INTERNATIONAL STANDARD ISO/IEC 19790:2012
TECHNICAL CORRIGENDUM 1

Published 2015-10-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Security requirements for cryptographic modules —

TECHNICAL CORRIGENDUM 1

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

RECTIFICATIF TECHNIQUE 1

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

ICS 35.040 **Ref. No. ISO/IEC 19790:2012/Cor.1:2015(E)**

Published in Switzerland

Contents

Page

Foreword

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

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

This corrected edition cancels and replaces the second edition (ISO/IEC 19790:2012), which has been technically revised and incorporates miscellaneous editorial corrections related to the following:

- 3.21: The term "cryptographic boundary" is corrected;
- 3.80: The term "non-security relevant" is corrected;
- 3.108: The term "self-test" is corrected;
- 7.2.2: The requirements **[02.04]**, **[02.05]** and **[02.06]** are corrected;
- 7.2.4.3: The requirement **[02.31]** is corrected;
- 7.3.3: The requirement **[03.14]** is corrected;
- 7.5: The requirements **[05.06]** and **[05.07]** are added. The requirements **[05.08]**, **[05.13]** and **[05.17]** through **[05.23]** are corrected;
- 7.6.3: The requirement **[06.06]** is corrected;
- 7.8: The requirement **[08.04]** is corrected;
- 7.9.1: The requirement **[09.04]** is corrected;
- 7.9.7: The requirement **[09.37]** is corrected;
- 7.10.2.2: The requirement **[10.17]** is corrected;

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

Introduction

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

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

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

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

- physical and environmental controls;
- access controls;
- software development;
- backup and contingency plans; and
- information and data controls.

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

Information technology — Security techniques — Security requirements for cryptographic modules

1 Scope

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

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

The documents listed in ISO/IEC 19790 Annexes C, D, E and F *Information technology – Security techniques – Security requirements for cryptographic modules*

3 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NOTE A CSP can be plaintext or encrypted.

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

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

3.21
cryptographic boundary
explicitly defined perimeter that establishes the boundary of all components (i.e. set of hardware, software or firmware components) of the cryptographic module

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

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

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

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

3.25
cryptographic module
module
set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary

3.26
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 or validation authority

NOTE See Annex B

3.27
data path
physical or logical route over which data passes

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

3.28
degraded operation
operation where a subset of the entire set of algorithms, security functions, services or processes are available and/or configurable as a result of reconfiguration from an error state

3.29
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

3.30
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)

3.31
direct entry
entry of a SSP or key component into a cryptographic module, using a device such as a keyboard

3.32
disjoint signature
one or more signatures which together represent an entire set of code

3.33
electromagnetic emanations
EME
intelligence-bearing signal, which, if intercepted and analyzed, potentially discloses the information that is transmitted, received, handled, or otherwise processed by any information-processing equipment

3.34
electronic entry
entry of SSPs or key components into a cryptographic module using electronic methods

NOTE The operator of the key can have no knowledge of the value of the key being entered.

3.35
encompassing signature
single signature for an entire set of code

3.36
encrypted key
cryptographic key that has been encrypted using an approved security function with a key encryption key. Considered protected

3.37
entity
person, group, device or process

3.38
entropy
measure of the disorder, randomness or variability in a closed system

NOTE The entropy of a random variable *X* is a mathematical measure of the amount of information provided by an observation of *X*.

3.39
environmental failure protection
EFP
use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions outside of the module's normal operating range

3.40
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 outside of the module's normal operating range

3.41
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

3.42
executable form
form of the code in which the software or firmware is managed and controlled completely by the operational environment of the module and does not require compilation (e.g. no source code, object code or just-in-time compiled code)

3.43
fault induction
technique to induce operating behaviour changes in hardware by the application of transient voltages, radiation, laser or clock skewing techniques

3.44
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

3.45
firmware
executable code of a cryptographic module that is stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution while operating in a non-modifiable or limited operational environment

EXAMPLE Storage hardware can include but not limited to PROM, EEPROM, FLASH, solid state memory, hard drives, etc

3.46
firmware module
module that is composed solely of firmware

3.47
functional specification
high-level description of the ports and interfaces visible to the operator and high-level description of the behaviour of the cryptographic module

3.48
functional testing
testing of the cryptographic module functionality as defined by the functional specification

3.49
hard / hardness
relative resistance of a metal or other material to denting, scratching, or bending; physically toughened; rugged, and durable

NOTE The relative resistances of the material to be penetrated by another object.

3. 50
hardware
physical equipment/components within the cryptographic boundary used to process programs and data

3.51
hardware module
module composed primarily of hardware, which may also contain firmware

3.52
hardware module interface
HMI
total set of commands used to request the services of the hardware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service

3.53
hash value
output of a cryptographic hash function

3.54
hybrid module
module whose cryptographic boundary delimits the composite of a software or firmware component and a disjoint hardware component

3.55
hybrid firmware module interface
HFMI
total set of commands used to request the services of the hybrid firmware module, including parameters that enter or leave the module’s cryptographic boundary as part of the requested service

3.56
hybrid software module interface
HSMI
total set of commands used to request the services of the hybrid software module, including parameters that enter or leave the module’s cryptographic boundary as part of the requested service

3.57
input data
information that is entered into a cryptographic module may be used for the purposes of transformation or computation using an approved security function

3.58
integrity
property that data has not been modified or deleted in an unauthorised and undetected manner

3.59
interface
logical entry or exit point of a cryptographic module that provides access to the module for logical information flows

3.60
ISO/IEC adopted
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

3.61
key agreement
SSP establishment procedure where the resultant key is a function of information by two or more participants, so that no party can predetermine the value of the key independently of the other party’s contribution using automated methods

3.62
key encryption key
KEK
cryptographic key that is used for the encryption or decryption of other keys

3.63
key loader
self-contained device that is capable of storing at least one plaintext or encrypted SSP or key component that can be transferred, upon request, into a cryptographic module

NOTE The use of a key loader requires human manipulation.

3.64
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

3.65
key transport
process of transferring a key from one entity to another entity using automated methods

3.66
limited operational environment
operational environment that is designed to accept only controlled firmware changes that successfully pass the software/firmware load test

3.67
low-level testing
testing of the individual components or group of components of the cryptographic module and their physical ports and logical interfaces

3.68
maintenance role
role assumed to perform physical maintenance and/or logical maintenance services

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

3.69
manual
requiring human operator manipulation

3.70
message authentication code
MAC
cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data

EXAMPLE A Hash Based Message Authentication Code

3.71
microcode
processor instructions that correspond to an executable program instruction

EXAMPLE Assembler code

3.72
minimum entropy
lower bound of entropy that is useful in determining a worst-case estimate of sample entropy

3.73
modifiable operational environment
operational environment that is designed to accept functional changes that may contain non-controlled software (i.e. untrusted)

3.74
multi-factor authentication
authentication with at least two independent authentication factors

NOTE 1 An authentication factor is a piece of information and process used to authenticate or verify the identity of an entity.

NOTE 2 Independent authentication factor categories are: something you know, something you have, and something you are.

3.75
multiple-chip embedded cryptographic module
physical embodiment in which two or more integrated circuit chips are interconnected and are embedded within an enclosure or a product that may not be physically protected

EXAMPLE Adapters and expansion boards

3.76
multiple-chip standalone cryptographic module
physical embodiment in which two or more integrated circuit chips are interconnected and the entire enclosure is physically protected

EXAMPLE Encrypting routers or secure radios

3.77
non-administrator guidance
written material that is used by the user and/or other non-administrative roles for operating the cryptographic module in an approved mode of operation

NOTE The non-administrator guidance describes the security functions of the cryptographic module and contains information and procedures for the secure use of the cryptographic module, including instructions, guidelines, and warnings.

3.78
non-invasive attack
attack that can be performed on a cryptographic module without direct physical contact with components within the cryptographic boundary of the module

NOTE An attack that does not alter or change the state of the cryptographic module.

3.79
non-modifiable operational environment
operational environment that is designed to not accept firmware changes

3.80
non-security relevant
implemented in a manner to not interfere or compromise the approved secure operation of the cryptographic module

3.81
normal operation
operation where the entire set of algorithms, security functions, services or processes are available and/or configurable

3.82
opaque
impenetrable by light (i.e. light within the visible spectrum of wavelength range of 400nm to 750nm); neither transparent nor translucent within the visible spectrum

3.83
operational environment
set of all software and hardware consisting of an operating system and hardware platform required for the module to operate securely

3.84
operational state
state where services or functions can be requested by an operator and the data results output from the cryptographic module’s data output interface

3.85
operator
individual or a process (subject) operating on behalf of the individual, authorised to assume one or more roles

3.86
output data
information or computed results produced by a cryptographic module

3.87
passivation
effect of a reactive process in semiconductor junctions, surfaces or components and integrated circuits constructed to include means of detection and protection

EXAMPLE Silicon dioxide or phosphorus glass

NOTE Passivation can modify the behaviour of the circuit. Passivation material is technology dependant.

3.88
password
string of characters used to authenticate an identity or to verify access authorisation

EXAMPLE Letters, numbers, and other symbols

3.89
personal identification number
PIN
numeric code used to authenticate an identity

3.90
physical protection
safeguarding of a cryptographic module, CSPs and PSPs using physical means

3.91
plaintext key
unencrypted cryptographic key or a cryptographic key obfuscated by non-approved methods which is considered unprotected

3.92
port
physical/logical input or output point of a cryptographic module that provides access to the module

3.93
pre-operational self-test
test performed by a cryptographic module between the time a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc.) and transitions to the operational state

3.94
private key
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.

3.95
production-grade
product, component or software that has been tested to meet operational specifications

3.96
public key
key of an entity's asymmetric key pair, which can be made public

NOTE 1 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 can only be available to all members of a pre-specified group.

NOTE 2 For the purposes of this International Standard, public keys are not considered CSPs.

3.97
public key certificate
public key information of an entity signed by an appropriate certification authority and thereby rendered unforgeable

3.98
public key (asymmetric) cryptographic algorithm
cryptographic algorithm that uses two related keys, a public key and a private key

NOTE The two keys have the property that deriving the private key from the public key is computationally infeasible.

3.99
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, one time passwords associated with a counter and internally held date and time

NOTE A PSP is considered protected if it cannot be modified or if its modification can be determined by the module.

3.100
random bit generator
RBG
device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased

3.101
removable cover
physical means which permits an intentionally designed non-damaging access to the physical contents of a cryptographic module

3.102
role
security attribute associated to a user defining the user access rights or limitations to services of a cryptographic module

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

3.103
role-based access control
RBAC
permissions attributed to a role granting access to an object

3.104
runtime environment
virtual machine state which provides software services for processes or programs while a computer is running

NOTE It can pertain to the operating system itself, or the software that runs beneath it. The primary purpose is to accomplish the objective of "platform independent" programming.

3.105
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

3.106
security function
cryptographic algorithms together with modes of operation, such as block ciphers, stream ciphers, symmetric or asymmetric key algorithms, message authentication codes, hash functions, or other security functions, random bit generators, entity authentication and SSP generation and establishment all approved either by ISO/IEC or an approval authority

NOTE See Annex C

3.107
seed key
secret value used to initialise a random bit generator

3.108
self-test
pre-operational or conditional test executed by the cryptographic module

3.109
sensitive data
data that, in user’s view, requires protection

3.110
sensitive security parameters
SSP
critical security parameters (CSP) and public security parameters (PSP)

3.111
service
any externally operator invoked operation and/or function that can be performed by a cryptographic module

3.112
service input
all data or control information utilised by the cryptographic module that initiates or obtains specific operations or functions

3.113
service output
all data and status information that results from operations or functions initiated or obtained by service input

3.114
simple power analysis
SPA
direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), in relation to the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to a cryptographic operation

3.115
single-chip cryptographic module
physical embodiment 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

EXAMPLE Single integrated circuit (IC) chips or smart cards with a single IC chip

3.116
software
executable code of a cryptographic module that is stored on erasable media which can be dynamically written and modified during execution while operating in a modifiable operational environment

EXAMPLE Erasable media can include but not limited to solid state memory, hard drives, etc.

