics and/or Hardware Description Language (HDL) listings for the hardware components. *(Security Levels 1, 2, 3, and 4).*

Functional specification that informally describes a cryptographic module, the external ports and interfaces of the module, and the purpose of the interfaces. *(Security Levels 2, 3, and 4).*

Specification of a formal model that describes the rules and characteristics of the cryptographic module security policy, using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory. *(Security Level 4).*

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Specification of a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module security policy. *(Security Level 4).*

Specification of an informal proof of the correspondence between the formal model and the functional specification. *(Security Level 4).*

For each hardware, software, and firmware component, source code annotation with comments that specify (1) the preconditions required upon entry into the module component, function or procedure in order to execute correctly and (2) the post conditions expected to be true when execution of the module component, function, or procedure is complete. *(Security Level 4).*

Specification of an informal proof of the correspondence between the design of the cryptographic module (as reflected by the precondition and post condition annotations) and the functional specification. *(Security Level 4).*

Guidance specification for the crypto officer:

- the administrative functions, security events, security parameters (and parameter values, as appropriate), physical ports, and logical interfaces of the cryptographic module available to the crypto officer *(Security Levels 1, 2, 3, and 4)*;
- procedures on how to administer the cryptographic module in a secure manner *(Security Levels 1, 2, 3, and 4)*; and
- assumptions regarding user behaviour that is relevant to the secure operation of the cryptographic module. *(Security Levels 1, 2, 3, and 4).*

Guidance specification for the user appears as:

- the approved security functions, physical ports, and logical interfaces available to the users of the cryptographic module *(Security Levels 1, 2, 3, and 4)*; and
- all user responsibilities necessary for the secure operation of the module. *(Security Levels 1, 2, 3, and 4).*

A.1.10 Mitigation of other attacks

If a cryptographic module is designed to mitigate one or more specific attacks, specification in the module's security policy of the security mechanisms employed by the cryptographic module to mitigate the attack(s). *(Security Levels 1, 2, 3, and 4).*

A.1.11 Security policy

Annex B specifies the minimum requirements of a cryptographic module security policy. The security policy shall include the rules derived from the requirements of this International Standard and the rules derived from any additional requirements imposed by the application. (*Security Levels 1, 2, 3, and 4*).

© ISO/IEC 2006 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(normative)

Cryptographic module security policy

B.1 Purpose

This annex specifies the minimum requirements of a cryptographic module security policy. The security policy shall include the rules derived from the requirements of this International Standard and the rules derived from any additional requirements imposed by the application.

B.2 Background

A cryptographic module security policy consists of a specification of the security rules, under which a cryptographic module shall operate, including the security rules derived from the requirements of the International Standard and the additional security rules imposed through the module development.

The specification is sufficiently detailed so as to answer the following questions.

1. What access does operator *X*, performing service *Y* while in role of *Z*, have access to security-relevant data item *W* for every role, service, and security-relevant data item contained in the cryptographic module?

2. What physical security mechanisms are implemented to protect a cryptographic module and what actions are required to ensure that the physical security of a module is maintained?

3. What security mechanisms are implemented in a cryptographic module to mitigate attacks for which testable requirements are not defined in this International Standard?

B.3 Objective

There are two major reasons for developing and following a precise cryptographic module security policy.

1. A module security policy provides a specification of the cryptographic security that will allow individuals and organizations to determine whether a cryptographic module, as implemented, satisfies a stated security policy.

2. A module security policy describes to individuals and organizations the capabilities, protection, and access rights provided by the cryptographic module, thereby allowing an assessment of whether the module will adequately serve the individual or organizational security requirements.

B.3.1 Identification and authentication policy

The cryptographic module security policy specifies an identification and authentication policy, including:

- all roles (e.g., user, crypto officer, and maintenance) and associated type of authentication (e.g., identity-based, role-based, or none); and

- the authentication data required of each role or operator (e.g., password or biometric data) and the corresponding strength of the authentication mechanism.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.3.2 Access control policy

The cryptographic module security policy specifies an access control policy. The specification is of sufficient detail to identify the CSPs and PSPs that the operator has access to while performing a service, and the type(s) of access the operator has to the parameters.

The security policy specifies:

- all roles supported by a cryptographic module;
- all services provided by a cryptographic module;
- all CSPs and PSPs employed by the cryptographic module, including;
    1. secret, private, and public cryptographic keys (both plaintext and encrypted),
    2. authentication data such as passwords or PINs, and
    3. other security-relevant information (e.g., audited events and audit data);
- for each role, the services an operator is authorised to perform within that role, and
- for each service within each role, the type(s) of access to the CSPs and PSPs.