3.117
software module
module that is composed solely of software

3.118
software/firmware load test
set of tests performed on software or firmware which has to pass successfully before it can be executed by a cryptographic module

NOTE Not applicable if the software or firmware is a complete image replacement and executed only after module power cycling

3.119
software/firmware module interface
SFMI
set of commands used to request the services of the software or firmware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service

3.120
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

NOTE All or a subset of the components can be required to perform the combination.

3.121
SSP establishment
process of making available a shared SSP to one or more entities

NOTE SSP establishment includes SSP agreement, SSP transport and SSP entry or output.

3.122
status information
information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module

3.123
strong
not easily defeated, having strength or power greater than average or expected, able to withstand attack or solidly built

3.124
symmetric cryptographic technique
cryptographic technique that uses the same secret key for both the encryption and the decryption transformations

3.125
tamper detection
automatic determination by a cryptographic module that an attempt has been made to compromise the security of the module

3.126
tamper evidence
observable indication that an attempt has been made to compromise the security of a cryptographic module

3.127
tamper response
automatic action taken by a cryptographic module when tamper detection has occurred

3.128
trust anchor
trusted information, which includes a public key algorithm, a public key value, an issuer name, and optionally, other parameters

EXAMPLE Other parameters can include but not limited to a validity period

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

3.129
trusted channel
trusted and safe communication link established between the cryptographic module and a sender or receiver to securely communicate unprotected plaintext CSPs, key components and authentication data

NOTE A trusted channel protects against eavesdropping, as well as physical or logical tampering by unwanted operators/entities, processes or other devices, between the module's defined input or output ports and along the communication link with the intended endpoint.

3.130
user
role taken by an individual or process (i.e. subject) acting on behalf of an individual that accesses a cryptographic module in order to obtain cryptographic services

3.131
validated
assurance of tested conformance by a validation authority

3.132
validation authority
entity that will validate the testing results for conformance to this International Standard

3.133
vendor
entity, group or association that submits the cryptographic module for testing and validation

NOTE The vendor has access to all relevant documentation and design evidence regardless if they did or did not design or develop the cryptographic module.

3.134
zeroisation
method of destruction of stored data and unprotected SSPs to prevent retrieval and reuse

4 Abbreviated terms

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

API	Application Program Interface
CBC	Cipher Block Chaining
CCM	Counter with Cipher block chaining-Message authentication code
ECB	Electronic Codebook
HDL	Hardware Description Language
IC	Integrated Circuit
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
URL	Uniform Resource Locator

5 Cryptographic module security levels

The following subclauses 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*. The cryptographic techniques are identical over the four security levels. Each security level levies increasing levels of security requirements for the protection of the module itself (e.g. access and knowledge of internal components and operation) and SSPs contained and controlled within the module. Each security requirement is identified by a **shall [xx.yy]** where **xx** indicates the clause and **yy** is a numeric index within the clause.

5.1 Security Level 1

Security Level 1 provides a baseline level of security. Basic security requirements are specified for a cryptographic module (e.g. at least one approved security function or approved sensitive security parameter establishment method shall be used). Software or firmware modules may operate in a non-modifiable, limited or modifiable operating environment. No specific physical security mechanisms are required in a Security Level 1 hardware cryptographic module beyond the basic requirement for production-grade components. Non-invasive mitigation methods or mitigation of other attacks which are implemented are documented. Examples of a Security Level 1 cryptographic module is a hardware encryption board found in a personal computer (PC) or a cryptographic toolkit executing in a handheld device or general purpose computer.

Such implementations are ideally appropriate for security applications where controls, such as physical security, network security, and administrative procedures are provided outside of the module but within the environment which it is to be deployed. For example, the implementation of Security Level 1 cryptographic module may be more cost-effective in such environments than corresponding modules at higher assurance levels which provide greater security of the modules SSPs, enabling organizations to select alternative cryptographic solutions to meet security requirements where attention to the environment the module is operating is crucial in providing overall security.

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 SSPs 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 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 a software cryptographic module to be executed in a modifiable environment that implements role-based access controls or, at the minimum, a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions through access control lists (e.g. ACLs), and with the capability of assigning each user to more than one group, and that protects against unauthorised execution, modification, and reading of cryptographic software.

5.3 Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 provides additional requirements to mitigate the unauthorised access to SSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at direct physical access, use or modification of the cryptographic module and probing through ventilation holes or slits. 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 manually established plaintext CSPs to be encrypted, utilise a trusted channel or use a split knowledge procedure for entry or output.

Security Level 3 also protects a cryptographic module against a security compromise due to environmental conditions 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 when the voltage and temperature boundaries are exceeded and zeroise CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected when outside of the normal operating range in a manner that can compromise the security of the module.

Non-invasive mitigation methods specified in 7.8 which are implemented in the module are tested at Security Level 3 metrics.

Security Level 3 is not offered in all clauses of this International Standard for software cryptographic modules, therefore, the overall highest security level achievable by software cryptographic module is limited to Security Level 2.

Security Level 3 modules require additional life-cycle assurances, such as automated configuration management, detailed design, low-level testing, and operator authentication using vendor-provided authentication information.

5.4 Security Level 4

Security Level 4 provides the highest level of security defined in this International Standard. This level includes all the appropriate security features of the lower levels, as well as extended features.

At Security Level 4, 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 SSPs 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 unprotected SSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 introduces the multi-factor authentication requirement for operator authentication. At minimum, this requires two of the following three attributes:

- something known, such as a secret password,

- something possessed, such as a physical key or token,

- a physical property, such as a biometric.

At Security Level 4 a cryptographic module is required to include special environmental protection features designed to detect voltage and temperature boundaries and zeroise all unprotected SSPs to provide a reasonable assurance that the module will not be affected when outside of the normal operating range in a manner that can compromise the security of the module.

Non-invasive mitigation methods specified in 7.8 which are implemented in the module are tested at Security Level 4 metrics.

Security Level 4 is not offered in all clauses of this International Standard for software cryptographic modules, therefore, the overall maximum security level achievable by software cryptographic modules is limited to Security Level 2.

The design of a Security Level 4 module is verified by the correspondence between both pre- and post-state conditions and the functional specification.

6 Functional security objectives

The security requirements specified in this International Standard relate to the secure design and implementation of a cryptographic module. The security requirements start with a baseline level of security objectives with increasing levels of security objectives. 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;
- prevent the unauthorised and undetected modification of the cryptographic module and cryptographic algorithms, including the unauthorised modification, substitution, insertion, and deletion of SSPs;
- 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;
- detect errors in the operation of the module and to prevent the compromise of SSPs resulting from these errors; and
- ensure the proper design, distribution and implementation of the cryptographic module.

7 Security requirements

7.1 General

This clause specifies the security requirements that **shall [01.01]** be satisfied by the 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; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operational environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks.

Table 1 summarises the security requirements in each of these areas.

A cryptographic module **shall [01.02]** be tested against the requirements of each area addressed in this clause. The cryptographic module **shall [01.03]** 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 highest 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 rating.

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

Many of the security requirements of this International Standard include specific documentation requirements that are summarised in Annexes A and B. All documentation, including copies of the user and installation manuals, design specifications, life-cycle documentation **shall [01.04]** be provided for a cryptographic module that is to undergo an independent verification or evaluation scheme.

Annexes C, D, E, and F provide references to approved security functions, approved sensitive security parameter establishment methods, approved authentication mechanisms and non-invasive attack mitigation test methods.

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 security functions, and normal and degraded modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. All services provide status information to indicate when the service utilises an approved cryptographic algorithm, security function or process in an approved manner.			
Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Trusted channel.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	Multi-factor authentication.
Software/Firmware Security	Approved integrity technique, or EDC based integrity test. Defined SFMI, HFMI and HSMI. Executable code.	Approved digital signature or keyed message authentication code- based integrity test.	Approved digital signature based integrity test.	
Operational Environment	Non-Modifiable, Limited or Modifiable. Control of SSPs.	Modifiable. Role-based or discretionary access control. Audit mechanism.		
Physical Security	Production-grade components.	Tamper evidence. Opaque covering or enclosure.	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing. EFP or EFT.	Tamper detection and response envelope. EFP. Fault injection mitigation.
Non-Invasive Security	Module is designed to mitigate against non-invasive attacks specified in Annex F.			
	Documentation and effectiveness of mitigation techniques specified in Annex F.		Mitigation Testing.	Mitigation Testing.
Sensitive Security Parameter Management	Random bit generators, SSP generation, establishment, entry and output, storage and zeroisation.			
	Automated SSP transport or SSP agreement using approved methods.			
	Manually established SSPs may be entered or output in plaintext form.		Manually established SSPs may be entered or output in either encrypted form, via a trusted channel or using split knowledge procedures.	
Self-Tests	Pre-operational: software/firmware integrity, bypass, and critical functions test.			
	Conditional: cryptographic algorithm, pair-wise consistency, software/firmware loading, manual entry, conditional bypass and critical functions test.			

		Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Life-Cycle Assurance	**Configuration Management**	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle.		Automated configuration management system.	
	Design	Module designed to allow testing of all provided security related services.			
	FSM	Finite state model.			
	Development	Annotated source code, schematics or HDL.	Software high-level language. Hardware high-level descriptive language.		Documentation annotated with pre- conditions upon entry into module components and post-conditions expected to be true when components is completed.
	Testing	Functional Testing.		Low-level Testing.	
	Delivery and Operation	Initialisation procedures.	Delivery Procedures.		Operator authentication using vendor provided authentication information.
	Guidance	Administrator and non-administrator guidance.			
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.

7.2 Cryptographic module specification

7.2.1 Cryptographic module specification general requirements

A cryptographic module **shall [02.01]** be a set of hardware, software, firmware, or some combination thereof, that at a minimum, implements a defined cryptographic service employing an approved cryptographic algorithm, security function or process and contained within a defined cryptographic boundary.

The documentation requirements specified in A.2.2 **shall [02.02]** be provided.

7.2.2 Types of cryptographic modules

A cryptographic module **shall [02.03]** be defined as one of the following module types:

— ***Hardware module*** is a module whose cryptographic boundary is specified at a hardware perimeter. Firmware and/or software, which may also include an operating system, may be included within this hardware cryptographic boundary.

— ***Software module*** is a module whose cryptographic boundary delimits the software exclusive component(s) (may be one or multiple software components) that execute(s) in a modifiable operational environment. The computing platform and operating system of the operational environment which the software executes in are external to the defined software module boundary.

— ***Firmware module*** is a module whose cryptographic boundary delimits the firmware exclusive component(s) that execute(s) in a limited or non-modifiable operational environment. The computing platform and operating system of the operational environment which the firmware executes in are external to the defined firmware module boundary but explicitly bound to the firmware module.

— ***Hybrid Software module*** is a module whose cryptographic boundary delimits the composite of a software component and a disjoint hardware component (i.e. the software component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment which the software executes in are external to the defined hybrid software module boundary.

— ***Hybrid Firmware module*** is a module whose cryptographic boundary delimits the composite of a firmware component and a disjoint hardware component (i.e. the firmware component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment which the firmware executes in are external to the defined hybrid firmware module boundary but explicitly bound to the hybrid firmware module.

For hardware and firmware modules, the applicable physical security and non-invasive security requirements found in 7.7 and 7.8 **shall [02.04]** apply.

For software modules executing in a modifiable environment, the physical security requirements found in 7.7 are optional and the applicable non-invasive security requirements in 7.8 **shall [02.05]** apply.

For hybrid modules, all applicable requirements of 7.5, 7.6, 7.7 and 7.8 **shall [02.06]** apply.

7.2.3 Cryptographic boundary

7.2.3.1 Cryptographic boundary general requirements

A cryptographic boundary **shall [02.07]** consist of an explicitly defined perimeter (i.e. set of hardware, software or firmware components) that establishes the boundary of all components of the cryptographic module. The requirements of this International Standard **shall [02.08]** apply to all algorithms, security functions, processes and components within the module's cryptographic boundary. The cryptographic boundary **shall [02.09]**, at a minimum, encompass all security relevant algorithms, security functions, processes and components of a cryptographic module (i.e. security relevant within the scope of this International Standard). Non-security relevant algorithms, security functions, processes or components may be included within the cryptographic boundary. Non-security relevant algorithms, security functions, processes or components may also be used in an approved mode of operation. Non-security relevant algorithms, security functions, processes or components which are used in an approved mode of operation **shall [02.10]** be implemented in a manner to not interfere or compromise the approved operation of the cryptographic module.

The defined name of a cryptographic module **shall [02.11]** be representative of the composition of the components within the cryptographic boundary and not representative of a larger composition or product. The cryptographic module **shall [02.12]** have, at minimum, specific versioning information representing the distinct individual hardware, software and/or firmware components.

Hardware, software and/or firmware components within the cryptographic boundary may be excluded from the requirements of this International Standard. The excluded hardware, software or firmware components **shall [02.13]** be implemented in a manner to not interfere or compromise the approved secure operation of the cryptographic module. The excluded hardware, software or firmware **shall [02.14]** be specified (Annex A).

7.2.3.2 Definitions of cryptographic boundary

The cryptographic boundary of a **hardware cryptographic module** **shall [02.15]** delimit and identify:

- The set of hardware components which may include:
  - physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between components,
  - active electrical components such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc.
  - physical structures, such as enclosures, potting or encapsulation materials, connectors, and interfaces,
  - firmware, which may include an operating system,
  - other components types not listed above.

The cryptographic boundary of a **software cryptographic module** **shall [02.16]** delimit and identify:

- The set of executable file or files that constitute the cryptographic module; and
- The instantiation of the cryptographic module saved in memory and executed by one or more processors.

The cryptographic boundary of a **firmware cryptographic module** **shall [02.17]** delimit and identify:

- The set of executable file or files that constitute the cryptographic module; and
- The instantiation of the cryptographic module saved in memory and executed by one or more processors.

The cryptographic boundary of a **hybrid cryptographic module** **shall [02.18]**:

- be the composite of the module's hardware component boundary and the disjoint software or firmware component(s) boundary; and
- include the collection of all ports and interfaces from each component.

  In addition to the disjoint software or firmware component(s), the hardware component can also include embedded software or firmware.

7.2.4 Modes of operations

7.2.4.1 Modes of operations general requirements

The operator **shall [02.19]** be able to operate the module in an approved mode of operation. An approved mode of operation **shall [02.20]** be defined as the set of services which include at least one service that utilises an approved cryptographic algorithm, security function or process and those services or processes specified in 7.4.3.

Non-approved cryptographic algorithms, security functions, and processes or other services not specified in 7.4.3 **shall [02.21]** not be utilised by the operator in an approved mode of operation unless the non-approved cryptographic algorithm or security function is part of an approved process and is not security relevant to the approved processes operation (e.g. a non-approved cryptographic algorithm or non-approved generated key may be used to obfuscate data or CSPs but the result is considered unprotected plaintext and provides no security relevant functionality until protected with an approved cryptographic algorithm).

7.2.4.2 Normal operation

Normal operation is where the entire set of algorithms, security functions, services or processes are available and/or configurable.

CSPs **shall [02.22]** be exclusive between approved and non-approved services and modes of operation (e.g. not shared or accessed). The output of an approved RBG may be provided to a non-approved algorithm, security function or process without the zeroisation of the RBG seed as long as the seed cannot be accessed in the non-approved mode.

The module's security policy **shall [02.23]** define the complete set of services that are provided for each defined mode of operation (both approved and non-approved).

All services **shall [02.24]** provide an indicator when the service utilises an approved cryptographic algorithm, security function or process in an approved manner and those services or processes specified in 7.4.3.

7.2.4.3 Degraded operation

A cryptographic module may be designed to support degraded functionality if the module enters the error state. For a cryptographic module to operate in degraded operation, the following **shall [02.25]** apply:

- degraded operation **shall [02.26]** be entered only after exiting an error state;
- the module **shall [02.27]** provide status information when re-configured and degraded operation entered;
- the mechanism or function that failed **shall [02.28]** be isolated;
- all conditional algorithm self-tests **shall [02.29]** be performed prior to the first operational use of the cryptographic algorithm after entering degraded operation; and
- services **shall [02.30]** provide an indicator if attempts are made to use a non-operational algorithm, security function, or process.

The cryptographic module **shall [02.31]** remain in degraded operation until such time the cryptographic module passes without failure all pre-operational self-tests successfully. The cryptographic module may perform certain diagnostics in addition to all pre-operational self-tests, as part of the condition to exit the degraded operation. If the cryptographic module fails the pre-operational self-tests, the module **shall not [02.32]** enter degraded operation.

7.3 Cryptographic module interfaces

7.3.1 Cryptographic module interfaces general requirements

A cryptographic module **shall [03.01]** restrict all logical information flow to only those physical access points and logical interfaces that are identified as entry and exit points to and from the cryptographic boundary of the module. The cryptographic module logical interfaces **shall [03.02]** be distinct 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 interface(s).

The documentation requirements specified in A.2.3 **shall [03.03]** be provided.

7.3.2 Types of interfaces

- *Hardware Module Interface (HMI):* The total set of interfaces used to request the services of the hardware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

- *Software* or *Firmware Module Interface (SFMI):* The total set of interfaces used to request the services of the software or the firmware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

- *Hybrid Software* or *Hybrid Firmware Module Interface (HSMI or HFMI):* The total set of interfaces used to request the services of the hybrid software or hybrid firmware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

7.3.3 Definition of interfaces

A cryptographic module **shall [03.04]** have the following five interfaces ("input" and "output" are indicated from the perspective of the module):

a) *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, SSPs, and status information from another module) **shall [03.05]** enter via the "data input" interface. Data may be accepted by the module through the data input interface while the module is performing self-tests (7.10).

b) *Data output interface*. All data (except status data output via the status output interface and control data output via the control output interface) that is output from a cryptographic module (including plaintext data, ciphertext data, and SSPs) **shall [03.06]** exit via the "data output" interface. All data output via the "data output" interface **shall [03.07]** be inhibited while performing manual entry, pre-operational self-tests, software/firmware loading and zeroisation; or when the cryptographic module is in an error state.

c) *Control input interface*. All input commands, signals (e.g clock input), 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 [03.08]** enter via the "control input" interface.

d) *Control output interface*. All output commands, signals, and control data (e.g. control commands to another module) used to control or indicate the state of operation of a cryptographic module **shall [03.09]** exit via the "control output" interface. All control output via the "control output" interface **shall [03.10]** be inhibited when the cryptographic module is in an error state unless exceptions are specified and documented in the security policy.

e) *Status output interface*. All output signals, indicators (e.g. error indicator), and status data (including return codes and physical indicators such as visual (display, indicator lamps), audio (buzzer, tone, ring), and mechanical (vibration)) used to indicate the status of a cryptographic module **shall [03.11]** exit via the "status output" interface. Status output may be either implicit or explicit.

Except for the software cryptographic modules, all modules **shall [03.12]** also have the following interface:

f) *Power interface*. All external electrical power that is input to a cryptographic module **shall [03.13]** enter via a power interface. A power interface is not required when all power is provided or maintained internally within the cryptographic boundary of the cryptographic module (e.g. an internal battery).

The cryptographic module **shall [03.14]** distinguish between data, control information, and power for input, and data, control information, status information, and power for output.

The cryptographic module specification **shall [03.15],** unambiguously, specify format of input data and control information, including length restrictions for all variable length inputs.

7.3.4 Trusted channel

A trusted channel is a link established between the cryptographic module and a sender or receiver to securely communicate unprotected plaintext CSPs, key components and authentication data. A trusted channel protects against eavesdropping, as well as physical or logical tampering by unwanted operators/entities, processes or other devices, between the module's defined input or output ports and along the communication link with the intended sender or receiver endpoint.

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, there are no requirements for a trusted channel.

SECURITY LEVEL 3

For Security Level 3,

- for the transmission of unprotected plaintext CSPs, key components and authentication data between the cryptographic module and the sender or receivers endpoint the cryptographic module **shall [03.16]** implement a trusted channel;
- the trusted channel **shall [03.17]** prevent unauthorised modification, substitution, and disclosure along the communication link;
- the physical ports used for the trusted channel **shall [03.18]** be physically separated from all other ports or the logical interfaces used for the trusted channel **shall [03.19]** be logically separated from all other interfaces;
- identity-based authentication **shall [03. 20]** be employed for all services utilising the trusted channel; and
- a status indicator **shall [03.21]** be provided when the trusted channel is in use.

SECURITY LEVEL 4

In addition to the requirements of Security Level 3, for Security Level 4 multi-factor identity-based authentication **shall [03.22]** be employed for all services utilising the trusted channel.

7.4 Roles, services, and authentication

7.4.1 Roles, services, and authentication general requirements

A cryptographic module **shall [04.01]** 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 [04.02]** 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.

The documentation requirements specified in A.2.4 **shall [04.03]** be provided.

7.4.2 Roles

A cryptographic module **shall [04.04], at a minimum,** support a *Crypto Officer Role*. The *Crypto Officer Role* **shall [04.05]** be assumed to perform cryptographic initialisation or management functions, and general security services (e.g. module initialisation, management of CSPs, PSPs, and audit functions).

A cryptographic module may support a *User Role*. If the cryptographic module supports a *User Role*, then the *User Role* **shall [04.06]** be assumed to perform general security services, including cryptographic operations and other approved security functions.

A cryptographic module may support a *Maintenance Role*. The *Maintenance Role* is a role assumed during the physical and/or logical maintenance services (e.g. opening service covers, performing certain diagnostics such as built in self-test (BIST)). All unprotected SSPs **shall [04.07]** be zeroised when entering or exiting the Maintenance Role.

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

7.4.3 Services

7.4.3.1 Services general requirements

Services **shall [04.08]** refer to all of the services, operations, or functions that can be performed by a module. *Service inputs* **shall [04.09]** consist of all data or control inputs to the module that initiate or obtain specific services, operations, or functions. *Service outputs* **shall [04.10]** consist of all data outputs, control outputs, and status outputs that result from services, operations, or functions initiated or obtained by service inputs. Each service input **shall [04.11]** result in a service output.

A cryptographic module **shall [04.12]** provide the following services to operators.

a) *Show module's versioning information.* The cryptographic module **shall [04.13]** output the name or module identifier and the versioning information that can be correlated with a validation record (e.g. hardware, software and/or firmware versioning information).

b) *Show status.* The cryptographic module **shall [04.14]** output current status. This may include the output of status indicators in response to a service request.

c) *Perform self-tests.* The cryptographic module **shall [04.15]** initiate and run the pre-operational self-tests as specified in 7.10.2.

d) *Perform approved security functions.* The cryptographic module **shall [04.16]** perform at least one approved security function used in an approved mode of operation as specified in 7.2.

e) *Perform zeroisation.* The cryptographic module **shall [04.17]** perform zeroisation of the parameters as specified in 7.9.7.

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).

7.4.3.2 Bypass capability

Bypass capability is the ability of a service to partially or wholly circumvent a cryptographic function or process. If the module can output a particular data or status item in a cryptographically protected form, or (as a result of module configuration or operator intervention) can also output the item in a non-protected form, then a bypass capability **shall [04.18]** be defined.

If a cryptographic module implements a *bypass* capability, then:

a) the operator **shall [04.19]** assume an authorised role before configuring the bypass capability;

b) two independent internal actions **shall [04.20]** be required to activate the capability to prevent the inadvertent bypass of plaintext data due to a single error. The two independent internal actions **shall [04.21]** modify software and/or hardware behaviour that is dedicated to mediate the bypass capability (e.g. two different software or hardware flags are set, one of which may be user-initiated); and

c) the module **shall [04.22]** 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); or

   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).

7.4.3.3 Self-Initiated cryptographic output capability

Self-initiated cryptographic output capability is the ability of the module to perform cryptographic operations and other approved security functions or SSP management techniques without external operator request. The self-initiated cryptographic output capability **shall [04.23]** be configured by the Crypto Officer and this configuration may be preserved over resetting, rebooting, or power cycling of the module.

If a cryptographic module implements a *self-initiated cryptographic output* capability, then:

— two independent internal actions **shall [04.24]** be required to activate the capability to prevent the inadvertent output due to a single error. The two independent internal actions **shall [04.25]** modify software and/or hardware behaviour that is dedicated to mediate the capability (e.g. two different software or hardware flags are set, one of which may be user-initiated); and

— the module **shall [04.26]** show status to indicate whether the self-initiated cryptographic output capability is activated.

7.4.3.4 Software/Firmware loading

If a cryptographic module has the capability of loading software or firmware from an external source, then the following requirements **shall [04.27]** apply:

— the loaded software or firmware **shall [04.28]** be validated by a validation authority prior to loading to maintain validation;

— all data output via the data output interface **shall [04.29]** be inhibited until the software/firmware loading and load test has completed successfully;

— the *Software/Firmware Load Test* specified in 7.10.3.4 **shall [04.30]** be performed before the loaded code can be executed;

— the cryptographic module **shall [04.31]** withhold execution of any loaded or modified approved security functions until after the pre-operational self-tests specified in 7.10.2 have been successfully executed; and

— the modules versioning information **shall [04.32]** be modified to represent the addition and/or update of the newly loaded software or firmware (7.4.3).

If the loading of new software or firmware is a complete image replacement, this **shall [04.33]** constitute an entirely new module which would require validation by a validation authority to maintain validation. The new software or firmware image **shall [04.34]** only be executed after the module transitions through a power-on reset. All SSPs **shall [04.35]** be zeroised prior to execution of the new image.

7.4.4 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. The following types of mechanisms are used to control access to the cryptographic module:

a) *Role-Based Authentication*: If role-based authentication mechanisms are supported by a cryptographic module, the module **shall [04.36]** require that one or more roles either be implicitly or explicitly selected by the operator and **shall [04.37]** 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 [04.38]** authenticate the assumption of any role that was not previously authenticated for that operator.

b) *Identity-Based Authentication*: If identity-based authentication mechanisms are supported by a cryptographic module, the module **shall [04.39]** require that the operator be individually and uniquely identified, **shall [04.40]** require that one or more roles either be implicitly or explicitly selected by the operator, and **shall [04.41]** 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 the module **shall [04.42]** 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 cryptographic module is reset, rebooted, powered off and subsequently powered on, the module **shall [04.43]** require the operator to be 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 (e.g. biometrics). Authentication data within a cryptographic module **shall [04.44]** be protected against unauthorised use, disclosure, modification, and substitution. Approved security functions may be used as part of the authentication mechanism.

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 [04.45]** be used to control access to the module and initialise the authentication mechanisms. If default authentication data is used to control access to the module, then default authentication data **shall [04.46]** be replaced upon first-time authentication. This default authentication data does not need to meet the zeroisation requirements (7.9.7).

The authentication mechanism may be a group of mechanisms of different authentication properties that jointly meet the requirements of this clause. If the cryptographic module uses security functions to authenticate the operator, then those security functions **shall [04.47]** be approved security functions.

— The module **shall [04.48]** implement an approved authentication mechanism as referenced in Annex E.

- The strength of the approved authentication mechanism **shall [04.49]** be specified in the security policy (Annex B).
- For each attempt to use the approved authentication mechanism, the module **shall [04.50]** meet the strength of the authentication objective. For multiple attempts to use the approved authentication mechanism during a one-minute period, the module **shall [04.51]** meet the strength of the authentication objective.
- The approved authentication mechanism **shall [04.52]** be met by the module's implementation and not rely on documented procedural controls or security rules (e.g. password size restrictions).
- For a software cryptographic module at Security Level 2, the operating system may implement the authentication mechanism. If the operating system implements the authentication mechanism, then the authentication mechanism **shall [04.53]** meet the requirements of this clause.
- Feedback of authentication data to an operator **shall [04.54]** be obscured during the authentication process (e.g. no visible display of characters when entering a password). Non-significant characters may be displayed in place of the actual authentication data.
- Feedback provided to an operator during an attempted authentication **shall [04.55]** prevent weakening of the authentication mechanism strength beyond the required authentication strength.

SECURITY LEVEL 1

For 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 [04.56]** require that the operator either implicitly or explicitly select one or more roles.

SECURITY LEVEL 2

For Security Level 2, a cryptographic module **shall [04.57]** at a minimum employ *role-based* authentication to control access to the module*.*

SECURITY LEVEL 3

For Security Level 3, a cryptographic module **shall [04.58]** employ *identity-based* authentication mechanisms to control access to the module.

SECURITY LEVEL 4

For Security Level 4, a cryptographic module **shall [04.59]** employ *multi-factor identity-based* authentication mechanisms to control access to the module.

7.5 Software/Firmware security

A cryptographic module is defined as either a hardware, software, firmware or hybrid module (7.2.2). The requirements of this clause **shall [05.01]** apply to software and firmware components of a cryptographic module.

A cryptographic module that is implemented completely in hardware is not subject to the software/firmware security requirements of this International Standard.

The public verification key or keyed message authentication key used for an approved integrity technique may reside within the module code and is not considered a SSP.

The documentation requirements specified in A.2.5 **shall [05.02]** be provided.

SECURITY LEVEL 1

The following requirements **shall [05.03]** apply to software and firmware components of a cryptographic module for Security Level 1:

- All software and firmware **shall [05.04]** be in a form that satisfies the requirements of this International Standard without modification prior to installation (7.11.7);
- For software and firmware modules and the software or firmware component of a hybrid module (except for the software and firmware components within a disjoint hardware component of a hybrid module):
  - A cryptographic mechanism using an approved integrity technique **shall [05.05]** be applied to all software and firmware components within the module's defined cryptographic boundary in one of the following ways:
    - by the cryptographic module itself; or
    - by another validated cryptographic module operating in an approved mode of operation.
- For software and firmware components of a hardware cryptographic module and the software or firmware components within a disjoint hardware component of a hybrid cryptographic module:
  - A cryptographic mechanism using an approved integrity technique or an error detection code (EDC) **shall [05.06]** be applied to all software and firmware components within the hardware module's defined cryptographic boundary or within disjoint hardware components of the hybrid module. If an EDC is used, the EDC **shall [05.07]** be at least 16 bits in length.
- If the integrity test fails (i.e. the calculated result is not successfully verified or the EDC cannot be verified depending on the module type), the module **shall [05.08]** enter the error state. The approved integrity technique may consist of a single encompassing message authentication code or signature, or multiple disjoint authentication codes or signatures of which failure of any disjoint authentication code or signature **shall [05.09]** cause the module to enter the error state. The expected referenced output of the integrity technique mechanism may be considered data and itself not subject to the integrity technique. The temporary value(s) generated during the integrity test of the module's software or firmware **shall [05.10]** be zeroised from the module upon completion of the integrity test;
- An operator **shall [05.11]** be able to perform the integrity test on demand via an HMI, SFMI, HSMI or HFMI service (7.3.2);
- All data and control inputs, and data, control and status outputs (specified in 7.3.3) of the cryptographic module and services (7.4.3) **shall [05.12]** be directed through a defined HMI, SFMI, HFMI or HSMI; and
- For a software or firmware module, if the loaded software or firmware image is a complete replacement or overlay of the validated module image, the software/firmware load test is not applicable (NA) as the replacement or overlay constitutes a new module.

  If the software or firmware that is loaded is associated, bound, modifies or is an executable requisite of the validated module, then the software/firmware load test is applicable and **shall [05.13]** be performed by the validated module with the following exceptions:

  - The cryptographic module is a software module and the loaded software image is a complete image replacement or overlay of the validated module.
  - The cryptographic module is a firmware module of physical Security Level 1 and the loaded firmware image is a complete image replacement or overlay of the validated module.

- The cryptographic module is a hybrid software module and the loaded software image is a complete image replacement or overlay of the disjoint software components.
- The cryptographic module is a hybrid firmware module of physical Security Level 1 and the loaded firmware image is a complete image replacement or overlay of the disjoint firmware components.

SECURITY LEVEL 2

In addition to the requirements of Security Level 1, the following requirements **shall [05.14]** apply to software and firmware components of a cryptographic module for Security Level 2:

- The software and firmware components of a cryptographic module **shall [05.15]** only include code that is in executable form (e.g. no source code, object code or just-in-time compiled code);
- There **shall [05.16]** be no services or control settings via the HMI, SFMI, HFMI or HSMI interface to allow the operator to initiate or perform debugging techniques;
- For software and firmware modules and the software or firmware component of a hybrid module for Security Level 2 (except for the software and firmware components within a disjoint hardware component of a hybrid module):
  - An approved digital signature or keyed message authentication code **shall [05.17]** be applied to all software and firmware within the module's defined cryptographic boundary. If the calculated result is not successfully verified, the test fails and the module **shall [05.18]** enter the error state.

SECURITY LEVELS 3 AND 4

In addition to the requirements of Security Levels 1 and 2, the following requirements **shall [05.19]** apply to software and firmware modules and the software or firmware component of a hybrid module for Security Levels 3 and 4 (except for the software and firmware components within a disjoint hardware component of a hybrid module):

A cryptographic mechanism using an approved digital signature **shall [05.20]** be applied to all software and firmware components within the module's defined cryptographic boundary. If the calculated result is not successfully verified, the test fails and the module **shall [05.21]** enter the error state.

The digital signature technique may consist of a single encompassing signature or multiple disjoint signatures of which failure of any disjoint signature **shall [05.22]** cause the module to enter the error state. The private signing key **shall [05.23]** reside outside the module.

7.6 Operational environment

7.6.1 Operational environment general requirements

The operational environment of a cryptographic module refers to the management of the software, firmware, and/or hardware required for the module to operate. The operational environment of a software, firmware, or hybrid module includes, at a minimum, the module components, the computing platform, and the operating system that controls or allows the execution of the software or firmware on the computing platform. A hardware module may have an operating environment within the module consisting of an operating system which allows the execution of internal software or firmware. The operating system is considered to include, when applicable, the virtual machine(s) (system and/or process) and the runtime environment (e.g. Java Runtime Environment – JRE).

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 and also manages system and operator(s) processes/thread(s), including general-purpose application software such as word processors.

The operational environment can be *non-modifiable*, *limited* or *modifiable*.

The following clause specifies the three specific operational environments.

a) A ***non-modifiable operational environment*** is designed or configured in a manner to prevent modification by an operator or process to the module components, the computing platform, or the operating system. This environment may consist of a firmware module operating in a non-programmable computing platform or a hardware module which prevents the loading of any additional software or firmware.

b) A ***limited operational environment*** is designed or configured in a manner to allow controlled modification by an operator or process to the module components, the computing platform, or the operating system. This environment may be firmware operating in a programmable hardware module where the loading of additional firmware meets the firmware loading requirements specified in 7.4.3.4.

c) 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 operating system, configurable smartcard operating system, or programmable software). Operating systems are considered to be modifiable operational environments if software components can be modified by an operator or process and/or an operator or process can load and execute software (e.g. a word processor) that is not part of the defined software, firmware, or hybrid module.

   A modifiable operational environment has the following characteristics:

   Functions may be added or modified within the operational environment. Those functions are not necessarily trusted to not interfere with the operation of the cryptographic module unless such interference is prohibited by the operational environment.

   In such an environment it is required that no function operating in the same operational environment that does not belong to the trusted part of the operational environment have access to SSPs other than via the defined interfaces of the cryptographic module.

   It is therefore required that the operational environment provides the capability to separate the cryptographic module during operation from other functions in the operational environment such that those functions can neither obtain information from the cryptographic module related to the CSPs nor be able to modify CSPs, PSPs or the execution flow of the cryptographic module other than via the interfaces provided by the cryptographic module itself.

   A specific configuration of the operational environment may be required to achieve adequate protection of the cryptographic module with its code and data (e.g. prohibiting specific kind of inter-process communication for the cryptographic module, assigning restrictive access rights to files containing SSPs or the code of the cryptographic module).

Some examples of operational environments are provided in the following table.

Table 2: Examples of operational environments

Configuration Examples	Operational Environment
A computing platform that does not permit the loading of code and does not permit operators to modify the configuration of the computing platform, operating system or cryptographic module.	Non-Modifiable
A computing platform containing an operating system that allows the loading of additional code that is authenticated and meets all applicable requirements of this International Standard.	Limited

A computing platform that allows the loading of code without meeting the software or firmware loading requirements of this International Standard.	Modifiable
A computing platform containing code whose operating system is reconfigurable by the operator allowing the removal of the security protections.	Modifiable

For a *non-modifiable* or *limited* environment, the controlling components which maintain the *non-modifiable* or *limited* environment may include attributes of the computing platform, the operating system or the cryptographic module itself *or* all of the above.

Code which is executed in a *non-modifiable* or *limited* environment is referred to as *firmware* within this International Standard. Code which is executed in a *modifiable* environment is referred to as *software* within this International Standard.

If the operational environment is *non-modifiable* or a *limited* operational environment, only the operating system requirements in 7.6.2 **shall [06.01]** apply.

If the operational environment is a *modifiable* operational environment, the operating system requirements in 7.6.3 **shall [06.02]** apply.

The documentation requirements specified in A.2.6 **shall [06.03]** be provided.

7.6.2 Operating system requirements for limited or non-modifiable operational environments

SECURITY LEVEL 1

The requirements in 7.6.3 Security Level 1 **shall [06.04]** be applicable if the module is Security Level 1 in 7.7.

SECURITY LEVELS 2, 3, AND 4

There are no additional requirements.

7.6.3 Operating system requirements for modifiable operational environments

SECURITY LEVEL 1

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

— Each instance of a cryptographic module **shall [06.05]** have control over its own SSPs.

— The operational environment **shall [06.06]** provide the capability to separate individual application processes from each other in order to prevent uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless if this data is in the process memory or stored on persistent storage within the operational environment. This ensures that direct access to CSPs and SSPs is restricted to the cryptographic module and the trusted parts of the operational environment. Restrictions to the configuration of the operational environment **shall [06.07]** be documented in the security policy of the cryptographic module.

— Processes that are spawned by the cryptographic module **shall [06.08]** be owned by the module and are not owned by external processes/operators.

NOTE These requirements cannot be enforced by administrative documentation and procedures, but must be enforced by the cryptographic module itself.

SECURITY LEVEL 2

In addition to the requirements of Security Level 1, for Security Level 2 an operating environment **shall [06.09]** meet the following requirements or as allowed by the validation authority.

- all cryptographic software, SSPs, and control and status information **shall [06.10]** be under the control of an operating system that implements either role-based access controls or, at the minimum, a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions for example through access control lists (ACLs), and with the capability of assigning each user to more than one group. The operating system **shall [06.11]** be configured to protect against unauthorised execution, modification, and reading of SSPs, control and status data;

- to protect plaintext data, cryptographic software, SSPs, and authentication data, the access control mechanisms of the operating system:

  - **shall [06.12]** be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to execute the stored cryptographic software;

  - **shall [06.13]** be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to modify (i.e. write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data;

  - **shall [06.14]** be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to read cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data; and

  - **shall [06.15]** be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to enter SSPs.

  and

- the following specifications **shall [06.16]** be consistent with the roles or designated groups' rights and services as defined in the security policy:

  - when not supporting a maintenance role, the operating system **shall [06.17]** prevent all operators and running processes from modifying running cryptographic processes (i.e. loaded and executing cryptographic program images). In this case, running processes refer to all processes, cryptographic or not, not owned or initiated by the operating system (i.e. operator-initiated);

  - the operating system shall **[06.18]** prevent user processes from gaining either read or write access to SSPs owned by other processes and to system SSPs; and

  - the configuration of the operating system that meets the above requirements shall **[06.19]** be specified in the Administrator Guidance. The Administrator Guidance shall **[06.20]** state that the operating system must be configured as specified for the module contents to be considered protected.

The identification and authentication mechanism to the operating system **shall [06.21]** meet the requirements of 7.4.3 and be specified in the module's security policy.

All cryptographic software, SSPs, control and status information **shall [06.22]** be under the control of:

- an operating system which **shall [06.23]** have, at a minimum, the following attributes:

- the operating system **shall [06.24]** provide an audit mechanism with the date and time of each audited event. The cryptographic module **shall [06.25]** not include SSPs as part of any audit record;
- the cryptographic module **shall [06.26]** provide the following events to be recorded by the audit mechanism of the operating system:
  - modifications, accesses, deletions, and additions of cryptographic data and SSPs;
  - attempts to provide invalid input for Crypto Officer functions;
  - addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by the cryptographic module);
  - the use of a security-relevant Crypto Officer function;
  - requests to access authentication data associated with the cryptographic module;
  - the use of an authentication mechanism (e.g. login) associated with the cryptographic module; and
  - explicit requests to assume a Crypto Officer role.
- the audit mechanism of the operating system **shall [06.27]** be capable of auditing the following operating system related events:
  - all operator read or write accesses to audit data stored in the audit trail;
  - access to files used by the cryptographic module to store cryptographic data or SSPs;
  - addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by operational environment);
  - requests to use authentication data management mechanisms;
  - attempts to use the trusted channel function and whether the request was granted, when trusted channel is supported at this security level; and
  - identification of the initiator and target of a trusted channel, when trusted channel is supported at this security level.
- the operating system **shall [06.28]** be configured to prevent operators other than those with the privileges identified in the security policy from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.

Only operating systems that are configured to meet the above security requirements **shall [06.29]** be permitted at this security level, whether or not the cryptographic module operates in an approved mode of operation. The audit record should be protected against unauthorised modification through the use of an approved security function.

7.7 Physical security

7.7.1 Physical security embodiments

A cryptographic module **shall [07.01]** 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, data components and SSPs within the cryptographic boundary **shall [07.02]** be protected.

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

The requirements of this clause **shall [07.03]** be applicable to hardware and firmware modules, and hardware and firmware components of hybrid modules.

The requirements of this clause **shall [07.04]** be applicable at the defined physical boundary of the module.

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

a) ***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.

b) ***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.

c) ***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, secure radios or USB tokens.

Depending on the physical security mechanisms of a cryptographic module, unauthorised attempts at physical access, use, or modification **shall [07.05]** have a high probability of being detected:

— subsequent to an attempt by leaving visible signs (i.e. tamper evidence);

and/or

— during an access attempt

and appropriate immediate actions **shall [07.06]** be taken by the cryptographic module to protect CSPs.

Table 3 summarises 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.

Table 3: Summary of physical security requirements for cryptographic modules

	General Requirements for all Embodiments	**Single-Chip**	**Multiple-Chip Embedded**	**Multiple-Chip Standalone**
Security Level 1	Production-grade components. Standard passivation. Procedural or automatic zeroisation when accessing the maintenance access interface.	No additional requirements.	Production-grade enclosure or removable cover.	Production-grade enclosure or removable cover.

	General Requirements for all Embodiments	Single-Chip	Multiple-Chip Embedded	Multiple-Chip Standalone
Security Level 2	Evidence of tampering. Opaque or translucent within the visible spectrum. Prevent direct observation through holes and slits.	Tamper-evident coating on chip or enclosure.	Tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Tamper response and zeroisation circuitry. Automatic zeroisation when accessing the maintenance access interface. Prevent probing through holes are slits. EFP or EFT for temperature and voltage.	Hard tamper-evident coating on chip or strong removal-resistant and penetration resistant enclosure.	Hard tamper-evident encapsulating material or strong enclosure.	Hard tamper-evident encapsulating material or strong enclosure.
Security Level 4	Tamper detection and response envelope. EFP for temperature and voltage. Protection from fault induction.	Hard removal-resistant coating on chip.	Tamper detection and response envelope with zeroisation capability.	Tamper detection and response envelope with zeroisation capability.

In general, Security Level 1 provides a baseline set of requirements. Security Level 2 requires the addition of tamper-evident mechanisms and the inability to gather information about the internal operations of the critical areas of the module (opaqueness). Security Level 3 adds requirements for the use of strong or hard conformal or non-conformal enclosures with tamper detection and response mechanisms for removable covers and doors and resistance to direct probing via openings or entry points. Environmental failure protection (EFP) or environmental failure testing (EFT) is required at Security Level 3. Security Level 4 adds requirements for the use of strong or hard conformal or non-conformal enclosures with tamper detection and response mechanisms for the entire enclosure or significant damage. Environmental failure protection (EFP) and protection from fault induced attacks are required at Security Level 4.

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).

Tamper detection and tamper response are not substitutes for tamper evidence.

The documentation requirements specified in A.2.7 **shall [07.07]** be provided.

7.7.2 Physical security general requirements

The following requirements **shall [07.08]** apply to all physical embodiments:

— documentation **shall [07.09]** specify the physical embodiment and the security level for which the physical security mechanisms of a cryptographic module are implemented;

- whenever zeroisation is performed for physical security purposes, the zeroisation **shall [07.10]** occur in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time of detection and the actual zeroisation;

- 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:

  - a maintenance access interface **shall [07.11]** be defined;

  - the maintenance access interface **shall [07.12]** include all physical access paths to the contents of the cryptographic module, including any removable covers or doors; and

  - any removable covers or doors included within the maintenance access interface **shall [07.13]** be safeguarded using the appropriate physical security mechanisms.

SECURITY LEVEL 1

The following requirements **shall [07.14]** apply to all cryptographic modules for Security Level 1:

- the cryptographic module **shall [07.15]** consist of production-grade components that 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); and

- when performing physical maintenance, zeroisation **shall [07.16]** 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 [07.17]** apply to all cryptographic modules for Security Level 2:

- the cryptographic module **shall [07.18]** provide evidence of tampering (e.g. on the cover, enclosure, and seal) when physical access to the module is attempted;

- the tamper-evident material, coating or enclosure **shall [07.19]** either be opaque or translucent within the visible spectrum (i.e. light of wavelength range of 400nm to 750nm) to prevent the gathering of information about the internal operations of the critical areas of the module; and

- if the cryptographic module contains ventilation holes or slits, then the module **shall [07.20]** be constructed in a manner to prevent the gathering of information of the module's internal construction or components by direct visual observation using artificial light sources in the visual spectrum of the module's internal construction or components.

SECURITY LEVEL 3

In addition to the general requirements for Security Levels 1 and 2, the following requirements **shall [07.21]** apply to all cryptographic modules for Security Level 3:

- if the cryptographic module contains any doors or removable covers or if a maintenance access interface is defined, then the module **shall [07.22]** contain tamper response and zeroisation capability. The tamper response and zeroisation capability **shall [07.23]** immediately zeroise all unprotected SSPs when a door is opened, a cover is removed, or when the maintenance access interface is accessed. The tamper response and zeroisation capability **shall [07.24]** remain operational when unprotected SSPs are contained within the cryptographic module;

- if the cryptographic module contains ventilation holes or slits, then the module **shall [07.25]** be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g. prevent probing by a single articulated probe);

- strong or hard conformal or non-conformal enclosures, coatings or potting materials **shall [07.26]** maintain strength and hardness characteristics over the module's intended temperature range of operation, storage and distribution,

- if tamper evident seals are employed, they **shall [07.27]** be uniquely numbered or independently identifiable (e.g. uniquely numbered evidence tape or uniquely identifiable holographic seals), and

- the module **shall [07.28]** either include EFP features or undergo EFT.

SECURITY LEVEL 4

In addition to the general requirements for Security Levels 1, 2, and 3, the following requirement **shall [07.29]** apply to all cryptographic modules for Security Level 4:

- the cryptographic module **shall [07.30]** be protected either by a hard opaque removal-resistant coating, or by a tamper detection envelope with tamper response and zeroisation capability;

- the module **shall [07.31]** include EFP features; and

- the cryptographic module **shall [07.32]** provide protection from fault induction. The fault induction mitigation techniques and the mitigation metrics employed **shall [07.33]** be documented as specified in Annex B.

7.7.3 Physical security requirements for each physical security embodiment

7.7.3.1 Single-chip cryptographic modules

In addition to the general physical security requirements specified in 7.7.2, 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 [07.34]** apply to single-chip cryptographic modules for Security Level 2:

- the cryptographic module **shall [07.35]** 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.

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements **shall [07.36]** apply to single-chip cryptographic modules for Security Level 3:

- the module **shall [07.37]** be covered with a hard opaque tamper-evident coating (e.g. a hard opaque epoxy covering the passivation), or

- the enclosure **shall [07.38]** be implemented so that attempts at removal or penetration of the enclosure **shall [07.39]** have a high probability of causing serious damage to the cryptographic module (i.e. the module will not function).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements **shall [07.40]** apply to single-chip cryptographic modules for Security Level 4:

- the cryptographic module **shall [07.41]** 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); and

- the removal-resistant coating **shall [07.42]** 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).

7.7.3.2 Multiple-chip embedded cryptographic modules

In addition to the general security requirements specified in 7.7.2, 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 [07.43]** be used.

SECURITY LEVEL 2

In addition to the requirement for Security Level 1, the following requirements **shall [07.44]** apply to multiple-chip embedded cryptographic modules for Security Level 2:

- the module components **shall [07.45]** be covered with a tamper-evident coating or potting material (e.g. etch-resistant coating or bleeding paint) to deter direct observation and to provide evidence of attempts to tamper with or remove module components,

  or

- the module **shall [07.46]** be entirely contained within a metal or hard plastic production-grade enclosure that may include doors or removable covers;

and

- the enclosure includes any doors or removable covers, then the doors or covers **shall [07.47]** be locked with pick-resistant mechanical locks employing physical or logical keys or **shall [07.48]** 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 [07.49]** apply to multiple-chip embedded cryptographic modules for Security Level 3.

- the multiple-chip embodiment of the circuitry within the cryptographic module **shall [07.50]** be covered with a hard coating or potting material (e.g. a hard epoxy material),

or

- the module **shall [07.51]** 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).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements **shall [07.52]** apply to multiple-chip embedded cryptographic modules for Security Level 4:

- the module components **shall [07.53]** be within a strong or hard conformal or non-conformal enclosure. The enclosure **shall [07.54]** be 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 [07.55]** detect tampering by means such as cutting, drilling, milling, grinding, burning, melting, or dissolving of the potting material or enclosure to an extent sufficient for accessing SSPs; and

- the module **shall [07.56]** contain tamper response and zeroisation circuitry that **shall [07.57]** continuously monitor the tamper detection envelope and, upon the detection of tampering, **shall [07.58]** immediately zeroise all unprotected SSPs. The tamper response circuitry **shall [07.59]** remain operational when unprotected SSPs are contained within the cryptographic module.

7.7.3.3 Multiple-chip standalone cryptographic modules

In addition to the general security requirements specified in 7.7.2, the following requirements are specific to multiple-chip standalone cryptographic modules.

SECURITY LEVEL 1

The cryptographic module **shall [07.60]** 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 [07.61]** apply to multiple-chip standalone cryptographic modules for Security Level 2:

- if the enclosure of the cryptographic module includes any doors or removable covers, then the doors or covers **shall [07.62]** be locked with pick-resistant mechanical locks employing physical or logical keys or **shall [07.63]** 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 [07.64]** apply to multiple-chip standalone cryptographic modules for Security Level 3:

- the module **shall [07.65]** 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).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements **shall [07.66]** apply to multiple-chip standalone cryptographic modules for Security Level 4:

- the enclosure of the cryptographic module **shall [07.67]** contain a tamper detection envelope that use 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 in 7.7.3.2 Security Level 4. The tamper detection mechanisms **shall [07.68]** respond to attacks such as cutting, drilling, milling, grinding, burning, melting, or dissolving to an extent sufficient for accessing SSPs; and

- the cryptographic module **shall [07.69]** contain tamper response and zeroisation capability that **shall [07.70]** continuously monitor the tamper detection envelope and, upon the detection of tampering, **shall [07.71]** immediately zeroise all unprotected SSPs. The tamper response and zeroisation capability **shall [07.72]** remain operational when unprotected SSPs are contained within the cryptographic module.

7.7.4 Environmental failure protection/testing

7.7.4.1 Environmental failure protection/testing general requirements

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 and 2 a module is not required to employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT). At Security Level 3, a module **shall [07.73]** either employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT). At Security Level 4, a module **shall [07.74]** employ environmental failure protection (EFP) features.

7.7.4.2 Environmental failure protection features

Environmental failure protection (EFP) features **shall [07.75]** protect a cryptographic module against unusual environmental conditions (accidental or induced) when outside of the module's normal operating range that can compromise the security of the module.

The cryptographic module **shall [07.76]** monitor and correctly respond when operating *temperature* and *voltage* are outside of the specified normal operating ranges.

If the temperature or voltage falls outside of the cryptographic module's normal operating range, the protection capability **shall [07.77]** either:

- shutdown the module to prevent further operation,

  or

- immediately zeroise all unprotected SSPs.

7.7.4.3 Environmental failure testing procedures

Environmental failure testing (EFT) **shall [07.78]** involve a combination of analysis, simulation, and testing of a cryptographic module to provide reasonable assurance that the environmental conditions (accidental or induced) when outside the module's normal operating ranges for temperature and voltage will not compromise the security of the module.

EFT **shall [07.79]** 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 [07.80]** the security of the cryptographic module be compromised.

The temperature range to be tested **shall [07.81]** be from a temperature within the normal operating temperature range to the lowest (i.e. coldest) temperature that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all unprotected SSPs; and from a temperature within the normal operating temperature range to the highest (i.e. hottest) temperature that either (1) shuts down or goes into an error state or (2) zeroises all unprotected SSPs. The temperature range to be tested **shall [07.82]** be from - 100° to + 200° Celsius (- 150° to + 400° Fahrenheit); however, the test **shall [07.83]** be interrupted as soon as either (1) the module is shutdown to prevent further operation, (2) all unprotected SSPs are immediately zeroised or (3) the module enters a failure state. Temperature **shall [07.84]** be monitored internally at the sensitive components and critical devices and not just at the physical boundary of the module.

The voltage range tested **shall [07.85]** be gradually decreasing from a voltage within the normal operating voltage range to a lower voltage that either (1) shuts down the module to prevent further operation or (2) immediately zeroises all unprotected SSPs; and **shall [07.86]** be gradually increasing from a voltage within the normal operating voltage range to a higher voltage that either (1) shuts down the module to prevent further operation or (2) immediately zeroises all unprotected SSPs.

7.8 Non-invasive security

Non-invasive attacks attempt to compromise a cryptographic module by acquiring knowledge of the module’s CSPs without physically modifying or invading the module. Modules may implement various techniques to mitigate against these types of attacks. The test metrics for non-invasive attack mitigation for each of the associated security functions addressed by this International Standard are referenced in Annex F.

This subclause is not applicable if the cryptographic module does not implement non-invasive attack mitigation techniques to protect the module’s unprotected SSPs from non-invasive attacks referenced in Annex F.

Non-invasive attack mitigation techniques implemented by the cryptographic module to protect the module’s SSPs that are not referenced in Annex F **shall [08.01]** meet the requirements in 7.12.

Non-invasive attack mitigation techniques implemented by the cryptographic module to protect the module’s SSPs that are referenced in Annex F **shall [08.02]** meet the following requirements.

The documentation requirements specified in A.2.8 **shall [08.03]** be provided.

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, documentation **shall [08.04]** specify all of the mitigation techniques employed to protect the module’s CSPs from the non-invasive attacks referenced in Annex F. Documentation **shall [08.05]** include evidence of the effectiveness of each of the attack mitigation techniques.

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, for Security Level 3, the cryptographic module **shall [08.06]** be tested to meet the approved non-invasive attack mitigation test metrics for Security Level 3 as referenced in Annex F.

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1 and 2, for Security Level 4, the cryptographic module **shall [08.07]** be tested to meet the approved non-invasive attack mitigation test metrics for Security Level 4 as referenced in Annex F.

7.9 Sensitive security parameter management

7.9.1 Sensitive security parameter management general requirements

Sensitive Security Parameters (SSPs) consist of Critical Security Parameters (CSPs) and Public Security Parameters (PSPs). The security requirements for SSP management encompass the entire lifecycle of SSPs employed by the module. SSP management includes random bit generators (RBGs), SSP generation, SSP establishment, SSP entry/output, SSP storage, and unprotected SSP zeroisation.

Encrypted CSPs refer to CSPs that are encrypted using an approved security function. CSPs encrypted or obfuscated using non-approved security functions are considered unprotected plaintext within the scope of this International Standard.

CSPs **shall [09.01]** be protected within the module from unauthorised access, use, disclosure, modification, and substitution.

PSPs **shall [09.02]** be protected within the module against unauthorised modification and substitution.

A module **shall [09.03]** associate an SSP which is generated, entered into or output from the module with the entity (i.e. person, group, role, or process) to which the SSP is assigned.

Hash values of passwords, RBG state information and intermediate key generation values **shall [09.04]** be considered as CSPs.

The documentation requirements specified in A.2.9 **shall [09.05]** be provided.

7.9.2 Random bit generators

A cryptographic module may contain RBGs, a chain of RBGs, or may be solely an RBG. Approved RBGs are listed in Annex C.

If an approved security function, SSP generation or SSP establishment method requires random values, then an approved RBG **shall [09.06]** be used to provide these values.

If entropy is collected from outside the cryptographic boundary of the module, the data stream generated using this entropy input **shall [09.07]** be considered a CSP.

7.9.3 Sensitive security parameter generation

A module may generate SSPs internally or they may be derived from SSPs entered into the module.

Compromising the security of the SSP generation method which uses the output of an approved RBG (e.g. guessing the seed value to initialise the deterministic RBG) **shall [09.08]** require at least as many operations as determining the value of the generated SSP.

SSPs generated by the module from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function or SSP establishment method **shall [09.09]** be generated using an approved SSP generation method listed in Annex D.

7.9.4 Sensitive security parameter establishment

SSP establishment may consist of

- *automated* SSP transport or SSP agreement methods or
- *manual* SSP entry or output via direct or electronic methods.

Automated SSP establishment **shall [09.10]** use an approved method listed in Annex D. Manual SSP establishment **shall [09.11]** meet the requirements of 7.9.5.

7.9.5 Sensitive security parameter entry and output

SSPs may be manually entered into or output from a module either *directly* (e.g. entered via a keyboard or number pad, or output via a visual display) or *electronically* (e.g. via a smart card/tokens, PC card, other electronic key loading device, or the module operating system). If SSPs are manually entered into or output from a module, the entry or output **shall [09.12]** be through the defined HMI, SFMI, HFMI or HSMI (7.3.2) interfaces.

All cryptographically protected SSPs, entered into or output from the module **shall [09.13]** be encrypted using an approved security function.

For directly entered SSPs, the entered values may be temporarily displayed to allow visual verification and to improve accuracy. If encrypted SSPs are directly entered into the module, then the plaintext values of the SSPs **shall not [09.14]** be displayed. Directly entered (plaintext or encrypted) SSPs **shall [09.15]** be verified during entry into a module for accuracy using the conditional manual entry test specified in 7.10.3.5.

To prevent the inadvertent output of sensitive information, two independent internal actions **shall [09.16]** be required in order to output any plaintext CSP. These two independent internal actions **shall [09.17]** be dedicated to mediating the output of the CSPs.

For electronic entry or output via a wireless connection; CSPs, key components and authentication data **shall [09.18]** be encrypted.

Manually entered PSPs do not need to be cryptographically authenticated.

SECURITY LEVELS 1 AND 2

Plaintext CSPs, key components and authentication data may be entered and output via physical port(s) and logical interface(s) shared with other physical ports and logical interfaces of the cryptographic module.

For software modules or the software components of a hybrid software module, CSPs, key components and authentication data may be entered into or output in either encrypted or plaintext form provided that the CSPs, key components and authentication data **shall [09.19]** be maintained within the operational environment and meet the requirements of 7.6.3.

SECURITY LEVEL 3

In addition to Security Levels 1 and 2, for Security Level 3, CSPs, key components and authentication data **shall [09.20]** be entered into or output from the module either encrypted or by a trusted channel.

CSPs which are plaintext secret and private cryptographic keys **shall [09.21]** be entered into or output from the module using split knowledge procedures using a trusted channel.

If the module employs split knowledge procedures, the module **shall [09.22]** employ separate identity-based operator authentication for entering or outputting each key component, and at least two key components **shall [09.23]** be required to reconstruct the original cryptographic key.

SECURITY LEVEL 4

In addition to Security Level 3, for Security Level 4 the module **shall [09.24]** employ multi-factor separate identity-based operator authentication for entering or outputting each key component.

7.9.6 Sensitive security parameter storage

SSPs stored within a module may be stored either in plaintext or encrypted form. A module **shall [09.25]** associate every SSP stored within the module with the entity (e.g. operator, role, or process) to which the SSP is assigned.

Access to plaintext CSPs by unauthorised operators **shall [09.26]** be prohibited. Modification of PSPs by unauthorised operators **shall [09.27]** be prohibited.

7.9.7 Sensitive security parameter zeroisation

A module **shall [09.28]** provide methods to zeroise all unprotected SSPs and key components within the module. Temporarily stored SSPs and other stored values owned by the module should be zeroised when they are no longer needed for future use.

A zeroised SSP **shall [09.29]** not be retrievable or reusable.

Except at security level 4, zeroisation of protected PSPs, 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.

SSPs need not meet these zeroisation requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialisation key).

Parameters used solely for self-test purposes in 7.10 need not meet zeroisation requirements.

SECURITY LEVEL 1

The zeroisation of unprotected SSPs may be performed procedurally by the module operator, and independent of the module's control (e.g. reformatting of a hard drive, the atmospheric destruction of a module during re-entry, etc.).

SECURITY LEVELS 2 AND 3

The cryptographic module **shall [09.30]** perform the zeroisation of unprotected SSPs (e.g. overwriting with all zeros or all ones or with random data). Zeroisation **shall [09.31]** exclude the overwriting of an unprotected SSP with another unprotected SSP. Temporary SSPs **shall [09.32]** be zeroised when they are no longer needed. The module **shall [09.33]** provide an output status indication when the zeroisation is complete.

SECURITY LEVEL 4

In addition to the requirements of Security Levels 2, and 3, the following requirements **shall [09.34]** be met:

- the zeroisation **shall [09.35]** be immediate and non-interruptible and **shall [09.36]** occur in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time zeroisation is initiated and the actual zeroisation completed; and

- all SSPs **shall [09.37]** be zeroised whether plaintext or cryptographically protected, such that the module is returned to the factory state.

7.10 Self-tests

7.10.1 Self-test general requirements

Cryptographic module pre-operational and conditional self-tests provides the operator assurance that faults have not been introduced that would prevent the module's correct operation. All self-tests **shall [10.01]** be performed, and determination of pass or fail **shall [10.02]** be made by the module, without external controls, externally provided input text vectors, expected output results, or operator intervention or whether the module will operate in an approved or non-approved mode.

The pre-operational self-tests **shall [10.03]** be performed and passed successfully prior to the module providing any data output via the data output interface.

Conditional self-tests **shall [10.04]** be performed when an applicable security function or process is invoked (i.e. security functions for which self-tests are required).

All self-tests identified in underlying algorithmic standards (Annexes C through E) **shall [10.05]** be implemented as applicable within the cryptographic module. All self-tests identified in addition or in lieu of those specified in the underlying algorithmic standards (Annexes C through E) **shall [10.06]** be implemented as referenced in Annexes C through E for each approved security function, SSP establishment method and authentication mechanism.

A cryptographic module may perform other pre-operational or conditional critical functions test in addition to the tests specified in this International Standard.

If a cryptographic module fails a self-test, the module **shall [10.07]** enter an error state and **shall [10.08]** output an error indicator as specified in 7.3.3. The cryptographic module **shall not [10.09]** perform any cryptographic operations or output control and data via the control and data output interface while in an error state. The cryptographic module **shall not [10.10]** utilise any functionality that relies upon a function or algorithm that failed a self-test until the relevant self-test has been repeated and successfully passed. If a module does not output an error status upon failure of a module self-test, the operator of the module **shall [10.11]** be able to determine if the module has entered an error state implicitly through an unambiguous procedure documented in the security policy (Annex B).

At Security Levels 3 and 4, the module **shall [10.12]** maintain an error log that is accessible by an authorised operator of the module. The error log **shall [10.13]** provide information, at a minimum, the most recent error event (i.e. which self-test failed).

The documentation requirements specified in A.2.10 **shall [10.14]** be provided.

7.10.2 Pre-operational self-tests

7.10.2.1 Pre-operational self-test general requirements

The *pre-operational self-tests* **shall [10.15]** be performed and passed successfully by a cryptographic module between the time a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc.) and before the module transitions to the operational state.

A cryptographic module **shall [10.16]** perform the following pre-operational self-tests, as applicable:

- pre-operational software/firmware integrity test;
- pre-operational bypass test; and

- pre-operational critical functions test.

7.10.2.2 Pre-operational software/firmware integrity test

All software and firmware components within the cryptographic boundary **shall [10.17]** be verified using an approved *integrity technique* or *EDC* satisfying the requirements defined in 7.5. If the verification fails, the pre-operational software/firmware integrity test **shall [10.18]** fail. The pre-operational software/firmware integrity test is not required for any software or firmware excluded from the security requirements of this International Standard or for any executable code stored in non-reconfigurable memory.

If a hardware module does not contain either software or firmware, the module **shall [10.19]**, at a minimum, implement one cryptographic algorithm self-test as specified in 7.10.3.2 as a pre-operational self-test.

A cryptographic algorithm that is used to perform the approved integrity technique for the pre-operational software/firmware test **shall [10.20]** first pass the cryptographic algorithm self-test specified in 7.10.3.2.

7.10.2.3 Pre-operational bypass test

If a cryptographic module implements a *bypass* capability, then the module **shall [10.21]** ensure the correct operation of the logic governing activation of the bypass capability by exercising that logic. The module **shall [10.22]** also verify the data path by:

- setting the bypass switch to provide cryptographic processing and verify that data transferred through the bypass mechanism is cryptographically processed, and

- setting the bypass switch to not provide cryptographic processing and verify that data transferred through the bypass mechanism is not cryptographically processed.

7.10.2.4 Pre-operational critical functions test

There may be other security functions critical to the secure operation of a cryptographic module that **shall [10.23]** be tested as a pre-operational test. Documentation **shall [10.24]** specify the pre-operational critical functions that are tested.

7.10.3 Conditional self-tests

7.10.3.1 Conditional self-test general requirements

Conditional self-tests **shall [10.25]** be performed by a cryptographic module when the conditions specified for the following tests occur: Cryptographic Algorithm Self-Test, Pair-Wise Consistency Test, Software/Firmware Load Test, Manual Entry Test, Conditional Bypass Test and Conditional Critical Functions Test.

7.10.3.2 Conditional cryptographic algorithm self-test

Cryptographic Algorithm Self-Test. A cryptographic algorithm test **shall [10.26]** be conducted for all cryptographic functions (e.g. security functions, SSP establishment methods and authentication) of each approved cryptographic algorithm implemented in the cryptographic module as referenced in Annexes C through E. The conditional test **shall [10.27]** be performed prior to the first operational use of the cryptographic algorithm.

A cryptographic algorithm self-test may be a *known-answer* test, a *comparison* test or a *fault-detection* test.

A *known-answer test* consists of a set of known input vectors (e.g. data, keying material, or constants in lieu of random bits) which are operated on by the cryptographic algorithm to generate a result. The result is compared to the known expected output result. If the calculated output does not equal the known answer, the cryptographic algorithm known-answer self-test **shall [10.28]** fail.

An algorithm self-test **shall [10.29]** at a minimum use the smallest approved key length, modulus size, DSA prime, or curves as appropriate that is supported by the module.

If an algorithm specifies multiple modes (e.g. ECB, CBC, etc), at a minimum, one mode **shall [10.30]** be selected for the self-test that is supported by the module or as specified by the validation authority.

Examples of known-answer tests:

— One-way functions: Input test vector(s) generate output which **shall [10.31]** be identical to expected output (e.g. hashing, keyed hashes, message authentication, RBG (fixed entropy vector), SSP agreement).

— Reversible functions: Both the forward and reverse function **shall [10.32]** be self-tested (e.g. symmetric key encryption and decryption, SSP transport encryption and decryption, digital signature generation and verification)

A *comparison test* compares the output of two or more independent cryptographic algorithm implementations, if the outputs are not equal, the cryptographic algorithm comparison self-test **shall [10.33]** fail.

A *fault-detection test* involves the implementation of fault detection mechanisms integrated within the cryptographic algorithm implementation, if a fault is detected, the cryptographic algorithm fault-detection self-test **shall [10.34]** fail.

7.10.3.3 Conditional pair-wise consistency test

If a cryptographic module generates public or private key pairs, a pair-wise consistency test **shall [10.35]** be performed for every generated public and private key pair as referenced in Annexes C through E for the applicable cryptographic algorithm.

7.10.3.4 Conditional software/firmware load test

If a cryptographic module has the capability of loading software or firmware from an external source, then the following requirements in addition to those in 7.4.3.4 **shall [10.36]** be performed:

— the cryptographic module **shall [10.37]** implement an approved authentication technique to verify the validity of the software or firmware that is loaded;

— the reference authentication key **shall [10.38]** be loaded independently in the module prior to the software or firmware loading; and

— the applied approved authentication technique **shall [10.39]** be successfully verified or the software/firmware load test **shall [10.40]** fail. Loaded software or firmware **shall not [10.41]** be used if the software/firmware load test fails.

7.10.3.5 Conditional manual entry test

If SSPs or key components are manually entered directly into a cryptographic module or if error on the part of the human operator could result in the incorrect entry of the intended value, then the following manual entry tests **shall [10.42]** be performed:

— the SSP or key components **shall [10.43]** have an error detection code (EDC) applied, or **shall [10.44]** be entered using duplicate entries.

If an EDC is used, the EDC **shall [10.45]** be at least 16 bits in length. If the EDC cannot be verified, or the duplicate entries do not match, the test **shall [10.46]** fail.

7.10.3.6 Conditional 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 suite of bypass tests **shall [10.47]** 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 [10.48]** 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 [10.49]** 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).

If a cryptographic module maintains internal information that governs the bypass capability, then the module **shall [10.50]** verify the integrity of the governing information through an approved integrity technique immediately preceding modification of the governing information, and **shall [10.51]** generate a new integrity value using the approved integrity technique immediately following the modification..

7.10.3.7 Conditional critical functions test

There may be other security functions critical to the secure operation of a cryptographic module that **shall [10.52]** be tested as a conditional self-test.

7.10.3.8 Periodic self-tests

SECURITY LEVELS 1 AND 2

A cryptographic module **shall [10.53]** permit operators to initiate the pre-operational or conditional self-tests on demand for periodic testing of the module. Acceptable means for the on-demand initiation of periodic self-tests are: provided service, resetting, rebooting, or power cycling.

SECURITY LEVELS 3 AND 4

In addition to the requirements at Security Levels 1 and 2, the module **shall [10.54]** repeatedly upon a defined time period automatically, without external input or control, perform the pre-operational or conditional self-tests. The time period and any conditions that may result in the interruption of the module's operations during the time to repeat the pre-operational or conditional self-tests **shall [10.55]** be specified in the security policy (Annex B) (e.g. If the module is performing mission critical services that can't be interrupted and the time period is passed for the initiation of the pre-operational self-tests; the self-tests may be deferred after the time period is passed again.).

7.11 Life-cycle assurance

7.11.1 Life-cycle assurance general requirements

Life-cycle assurance refers to the use of best practices by the vendor of a cryptographic module during the design, development, operation and end of life of a cryptographic module, providing assurance that the module is properly designed, developed, tested, configured, delivered, installed and disposed, and that the proper operator guidance documentation is provided. Security requirements are specified for configuration management, design, finite state model, development, testing, delivery and operation, and guidance documentation.

The documentation requirements specified in A.2.11 **shall [11.01]** be provided.

7.11.2 Configuration management

Configuration management specifies the requirements for a configuration management system implemented by a cryptographic module vendor, providing assurance that the integrity of the cryptographic module is preserved by requiring discipline and control in the processes of refinement and modification of the cryptographic module and related documentation. A configuration management system is put in place to prevent accidental or unauthorised modifications to, and provide change traceability for, the cryptographic module and related documentation.

SECURITY LEVELS 1 AND 2

The following security requirements **shall [11.02]** apply to cryptographic modules for Security Levels 1 and 2:

- a configuration management system **shall [11.03]** be used for the development of a cryptographic module and module components within the cryptographic boundary, and of associated module documentation;
- each version of each configuration item (e.g. cryptographic module, module hardware parts, module software components, module HDL, user guidance, security policy, etc.) that comprises the module and associated documentation **shall [11.04]** be assigned and labelled with a unique identifier; and
- the configuration management system **shall [11.05]** track and maintain the changes to the identification and version or revision of each configuration item throughout the life-cycle of the validated cryptographic module.

SECURITY LEVELS 3 AND 4

In addition to the requirements for Security Levels 1 and 2, the configuration items **shall [11.06]** be managed using an automated configuration management system.

7.11.3 Design

A design is an engineering solution that addresses the functional specification for a cryptographic module. The design is intended to provide assurance that the functional specification of a cryptographic module corresponds to the intended functionality described in the security policy.

Cryptographic modules **shall [11.07]** be designed to allow the testing of all provided security related services.

7.11.4 Finite state model

The operation of a cryptographic module **shall [11.08]** be specified using a Finite State Model (or equivalent) represented by a state transition diagram and a state transition table and state descriptions. The FSM **shall [11.09]** be sufficiently detailed to demonstrate that the cryptographic module complies with all of the requirements of this International Standard.

The FSM of a cryptographic module **shall [11.10]** include, as a minimum, the following operational and error states:

- *Power on/off state*. A state in which the module is powered off, placed in standby mode (volatile memory maintained), or the operational state preserved in non-volatile memory (e.g. hibernation mode) and in which primary, secondary, or backup power is applied to the module. This state may distinguish between power sources being applied to a cryptographic module. For a software module, power on is the action of spawning an executable image of the cryptographic module.

— *General initialisation state*: A state in which the cryptographic module is undergoing initializing before the module transitions to the approved state.

— *Crypto Officer State*: a state in which the Crypto Officer services are performed (e.g. cryptographic initialisation, secure administration, and key management).

— *CSP entry state:* a state for entering the CSPs into the cryptographic module.

— *User state:* (if a User role is implemented): a state in which authorised users obtain security services, perform cryptographic operations, or perform other approved functions.

— *Approved state*: a state in which approved security functions are performed.

— *Self-test state*: a state in which the cryptographic module is performing self-tests.

— *Error state*: a state when the cryptographic module has encountered an error condition (e.g. failed a self-test). There may be one or more error conditions that result in a single module error state. 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 [11.11]** be possible, except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.

Each distinct cryptographic module service, security function use, error state, self-test, or operator authentication **shall [11.12]** be depicted as a separate state.

Changing to the Crypto Officer state from any other role other than the Crypto Officer role **shall [11.13]** be prohibited.

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

— *Bypass state*: a state in which a service, as a result of module configuration or operator intervention, causes the plaintext output of a particular data or status item that would normally be output in encrypted form.

— *Quiescent state:* a state in which the cryptographic module is dormant (e.g. low power, suspended or in hibernation).

7.11.5 Development

A proper *development* process provides assurance that the implementation of a cryptographic module corresponds to the module functional specification and security policy, that the cryptographic module is maintainable, and that the validated cryptographic module is reproducible. This clause specifies the security requirements for the representation of a cryptographic module’s security functionality at various levels of abstraction from the functional specification to the implementation representation.

SECURITY LEVEL 1

The following requirements **shall [11.14]** apply to cryptographic modules for Security Level 1:

— if a cryptographic module contains software or firmware, the source code, language reference, the compilers, compiler versions and compiler options, the linker and linker options, the runtime libraries and runtime library settings, configuration settings, build processes and methods, the build options, environmental variables and all other resources used to compile and link the source code into an executable form **shall [11.15]** be tracked using the configuration management system;

- if a cryptographic module contains software or firmware, the source codes **shall [11.16]** be annotated with comments that depict the correspondence of the software or firmware to the design of the module;
- if a cryptographic module contains hardware, documentation **shall [11.17]** specify the schematics and/or Hardware Description Language (HDL), as applicable;
- if a cryptographic module contains hardware, the HDL **shall [11.18]** be annotated with comments that depict the correspondence of the hardware to the design of the module;
- for software and firmware cryptographic modules and the software or firmware component of a hybrid module:
  - the result of the integrity and authentication technique mechanisms specified in 7.5 and 7.10 **shall [11.19]** be calculated and integrated into the software or firmware module by the vendor during the module development;
  - the cryptographic module documentation **shall [11.20]** specify the compiler, configuration settings and methods to compile the source code into an executable form; and
  - the cryptographic module **shall [11.21]** be developed using production-grade development tools (e.g. compilers).

SECURITY LEVELS 2 AND 3

In addition to the requirements for Security Level 1, the following requirements **shall [11.22]** apply to cryptographic modules for Security Levels 2 and 3:

- all software or firmware **shall [11.23]** be implemented using a high-level, non-proprietary language or rationale **shall [11.24]** be provided for the use of a low-level language (e.g. assembly language or microcode) if essential to the performance of the module or when a high-level language is not available;
- custom integrated circuits within a cryptographic module **shall [11.25]** be implemented using a high-level Hardware Description Language (HDL) (e.g. VHDL or Verilog); and
- all software or firmware **shall [11.26]** be designed and implemented in a manner that avoids the use of code, parameters or symbols not necessary for the module's functionality and execution.

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2 and 3, the following requirement **shall [11.27]** apply to cryptographic modules for Security Level 4:

- for each cryptographic module hardware and software component, the documentation **shall [11.28]** be annotated with comments that specify (1) the pre-conditions required upon entry into each module component, function, and procedure in order to execute correctly and (2) the post-conditions expected to be true when the execution of each module component, function, and procedure is complete. The pre-conditions and post-conditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behavior of the cryptographic module component, function, and procedure.

7.11.6 Vendor testing

This clause specifies the requirements for *vendor testing* of the cryptographic module, including testing of the security functionality implemented in the cryptographic module, providing assurance that the cryptographic module behaves in accordance with the module security policy and functional specifications.

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, documentation **shall [11.29]** specify the functional testing performed on the cryptographic module.

For software or firmware cryptographic modules and the software or firmware component of a hybrid module, the vendor **shall [11.30]** use automated security diagnostic tools (e.g. detect buffer overflow).

SECURITY LEVELS 3 AND 4

In addition to the requirements for Security Levels 1 and 2, documentation **shall [11.31]** specify the procedures for and the results of low-level testing performed on the cryptographic module.

7.11.7 Delivery and operation

This clause specifies the security requirements for the secure delivery, installation, and startup 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

For Security Level 1, documentation **shall [11.32]** specify the procedures for secure installation, initialisation, and startup of the cryptographic module.

SECURITY LEVELS 2 AND 3

In addition to the requirement of Security Level 1, documentation **shall [11.33]** specify the procedures required for maintaining security while distributing, installation and the initialisation of versions of a cryptographic module to authorised operators. The procedures **shall [11.34]** specify how to detect tamper during the delivery, installation and initialisation of the module to the authorised operators.

SECURITY LEVEL 4

In addition to the requirements of Security Levels 1, 2 and 3, the procedures **shall [11.35]** require the authorised operator to be authenticated by the module using the operator specific authentication data provided by the vendor.

7.11.8 End of life

This clause specifies the security requirements when a cryptographic module is no longer deployed or intended for further use by the operator.

SECURITY LEVELS 1 AND 2

For Security Level 1 and 2, documentation **shall [11.36]** specify the procedures for secure sanitization of the cryptographic module. Sanitization is the process of removing sensitive information (e.g. SSPs, user data, etc.) from the module, so that it may either be distributed to other operators or disposed.

SECURITY LEVELS 3 AND 4

In addition to the requirement of Security Levels 1 and 2, documentation **shall [11.37]** specify the procedures required for the secure destruction of the module.

7.11.9 Guidance documents

The requirements in this clause are intended to ensure that all entities using the cryptographic module have adequate guidance and procedures to administer and use the module in an approved mode of operation.

Guidance documentation consists of administrator and non-administrator guidance.

Administrator guidance **shall [11.38]** specify:

- 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 and/or other administrative roles;
- procedures required to keep operator authentication data and mechanisms functionally independent;
- procedures on how to administer the cryptographic module in an approved mode of operation; and
- assumptions regarding User behavior that are relevant to the secure operation of the cryptographic module.

Non-administrator guidance **shall [11.39]** specify:

- the approved and non-approved security functions, physical ports, and logical interfaces available to the users of a cryptographic module; and
- all User responsibilities necessary for the approved mode of operation of a cryptographic module.

7.12 Mitigation of other attacks

Susceptibility of a cryptographic module to attacks not defined elsewhere in this International Standard depends on the 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). These attacks generally rely on the analysis of information obtained from sources that are physically external to the module. In all cases, the attacks attempt to determine some knowledge about the CSPs within the cryptographic module.

The documentation requirements specified in A.2.12 **shall [12.01]** be provided.

SECURITY LEVELS 1, 2 AND 3

If a cryptographic module is designed to mitigate one or more specific attack(s) not defined elsewhere in this International Standard, then the module's supporting documents **shall [12.02]** enumerate the attack(s) the module is designed to mitigate. The existence and proper functioning of the security mechanisms used to mitigate the attack(s) will be validated when requirements and associated tests are developed.

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2 and 3, the following requirement **shall [12.03]** apply to cryptographic modules for Security Levels 4:

- If the mitigation of specific attacks not defined elsewhere in this International Standard is claimed, documentation **shall [12.04]** specify the methods used to mitigate the attacks and the methods to test the effectiveness of mitigation techniques.

Annex A
(normative)

Documentation requirements

A.1 Purpose

This annex specifies the minimum documentation which **shall [A.01]** be required for a cryptographic module that is to undergo an independent verification scheme.

A.2 Items

A.2.1 General

No general documentation requirements specified.

A.2.2 Cryptographic module specification

- Specification of the module type (hardware, software, firmware, hybrid software or hybrid firmware module). *(Security Levels 1, 2, 3 and 4)*
- Specification of the module boundary. *(Security Levels 1, 2, 3 and 4)*
- Specification of the hardware, software and firmware components of the cryptographic module, and description of the physical configuration of the module. *(Security Levels 1, 2, 3 and 4)*
- Specification of hardware, software or firmware components of the 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)*
- Specification of the physical ports and logical interfaces of a cryptographic module. *(Security Levels 1, 2, 3 and 4)*
- 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)*
- Specification 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)*
- 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)*
- Specification of the design of the hardware, software and firmware of a cryptographic module. *(Security Levels 1, 2, 3 and 4)*