B.3.3 Physical security policy

The cryptographic module security policy specifies a physical security policy, including the:

- physical security mechanisms that are implemented in a cryptographic module (e.g., tamper-evident seals, locks, tamper response and zeroisation switches, and alarms); and
- actions required by the operator(s) to ensure that physical security is maintained (e.g., periodic inspection of tamper-evident seals or testing of tamper response and zeroisation switches).

B.3.4 Mitigation of other attacks policy

The cryptographic module security policy specifies a security policy for mitigation of other attacks, including the security mechanisms implemented to mitigate the attacks.

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C
(normative)

Approved protection profiles

This annex provides a list of the ISO/IEC approved protection profiles applicable to ISO/IEC 19790.

In addition, protection profiles approved by an approval authority may be used.

a) Controlled Access Protection Profile (CAPP), http://niap.nist.gov/cc-scheme/pp/PP_CAPP_V1.d.pdf

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

Annex D
(informative)

Approved security functions

D.1 Purpose

This annex provides a list of the ISO/IEC approved standards that specify approved security functions applicable to ISO/IEC 19790. The categories include block ciphers, stream ciphers, asymmetric key, message authentication codes, hash functions, entity authentication, key establishment and random bit generators. This list is not exhaustive.

This does not preclude the use of Approval authority approved security functions.

D.1.1 Block ciphers

a. ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

D.1.2 Stream ciphers

a. ISO/IEC 18033-4, *Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers*

D.1.3 Asymmetric algorithms and techniques

a. ISO/IEC 9796-2, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

b. ISO/IEC 9796-3, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms*

c. ISO/IEC 14888 (all parts), *Information technology — Security techniques — Digital signatures with appendix*

d. ISO/IEC 15946 (all parts), *Information technology — Security techniques — Cryptographic techniques based on elliptic curves*

e. ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*[1)]

D.1.4 Message authentication codes

a. ISO/IEC 9797-2, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*

1) To be published.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.1.5 Hash functions

a. ISO/IEC 10118-2, Information *technology — Security techniques — Hash-functions — Part 2*: *Hash-functions using an n-bit block cipher*

b. ISO/IEC 10118-3, *Information technology — Security techniques — Hash-functions —Part 3: Dedicated hash-functions*

c. ISO/IEC 10118-4, *Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic*

D.1.6 Entity authentication

a. ISO/IEC 9798-2, *Information technology — Security techniques — Entity authentication — Part 2: Mechanisms using symmetric encipherment algorithms*

b. ISO/IEC 9798-3, *Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques*

c. ISO/IEC 9798-4, *Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function*

d. ISO/IEC 9798-5, *Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques*

e. ISO/IEC 9798-6, *Information technology — Security techniques — Entity authentication — Part 6: Mechanisms using manual data transfer*

f. ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

g. ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

h. ISO/IEC 11770-4, *Information technology — Security techniques — Key management — Part 4: Key establishment mechanisms based on weak secrets*

D.1.7 Random bit generator

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex E
(informative)

Approved key establishment methods

E.1 Purpose

This annex provides a list of the ISO/IEC approved key establishment methods applicable to ISO/IEC 19790. It does not preclude the use of Approval authority approved key establishment methods. This list is not exhaustive.

E.1.1 Key establishment methods

a. ISO/IEC 11770-2*, Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques.*

b. ISO/IEC 11770-3*, Information technology – Security techniques – Key Management – Part 3: Mechanisms using asymmetric techniques.*

c. ISO/IEC 15946-3*, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment.*

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex F
(informative)

Recommended software development practices

F.1 Purpose

This annex provides guidance for best practice software development. It does not contain security requirements applicable to cryptographic modules within the scope of this International Standard.

F.2 Background

Life-cycle software engineering recommendations (dealing with the specification, construction, verification, testing, maintenance, and documentation of software) should be followed. Software engineering practices may include documented unit testing, code reviews, explicit high-level and low-level design documents, explicit requirements and functional specifications, structure charts and data flow diagrams, function-point analysis, defect and resolution tracking, configuration management, and a documented software development process.

For all software development, both large and small, the following programming techniques are consistent with current practices and should be used to facilitate analysis of software components of a cryptographic module and to reduce chances of programming errors.

F.3 Modular design

A modular design is recommended, especially for moderate to large-scale software development efforts. Each software module should have well-defined and readily understood logical interfaces.

Software components should be constructed using the principles of data abstraction. If available, an object-oriented, high-level language that supports the construction of abstract data types should be used.

The software should be hierarchically structured as a series of layers.

F.4 Software module/procedure interfaces

Entries to a software module or procedure should be through external calls on explicitly defined interfaces.

Each procedure should have only one entry point and at most two exit points, one for normal exits and one for error exits.

Data should be communicated between software modules and between procedures through the use of argument lists and/or explicit return values. Global variables should not be used among procedures except where necessary for the implementation of abstract data types. Input and output values should be checked for range errors using assertion statements (if provided by the programming language in use).

When CSPs are used as in input value, it should be communicated via its memory address to the called function. That doesn't allow the duplication of sensitive information.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

F.5 Internal construction

Each procedure should perform only a single, well-defined function.

Control flow within a single thread of execution should be defined using only sequencing, structured programming constructs for conditionals (e.g., if-then-else or case), and structured constructs for loops (e.g., while-do or repeat-until).

If concurrent execution is employed (e.g., via multiple threads, tasks, or processes), the software components should enforce limits on the maximum allowable degree of concurrency and should use structured synchronization constructs to control access to shared data.

Equivalence of variables should not be used to permit multiple memory usage for conflicting purposes.

Robust command parsing and range checking mechanisms should be implemented to guard against malformed requests, out-of-range parameters, and I/O buffer overflows.

If the use of an intermediate variable (e.g. memory allocation) is required by the procedure to compute a CSP, the software component should ensure that the intermediate variable is zeroised after it's used.

F.6 In-line documentation

Each software module, procedure, and major programming construct should be documented specifying the functions performed along with a (formal or informal) specification of preconditions and post conditions.

Each loop should be preceded by a convincing argument (as a comment) that termination is guaranteed.

Variable names should be used in only one context within the same procedure.

Each variable should have an associated comment identifying the purpose of the variable and noting the range of allowable values, including if the range is unrestricted.

If concurrency is employed, the documentation should specify how limits are enforced on the maximum allowable degree of concurrency and how accesses to shared data are synchronized in order to avoid (possibly undetected) run-time errors.

F.7 Assembly language

The following additional programming practices should be used when the implementation is in assembly language.

- All code should be position independent except where appropriate security concerns, efficiency, or hardware constraints require position dependency.
- All register references should use symbolic register names.
- Self-modifying code should not be used.
- All procedures should be responsible for saving and restoring the contents of any register that is used within the procedure.
- Control transfer instructions should not use numeric literals.
- Each unit should contain comments describing register use in the unit.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex G
(informative)

Examples of mitigation of other attacks

Power Analysis: Attacks based on the analysis of power consumption can be divided into two general categories, Simple Power Analysis (SPA) and Differential Power Analysis (DPA). SPA involves a direct (primarily visual) analysis of electrical power consumption patterns and timings derived from the execution of individual instructions carried out by a cryptographic module during a cryptographic process. The patterns are obtained through monitoring the variations in electrical power consumption of a cryptographic module for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently values of cryptographic keys. DPA has the same goals but utilizes advanced statistical methods and/or other techniques to analyse the variations of the electrical power consumption of a cryptographic module. Cryptographic modules that utilize external power (direct current) sources appear to be at greatest risk. Methods that may reduce the overall risk of Power Analysis attacks include the use of capacitors to level the power consumption, the use of internal power sources, and the manipulation of the individual operations of the algorithms or processes to level the rate of power consumption during cryptographic processing.

Timing Analysis: Timing Analysis attacks rely on precisely measuring the time required by a cryptographic module to perform specific mathematical operations associated with a cryptographic algorithm or process. The timing information collected is analysed to determine the relationship between the inputs to the module and the cryptographic keys used by the underlying algorithms or processes. The analysis of the relationship may be used to exploit the timing measurements to reveal the cryptographic key or CSPs. Timing Analysis attacks assume that the attacker has knowledge of the design of the cryptographic module. Manipulation of the individual operations of the algorithms or processes to reduce timing fluctuations during processing is one method to reduce the risk of this attack.

Fault Induction: Fault Induction attacks utilize external forces such as microwaves, temperature extremes, and voltage manipulation to cause processing errors within the cryptographic module. An analysis of these errors and their patterns can be used in an attempt to reverse engineer the cryptographic module, revealing certain features and implementations of cryptographic algorithms and subsequently revealing the values of cryptographic keys. Cryptographic modules with limited physical security appear to be at greatest risk. Proper selection of physical security features may be used to reduce the risk of this attack.

© ISO/IEC 2006 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-2, May 25, 2001 (with latest change notices).

[2] ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*

[3] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[4] ISO/IEC 9798 (all parts), *Information technology — Security techniques — Entity authentication mechanisms*

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2006 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 51 pages

© ISO/IEC 2005 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale