International Standard

# ISO/IEC 19790

Third edition
2025-02

# Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules

*Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences de sécurité pour les modules cryptographiques*



Reference number
ISO/IEC 19790:2025(en)



ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

# Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 19790:2012), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 19790:2012/Cor 1:2015.

The main changes are as follows:

— Clauses 3, 4 and 5 have been refined and updated to reflect changes in requirements in Clause 7;

— the language in Clause 6 has been refined and modernized;

— in Clause 7, the requirements have been reworded and rearranged for clarity. New requirements have been added, and redundant or unnecessary requirements removed;

— Annexes A and B have been updated to reflect changes in requirements in Clause 7;

— Annexes C, D and E have been restructured and updated in line with standards published since the previous edition, as well as with examples of rate limiting methods;

— Annex F has been updated with the inclusion of ISO/IEC 17825; and

— new Annex G on module secure development, manufacturing and operation has been added.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

# Introduction

In information technology there is an ever-increasing need to use cryptographic mechanisms, such as for the protection of data against unauthorized 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 document provides 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 defined in this document. 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 or the security level within each area of a cryptographic module is chosen to provide a level of security which is appropriate for the security requirements of the application and environment in which the module is utilized and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilize cryptographic modules provide an appropriate 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, conformity with this document 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;

— system security maintenance and patch management;

— 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.

Conformity with this document is not sufficient to ensure that a 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.

Owners of sensitive information are expected to assess the risks to their information and to deploy cryptographic modules as part of their overall risk mitigation plan, in order to mitigate specific identified risks. The security policy of the module, which outlines its strengths and limitations, is expected to be followed for any given deployment.

# Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules

## 1 Scope

This document specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in Information and Communication Technologies (ICT). It defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity and a diversity of application environments. This document specifies up to four security levels for each of the 11 requirement areas with each security level increasing security over the preceding level.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

**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 either the *crypto officer* (3.30) or any other administrative *role* (3.119) for the correct configuration, maintenance, and administration of the *cryptographic module* (3.35)

**3.3**
**automated**
without *manual* (3.81) intervention or input (e.g. electronic means such as through a computer network)

**3.4**
**approved data authentication technique**
approved method providing assurance that the originator of the data is as claimed

Note 1 to entry: Approved data authentication techniques can include the use of an approved *digital signature* (3.43), approved *message authentication code* (3.82) or approved keyed hash. Approved data authentication techniques are specified in Annex C.

**3.5**
**approved integrity technique**
approved method of verifying whether or not data has been corrupted or modified

Note 1 to entry: Approved integrity techniques can be keyed, and can include an approved hash, a *message authentication code* (3.82) or a *digital signature* (3.43) algorithm.

Note 2 to entry: Approved integrity techniques are specified in Annex C.

**3.6**
**approved process**
set of interrelated functions that includes at least one *approved security function* (3.8), and can include a non-cryptographic function or non-approved *security function* (3.126) which are not security relevant to the process's operation

Note 1 to entry: A banking transaction, a compression service that includes encryption, etc.

**3.7**
**approved service**
*service* (3.136) which includes at least one *approved security function* (3.8) or process, and can include *non-security relevant* (3.91) functions or processes

Note 1 to entry: Any *security relevant* (3.128) but non-approved security functions or processes are excluded from approved services.

**3.8**
**approved security function**
*security function* (3.126) that is permitted for use in an *approved service* (3.7)

Note 1 to entry: Approved security functions are referenced in Annex C, which references Annex D and Annex E.

**3.9**
**asymmetric algorithm**
asymmetric technique
*cryptographic algorithm* (3.31) or technique that uses two related transformations: a public transformation (defined by the *public key* (3.113)) and a private transformation (defined by the *private key* (3.110))

Note 1 to entry: 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**
**attestation**
process used to allow an *entity* (3.49) outside the boundary of the *cryptographic module* (3.35) to securely verify the identity and other physical or logical characteristics of the cryptographic module using an *attestation record* (3.11)

Note 1 to entry: An attestation conforms to the attestation standards and methods listed in Annex G.

**3.11**
**attestation record**
record that is generated by and retrievable from a *cryptographic module* (3.35) that supports the *attester service* (3.12)

Note 1 to entry: The attestation record contains measurement details about *software* (3.140), *firmware* (3.58) or *hardware* (3.64) components within the cryptographic module. Measurements can include hash values or copies of software, firmware, or hardware components within the cryptographic module as well as configuration settings, *status information* (3.145), registers, and fuse values.

**3.12**
**attester service**
*service* (3.136) that a *cryptographic module* (3.35) can support, which requires the module to support an identity and the generation of an *attestation record* (3.11)

**3.13**
**authentication data**
data entered into the *cryptographic module* (3.35) by the *operator* (3.98), used to authenticate the operator to the module

Note 1 to entry: Authentication data within the module are transient and are considered a temporary *critical security parameter* (3.29).

Note 2 to entry: During an authentication attempt, authentication data are submitted to the module as:

a) a data input by the operator (e.g. a *password* (3.102), *personal identification number* (3.103), *cryptographic key* (3.34) or equivalent); or

b) the result of a method/process involving operator related information (e.g. the signing of a challenge with a *private key* (3.110), insertion of a physical key, processing of *biometric* (3.15) data).

**3.14**
**authorized**
when an *operator* (3.98) has authority to assume a specific *role* (3.119) and perform a corresponding set of services

**3.15**
**biometric**
measurable, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of an *operator* (3.98)

**3.16**
**bitstream**
series of instructions parsed by a field programmable gate array (FPGA) on start-up to configure its internal logic

Note 1 to entry: Bitstream is considered a highly customized form of executable code.

**3.17**
**certificate**
data of an entity, which is rendered unforgeable with the private or secret key of a certification authority (CA)

Note 1 to entry: This term should not to be confused with a module's validation certificate issued by a *certification body* (3.18).

**3.18**
**certification body**
third-party conformity assessment body operating a certification scheme

Note 1 to entry: A certification body can be non-governmental or governmental (with or without regulatory authority).

Note 2 to entry: A certification body that assesses conformance to this document is known as a validation authority.

Note 3 to entry: A certification scheme is a system related to specified products, to which the same specified requirements, specific rules and procedures apply.

[SOURCE: ISO/IEC 17065:2012, 3.12]

**3.19**
**compromise**
unauthorized disclosure, modification, substitution, or use of a *critical security parameter* (3.29), the unauthorized modification or substitution of a *public security parameter* (3.115), or the loss of *integrity* (3.72) or availability of the *cryptographic module* (3.35) itself, which can result in an unintended bypass of security functions supported by the module

**3.20**
**conditional self-test**
test performed by a *cryptographic module* (3.35) when the conditions specified for the test occur

**3.21**
**confidential**
intending that information is not made available or disclosed to unauthorized entities

**3.22**
**configuration management**
discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specific requirements

[SOURCE: ISO/IEC/IEEE 24765:2017 3.779.1, modified — in the definition "specified" has been replaced by "specific".]

**3.23**
**configuration management system**
CMS
set of procedures and tools (including their documentation) used by a *vendor* (3.156) to develop and maintain configurations of a *cryptographic module* (3.35) during its life cycle

**3.24**
**control information**
commands, signals (e.g. clock input/output), and control data (including function calls and *manual* (3.81) control data such as from switches, buttons, and keyboards) used to direct or control the operation of a *cryptographic module* (3.35) or disjoint components of a *hybrid module* (3.68)

**3.25**
**control input**
*control information* (3.24) that is input into a *cryptographic module* (3.35) or disjoint components of a *hybrid module* (3.68)

**3.26**
**control input interface**
module interface(s) for which all *control information* (3.24) is input into the *cryptographic module* (3.35)

**3.27**
**control output**
*control information* (3.24) that is output from a *cryptographic module* (3.35) or disjoint component of a *hybrid module* (3.68) to be used as *control input* (3.25) into another cryptographic module or disjoint component of a hybrid module

**3.28**
**control output interface**
module interface(s) for which all *control information* (3.24) is output from the *cryptographic module* (3.35)

**3.29**
**critical security parameter**
CSP
security related information whose unauthorized access, use, disclosure, modification and substitution can cause a *compromise* (3.19) of the security of a *cryptographic module* (3.35)

EXAMPLE Secret and private *cryptographic key* (3.34), *authentication data* (3.13) or *verifier data* (3.157) such as a *password* (3.102) or *personal identification number* (3.103).

Note 1 to entry: A CSP can be *plaintext* (3.105) or encrypted.

**3.30**
**crypto officer**
*role* (3.119) taken by an *operator* (3.98) that accesses a *cryptographic module* (3.35) in order to perform cryptographic initialization or management functions of a cryptographic module (e.g. module initialization, management of *sensitive security parameters* (3.131) and auditing)

**3.31**
**cryptographic algorithm**
well-defined computational procedure that takes variable inputs, which can include a *cryptographic key* (3.34), and produces an output

Note 1 to entry: Approved cryptographic algorithm standards are included in Annex C.

**3.32**
**cryptographic boundary**
explicitly defined perimeter that establishes the boundary of all components (i.e. set of *hardware* (3.64), *software* (3.140) or *firmware* (3.58) components) of the *cryptographic module* (3.35)

**3.33**
**cryptographic bypass**
ability of a *service* (3.136) to partially or wholly circumvent a cryptographic function or process

**3.34**
**cryptographic key**
key
sequence of symbols that controls the operation of a cryptographic transformation

Note 1 to entry: A cryptographic transformation can include but is not limited to encipherment, decipherment, cryptographic check value computation, signature generation, or signature verification.

**3.35**
**cryptographic module**
module
set of *hardware* (3.64) and either *software* (3.140) or *firmware* (3.58) that implements security functions and are contained within the *cryptographic boundary* (3.32)

**3.36**
**cryptographic module security policy**
security policy
precise specification of the security rules under which a *cryptographic module* (3.35) will operate, including the rules derived from the requirements of this document and additional rules imposed by the module or *certification body* (3.18)

Note 1 to entry: See Annex B.

**3.37**
**cryptographic operation**
implementation of one or more *cryptographic algorithm* (3.31) in the *cryptographic module* (3.35)

**3.38**
**data input interface**
module interface(s) for which all *input data* (3.71) is input into the *cryptographic module* (3.35)

**3.39**
**data output interface**
module interface(s) for which all *output data* (3.99) is output from the *cryptographic module* (3.35)

**3.40**
**data path**
physical or logical route over which data passes

Note 1 to entry: A physical data path can be shared by multiple logical data paths.

**3.41**
**debugging technique**
method used to halt or alter the execution of the *cryptographic module* (3.35) to analyse malfunctions, using interfaces or tools that can modify objects in memory (e.g. including executable code), in a way that it is possible to bypass security controls

Note 1 to entry: Security controls are considered to be any feature of the executable code required to meet the functional requirements of this document.

**3.42**
**degraded operation**
operation where a subset of the entire set of security functions, services or processes are either available or configurable or both as a result of reconfiguration from an error state

**3.43**
**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* (3.72) of the data unit and protect against forgery (e.g. by the recipient)

**3.44**
**direct entry**
entry of a *sensitive security parameter* (3.131) or *key component* (3.74) into a *cryptographic module* (3.35), using a device such as a keyboard or number pad

**3.45**
**disjoint signature**
signature used as part of a group of signatures, which together represent an entire set of code

**3.46**
**electronic entry**
entry of a *sensitive security parameter* (3.131) or *key component* (3.74) into a *cryptographic module* (3.35) using electronic methods

Note 1 to entry: It is possible that the *operator* (3.98) of the *cryptographic module* (3.35) has no knowledge of the value of the key being entered.

**3.47**
**encompassing signature**
single signature for an entire set of code

**3.48**
**encrypted critical security parameter**
encrypted CSP
*critical security parameter* (3.29) that has been encrypted using an *approved security function* (3.8)

**3.49**
**entity**
person, group, device or process

**3.50**
**entropy**
measure of the disorder, randomness or variability in a closed system

Note 1 to entry: The entropy of a random variable $X$ is a mathematical measure of the amount of information provided by an observation of $X$.

**3.51**
**environmental failure protection**
EFP
use of features to protect against a *compromise* (3.19) of the security of a *cryptographic module* (3.35) due to environmental conditions outside of the module's normal operating range

**3.52**
**environmental failure testing**
EFT
use of specific methods to provide reasonable assurance that the security of a *cryptographic module* (3.35) will not be compromised by environmental conditions outside of the module's normal operating range

**3.53**
**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

**3.54**
**executable form**
form of the code in which the *software* (3.140) or *firmware* (3.58) is managed and controlled completely by the *operational environment* (3.96) of the *cryptographic module* (3.35) and does not require compilation

**3.55**
**factory state**
default settings consistent with how the *cryptographic module* (3.35) left the factory

Note 1 to entry: It is possible that some *sensitive security parameters* (3.131) will be replaced during the lifetime of the module and still be considered part of the factory state, such as a trust anchor.

**3.56**
**fault injection**
technique to induce operating behaviour changes in *hardware* (3.64), such as by the application of transient voltages, radiation, laser or clock skewing techniques

**3.57**
**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

**3.58**
**firmware**
code that is executed in a *non-modifiable operational environment* (3.90) or *limited operational environment* (3.77)

**3.59**
**firmware module**
*cryptographic module* (3.35) whose *cryptographic boundary* (3.32) delimits the *firmware* (3.58) exclusive files(s) that execute(s) in a *limited operational environment* (3.77) or *non-modifiable operational environment* (3.90)

Note 1 to entry: The computing platform and operating system of the *operational environment* (3.96) in which the firmware executes are external to the defined firmware module's cryptographic boundary. However, the version of the computing platform and the version of the operating system of the operational environment are explicitly bound to the firmware module.

**3.60**
**functional specification**
high-level description of any *port* (3.107) or interface visible to the *operator* (3.98) and high-level description of the behaviour of the *cryptographic module* (3.35)

**3.61**
**functional testing**
testing of the *cryptographic module* (3.35) functionality as defined by the *functional specification* (3.60)

**3.62**
**hard**
resistant to bending, and ability to resist penetration by another object; physically toughened; rugged, and durable

**3.63**
**hardness**
relative resistance of a metal or other material to denting, scratching, or bending, including a material's ability to resist penetration by another object

**3.64**
**hardware**
physical equipment/elements

**3.65**
**hardware module**
*cryptographic module* (3.35) whose *cryptographic boundary* (3.32) is specified at a *hardware* (3.64) perimeter

Note 1 to entry: *Firmware* (3.58), which can also include an operating system, can be included within this hardware cryptographic boundary.

Note 2 to entry: A *bitstream* (3.16) contains a series of instructions parsed by a field programmable gate array (FPGA) on start-up to configure its internal logic. Bitstreams used to configure FPGAs in a hardware module or hardware component are subject to the requirements of 7.4.3.4, 7.5, 7.10.3.2 and 7.10.4.4.

**3.66**
**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

**3.67**
**hash value**
output of a cryptographic *hash function* (3.66)

**3.68**
**hybrid module**
*cryptographic module* (3.35) whose *cryptographic boundary* (3.32) delimits the composite of a *software* (3.140) or *firmware* (3.58) component and a disjoint *hardware* (3.64) component

Note 1 to entry: *Hybrid firmware module* (3.69) and *hybrid software module* (3.70) are the sub-categories of the hybrid module.

**3.69**
**hybrid firmware module**
*cryptographic module* (3.35) whose *cryptographic boundary* (3.32) delimits the composite of a *firmware* (3.58) component and a disjoint *hardware* (3.64) component (i.e. the firmware component is not contained within the hardware component)

Note 1 to entry: The computing platform and operating system of the operational environment in which the firmware executes are external to the defined hybrid firmware module's cryptographic boundary but explicitly bound to the hybrid firmware module.

**3.70**
**hybrid software module**
*cryptographic module* (3.35) whose *cryptographic boundary* (3.32) delimits the composite of a *software* (3.140) component and a disjoint *hardware* (3.64) component (i.e. the software component is not contained within the hardware component)

Note 1 to entry: The computing platform and operating system of the operational environment in which the software executes are external to the defined hybrid software module's cryptographic boundary.

**3.71**
**input data**
data (except control data entered via the *control input interface* (3.26)) that is input to and processed by a *cryptographic module* (3.35), including *plaintext* (3.105) data, ciphertext data, *sensitive security parameters* (3.132) and *status information* (3.145) from another module

**3.72**
**integrity**
property indicating that data have not been modified or deleted in an unauthorized and undetected manner

**3.73**
**logical interface**
interface
logical entry or exit point of a *cryptographic module* (3.35) that provides access to the module for logical information flows

Note 1 to entry: Logical interfaces are separated into seven categories: *data input interface* (3.38), *data output interface* (3.39), *control input interface* (3.26), *control output interface* (3.28), *status output interface* (3.147), *maintenance interface* (3.79), and *power interface* (3.108).

**3.74**
**key component**
parameter used in conjunction with other key components in an *approved security function* (3.8) to form a *plaintext* (3.105) *critical security parameter* (3.29) or perform a cryptographic function

**3.75**
**key loading device**
self-contained device that is capable of storing at least one *plaintext* (3.105) or encrypted *sensitive security parameter* (3.131) or *key component* (3.74) that can be transferred, upon request, into a *cryptographic module* (3.35)

Note 1 to entry: The use of a key loading device requires human manipulation.

**3.76**
**key management**
administration and use of the generation, establishment, entry and output, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation, and destruction of keying material in accordance with a security policy

**3.77**
**limited operational environment**
*operational environment* (3.96) that is designed to accept only controlled *firmware* (3.58) changes that successfully pass the *software/firmware load test* (3.143)

**3.78**
**low-level testing**
testing of the individual components or group of components of the *cryptographic module* (3.35) and their physical ports and *logical interfaces* (3.73)

**3.79**
**maintenance interface**
physical or logical interface to the *cryptographic module* (3.35) that is utilized when in a *maintenance role* (3.80)

**3.80**
**maintenance role**
*role* (3.119) assumed to perform either physical, logical or both physical and logical maintenance services

EXAMPLE Maintenance services can include but are not limited to *hardware* (3.64) and *software* (3.140) diagnostics.

**3.81**
**manual**
requiring human *operator* (3.98) manipulation

**3.82**
**message authentication code**
MAC
cryptographic checksum on data that uses a symmetric key which provides data source confirmation and the detection of both accidental and intentional modifications to data

EXAMPLE A hash-based message authentication code.

**3.83**
**microcode**
processor instructions that correspond to an executable program instruction

EXAMPLE Assembler code.

**3.84**
**minimum entropy**
lower bound of *entropy* (3.50) that is useful in determining a worst-case estimate of sample entropy

**3.85**
**modifiable operational environment**
*operational environment* (3.96) that is designed to accept functional changes that can contain non-controlled *software* (3.140) (i.e. untrusted)

**3.86**
**multi-factor authentication**
authentication of an *operator* (3.98) using at least two independent authentication factors

Note 1 to entry: All *authentication data* (3.13) is verified by the *cryptographic module* (3.35).

Note 2 to entry: An authentication factor is operator related information that resides outside the module, is used as proof of identity, and can include a method/process to produce varying or short-lived authentication data from the operator related information.

Note 3 to entry: Independent authentication factor categories for human operators include: something known, such as a secret *password* (3.102), something possessed, such as a physical key or token, and a physical property, such as a *biometric* (3.15).

**3.87**
**multiple-chip cryptographic module**
physical embodiment in which two or more integrated circuit chips are interconnected within a defined boundary

EXAMPLE Encrypting routers, secure radios, adapters, or expansion boards.

**3.88**
**non-administrator guidance**
written material that is used by either the *user* (3.154) or any other non-administrative *role* (3.119) for operating the *cryptographic module* (3.35)

Note 1 to entry: 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.

**3.89**
**non-invasive attack**
attack that uses side channels (information gained from the physical implementation) emitted by the *cryptographic module* (3.35)

Note 1 to entry: Examples of side channels include power consumption, electromagnetic emissions and computation time.

**3.90**
**non-modifiable operational environment**
*operational environment* (3.96) that is designed to not accept *firmware* (3.58) changes

**3.91**
**non-security relevant**
quality of a function or process implemented in a manner to not interfere or cause a *compromise* (3.19) to the approved secure operation of the *cryptographic module* (3.35)

**3.92**
**normal operating temperature**
range of operating temperatures defined by the *cryptographic module* (3.35) manufacturer over which the module can be expected to operate without experiencing any temperature induced errors

**3.93**
**normal operation**
operation where the entire set of security functions, services or processes are available and can be configured

**3.94**
**normal voltage range**
range of input voltages defined by the *cryptographic module* (3.35) manufacturer over which the module can be expected to operate without experiencing any voltage induced errors

**3.95**
**opaque**
impenetrable by light (i.e. light within the visible spectrum of wavelength range of 400 nm to 750 nm); neither transparent nor *translucent* (3.153) within the visible spectrum

**3.96**
**operational environment**
OE
operating system (including virtual machine(s) and *runtime environment* (3.121) where applicable) and *hardware* (3.64) platform required for the *cryptographic module* (3.35) to operate

Note 1 to entry: This can include, where applicable, integrated circuits, processors, libraries, memory management, process control, device drivers for hardware, power supplies and enclosures.

**3.97**
**operational state**
state where services or functions can be requested by an *operator* (3.98) and the data results output from the *data output interface* (3.39) of the *cryptographic module* (3.35)

**3.98**
**operator**
*entity* (3.49) external to the *cryptographic module* (3.35) that exercises the module's services via the provided interfaces

Note 1 to entry: In this definition, entity means an individual (person), organization, device, process or another module.

**3.99**
**output data**
data (except status data output via the *status output interface* (3.147) and control data output via the *control output interface* (3.28)) that is output from a *cryptographic module* (3.35) (including *plaintext* (3.105) data, ciphertext data, and *sensitive security parameters* (3.131))

**3.100**
**overall security rating**
minimum *security level* (3.128) of the independent *security level* (3.128) achieved in each security area

**3.101**
**passivation**
effect of a reactive process in semiconductor junctions, surfaces or elements and integrated circuits constructed to include means of detection and protection

EXAMPLE Silicon dioxide or phosphorus glass.

Note 1 to entry: Passivation can modify the behaviour of the circuit. Passivation material is technology dependant.

**3.102**
**password**
string of characters used to authenticate an identity or to verify access authorization

Note 1 to entry: Passwords can include letters, numbers, and other symbols.

**3.103**
**personal identification number**
PIN
numeric code used to authenticate an identity or to verify access authorization

**3.104**
**physical protection**
safeguarding of a *cryptographic module* (3.35), *critical security parameter* (3.29) and *public security parameter* (3.115) using physical means

**3.105**
**plaintext**
unencrypted, or obfuscated by non-approved methods

**3.106**
**plaintext trusted path**
protected communication link established between the *cryptographic module* (3.35) and a sender or receiver to securely communicate a *plaintext* (3.105) *critical security parameter* (3.29) or *key component* (3.74) without using cryptography

Note 1 to entry: A plaintext trusted path protects against eavesdropping, as well as physical or logical tampering, by an unwanted *operator* (3.98) or *entity* (3.49), between the module's defined input or output *port* (3.107) and along the communication link with the intended end point, without using cryptographic methods.

**3.107**
**port**
physical/logical input or output point of a *cryptographic module* (3.35) that provides access to the module

**3.108**
**power interface**
module interface(s) for which power is input to or output from a *cryptographic module* (3.35)

**3.109**
**pre-operational self-test**
test performed by a *cryptographic module* (3.35) after a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc.) and primary, secondary, or backup power is applied to the module, and before it transitions to the *operational state* (3.97)

**3.110**
**private key**
*cryptographic key* (3.34) of an entity's asymmetric key pair, which should only be used by that *entity* (3.49)

Note 1 to entry: 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.

**3.111**
**production-grade**
product, element or *software* (3.140) that has been tested to meet operational specifications

**3.112**
**protected internal path**
interfaces between integrated circuits within the *cryptographic boundary* (3.32) in a multi-chip module using approved cryptographic methods to protect the confidentiality and *integrity* (3.72) of the data

**3.113**
**public key**
*cryptographic key* (3.34) of an entity's asymmetric key pair, which can be made public

Note 1 to entry: 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.

**3.114**
**public key certificate**
electronic document used to prove the validity and origin of a *public key* (3.113)

**3.115**
**public security parameter**
PSP
security related public information whose modification can cause a *compromise* (3.19) of the security of a *cryptographic module* (3.35)

EXAMPLE *Public key* (3.113), *public key certificate* (3.114), self-signed certificate, trust anchor, one-time *password* (3.102) associated with a counter and internally held date and time.

Note 1 to entry: A PSP is considered protected if it cannot be modified or substituted without detection by the *cryptographic module* (3.35).

**3.116**
**random bit generator**
RBG
device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased

**3.117**
**rate limiting method**
method intended to slow down and render impractical *automated* (3.3) guessing attacks on *authentication data* (3.13)

EXAMPLE A time delay (fixed or increasing) between authentication attempts or locking the authentication mechanism.

**3.118**
**removable cover**
physical means which permits an intentionally designed non-damaging access to the physical contents of a *cryptographic module* (3.35)

**3.119**
**role**
security attribute associated with a user defining the user access rights or limitations when accessing services of a *cryptographic module* (3.35)

Note 1 to entry: 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.

**3.120**
**role-based access control**
permissions attributed to a *role* (3.119) granting access to an object

Note 1 to entry: An object can be data, a *service* (3.136), or other.

**3.121**
**runtime environment**
environment in which a program or application is executed

Note 1 to entry: It can pertain to the operating system itself, or the *software* (3.140) that runs beneath it. The primary purpose is to accomplish the objective of "platform independent" programming.

**3.122**
**salted password**
*password* (3.102) to which unique data has been added ahead of creating the stored password hash

**3.123**
**scheme owner**
person or organization responsible for developing and maintaining a specific certification scheme

Note 1 to entry: The scheme owner can be the certification body itself, a governmental authority, a trade association, a group of certification bodies or others.

Note 2 to entry: One of the responsibilities of a scheme owner for a scheme that assesses conformance to this document, is to be an approval authority, which approves security functions for use by the scheme.

[SOURCE: ISO/IEC 17065:2012, 3.11, modified — Note 2 to entry has been added.]

**3.124**
**secure container**
isolated execution space internal to the cryptographic module's physical enclosure where *firmware* (3.58) can execute in such a way that the module is protected against the *secure container firmware* (3.125) interfering or compromising the *cryptographic module* (3.35)

Note 1 to entry: Firmware executed within the secure container is considered outside the cryptographic boundary of the module and is not subject to requirements of this document other than requirements defined in 7.5.

**3.125**
**secure container firmware**
*firmware* (3.58) executing within a *secure container* (3.124)

**3.126**
**security function**
*cryptographic algorithm* (3.31) together with modes of operation, such as block ciphers, stream ciphers, symmetric or asymmetric key algorithms, message authentication codes, hash functions, random bit generators, etc. or other security functions such as entity authentication, *sensitive security parameter* (3.131) generation and establishment

**3.127**
**security level**
well-defined set of security requirements in a security area

**3.128**
**security relevant**
function of the *cryptographic module* (3.35) that, if bypassed, modified or substituted can ultimately contribute to the potential *compromise* (3.19) of the module

Note 1 to entry: This term is not the inverse of *non-security relevant* (3.91).

Note 2 to entry: Security relevant is considered as applicable within this scope of this document.

**3.129**
**seed**
secret value used to initialize a *random bit generator* (3.117)

**3.130**
**self-test**
pre-operational or conditional test executed by the *cryptographic module* (3.35)

**3.131**
**sensitive security parameter**
SSP
*critical security parameter* (3.29) or *public security parameter* (3.115)

**3.132**
**sensitive security parameter agreement**
**SSP agreement**
key establishment procedure where the resulting *cryptographic key* (3.34) is a function of information from two or more participants, so that no party can predetermine the value of the key independently of the other party's contribution

**3.133**
**sensitive security parameter establishment**
**SSP establishment**
process of making available a shared *sensitive security parameter* (3.131) (SSP) to one or more entities

Note 1 to entry: SSP establishment includes *SSP agreement* (3.132), *sensitive security parameter transport* (3.135) and SSP entry or output.

Note 2 to entry: *Automated* (3.3) SSP establishment can include generation and derivation.

**3.134**
**sensitive security parameter generation**
**SSP generation**
process of creating a *sensitive security parameter* (3.131) within the *cryptographic module* (3.35)

**3.135**
**sensitive security parameter transport**
**SSP transport**
process of transferring a *sensitive security parameter* (3.131) from one *entity* (3.49) to another entity using approved cryptographic methods

**3.136**
**service**
operation or function that can be performed by a *cryptographic module* (3.35) invoked by an external *operator* (3.98)

**3.137**
**service input**
data or *control information* (3.24) utilized by the *cryptographic module* (3.35) that initiates or obtains specific operations or functions

**3.138**
**service output**
data, control and *status information* (3.145) that results from operations or functions initiated or obtained by *service input* (3.137)

**3.139**
**single-chip cryptographic module**
physical embodiment in which a single integrated circuit (IC) chip is used as a standalone device or is embedded within an enclosure or a product

EXAMPLE Single IC chips or smart cards with a single IC chip.

Note 1 to entry: The enclosure can include non-IC components that are *security relevant* (3.128) and require physical protection.

Note 2 to entry: The enclosure can include other excluded IC components.

**3.140**
**software**
code that is executed in a *modifiable operational environment* (3.85)

**3.141**
**software module**
*cryptographic module* (3.35) whose *cryptographic boundary* (3.32) delimits the *software* (3.140) exclusive files(s), which can be one or multiple software files that execute(s) in a *modifiable operational environment* (3.85)

Note 1 to entry: The computing platform and operating system of the *operational environment* (3.96) in which the software executes are external to the defined software module's cryptographic boundary.

**3.142**
**software/firmware integrity test**
*self-test* (3.130) performed on the *software* (3.140) or *firmware* (3.58) components of a *cryptographic module* (3.35) to ensure *integrity* (3.72) of those components

**3.143**
**software/firmware load test**
conditional *self-test* (3.130) performed on *software* (3.140) or *firmware* (3.58) components after the components have been introduced into the *cryptographic module* (3.35) boundary, and which is passed successfully before the new components are executed by the module

**3.144**
**split-knowledge**
process by which a *cryptographic key* (3.34) is split into multiple key components, individually sharing no knowledge of the original key, which can be subsequently input, or output from, a *cryptographic module* (3.35) by separate operators and combined to recreate the original key

Note 1 to entry: All or a subset of the components are required to recover the original split-key.

**3.145**
**status information**
output signals, indicators (e.g. error indicator), and status data [e.g. 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* (3.35)

**3.146**
**status output**
*status information* (3.145) that is output from a *cryptographic module* (3.35)

**3.147**
**status output interface**
module interface(s) for which all *status output* (3.146) is output from the *cryptographic module* (3.35)

**3.148**
**strong**
not easily defeated, having strength or power greater than average or expected, able to withstand attack or solidly built

**3.149**
**tamper detection**
automatic determination by a *cryptographic module* (3.35) that an attempt has been made to cause a *compromise* (3.19) of the security of the cryptographic module

**3.150**
**tamper evidence**
observable indication that an attempt has been made to cause a *compromise* (3.19) of the security of a *cryptographic module* (3.35)

**3.151**
**tamper response**
automatic action taken by a *cryptographic module* (3.35) when *tamper detection* (3.149) has occurred

**3.152**
**temporary sensitive security parameter**
*sensitive security parameter* (3.131) (SSP) that, after its use to perform an approved function, is no longer needed

Note 1 to entry: Temporary SSPs are often ephemeral in nature and then cleared when no longer needed.

**3.153**
**translucent**
penetrable by light (i.e. light within the visible spectrum of wavelength range of 400 nm to 750 nm); yet preventing the gathering of information of the module's internal construction or components by direct visual observation using artificial light sources in the visual spectrum

**3.154**
**user**
*operator* (3.98) that accesses a *cryptographic module* (3.35) in order to perform general security services, including cryptographic operations and other *approved security function* (3.8)

**3.155**
**validated**
assurance of tested conformance to this document by a *certification body* (3.18)

**3.156**
**vendor**
*entity* (3.49), group or association that submits the *cryptographic module* (3.35) for testing and validation

Note 1 to entry: The vendor has access to all relevant documentation and design evidence regardless of whether they did or did not design or develop the cryptographic module.

**3.157**
**verifier data**
data used by the *cryptographic module* (3.35) to verify that the correct *authentication data* (3.13) was entered into the module by an *operator* (3.98) authenticating themselves to the module

Note 1 to entry: Verifier data resides inside the module (or its *operational environment* (3.96) if the operational environment implements the authentication mechanism as per 7.6.3.2), until it is updated or zeroized. It is possible that it was generated inside or outside the module. Verifier data are a *sensitive security parameter* (3.131).

EXAMPLE 1 Verifier data that is a *critical security parameter* (3.29) can include a *password* (3.102), *biometric* (3.15) data reference, or their hash.

EXAMPLE 2 Verifier data that is a *public security parameter* (3.115) can include a *public key* (3.113) or a *user* (3.154) *public key certificate* (3.114).

**3.158**
**zeroization**
method of destruction of a stored *plaintext* (3.105) or encrypted *critical security parameter* (3.29) and *public security parameter* (3.115) to prevent retrieval and reuse

Note 1 to entry: The zeroization of an encrypted critical security parameter depends on the level claimed in 7.9.7.

## 4 Abbreviated terms

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

| | |
|---|---|
| ACL | access control list |
| CBC | cipher block chaining |
| CCM | counter with cipher block chaining-message authentication code |
| CPLD | complex programmable logic device |
| CSP | critical security parameter |
| ECB | electronic codebook |
| EDC | error detection code |
| EFP | environmental failure protection |
| EFT | environmental failure testing |
| FPGA | field programmable gate array |
| FSM | finite state model |
| HDL | hardware description language |
| IC | integrated circuit |
| JRE | Java™ [a] runtime environment |
| OE | operational environment |
| PC | personal computer |
| PIN | personal identification number |
| PSP | public security parameter |
| RBG | random bit generator |
| SSP | sensitive security parameter |

[a] Java ™ is the trademark of a product supplied by Oracle. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of the product named.



# 5 Cryptographic module security levels

## 5.1 General

An overview of the four security levels is provided in 5.2 to 5.5. Common examples, given to illustrate how the requirements can be met, are not intended to be restrictive or exhaustive. 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 files, 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 subclause within Clause 7 and “yy” is a numeric index within the subclause.

## 5.2 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 as specified in Annex C shall be used). Software and hybrid software modules operate in a modifiable operational environment (OE). Hardware, firmware and hybrid firmware modules operate in a non-modifiable or limited OE. No specific physical

security mechanisms are required in a security level 1 hardware cryptographic module, beyond the basic requirement for production-grade elements. Non-invasive mitigation methods or mitigation of other attacks that are implemented are documented. CSPs may be manually entered and output from the module in plaintext form. They may also be entered and output electronically in plaintext form to and from software and hybrid software modules, provided that the module does not output them from the OE. Periodic self-tests may be triggered by the user.

An example of a security level 1 cryptographic module is a hardware encryption board found in a PC or a cryptographic toolkit executing in a hand-held device or general-purpose computer. Such implementations are 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 where it is to be deployed. For example, the implementation of security level 1 cryptographic module can be more cost-effective in such environments than corresponding modules at higher assurance levels which provide greater security of the module's SSPs. These modules enable organizations to select alternative cryptographic solutions to meet security requirements, where attention to the environment in which the module is operating is crucial in providing overall security.

## 5.3 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 is 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 unauthorized physical access.

Security level 2 requires role-based authentication in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform a corresponding set of services. A zeroization capability is offered by the cryptographic module.

Security level 2 allows a software or hybrid software cryptographic module to be executed in a modifiable environment that implements role-based access controls. Alternatively, the modifiable environment may, at a minimum, support a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions through multiple access control lists (ACLs). The capability protects against unauthorized execution, modification, and reading of cryptographic software. Software and firmware modules or the software and firmware components of hybrid modules use an approved integrity technique or EDC to protect module software or firmware integrity.

## 5.4 Security level 3

In addition to the tamper-evident physical security mechanisms required at security level 2, physical security at level 3 provides additional requirements to mitigate the unauthorized 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 zeroize all plaintext CSPs, plaintext PSPs and plaintext key components when the removable covers/doors of the cryptographic module are opened.

Roles, services, and authentication at 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 authorized to assume a specific role and perform a corresponding set of services.

SSP management at security level 3 requires manually established cryptographic keys to be encrypted or to utilize a plaintext trusted path, optionally with a split-knowledge procedure, for entry or output.

Physical 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 defeat a cryptographic module's defences. A cryptographic module is required to either include special environmental protection features designed to detect and protect the module when the voltage and temperature boundaries are exceeded, 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 cryptographic 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 document for software and hybrid software cryptographic modules, therefore, the highest overall security rating achievable by software and hybrid software cryptographic modules is limited to security rating 2.

Life-cycle assurances at security level 3 modules require additional methods, such as automated configuration management, detailed design and low-level testing.

## 5.5 Security level 4

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

At security level 4, in addition to the physical security requirements at security level 3, the module physical security mechanisms provide:

a) resistance to peeling, prying or dissolving of hard coating or strong enclosure or package 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); or

b) tamper detection and response with zeroization capability. The module detects and responds to all unauthorized 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 zeroization of all plaintext CSPs, plaintext PSPs and plaintext key components.

Security level 4 cryptographic modules are useful for operation in physically unprotected environments. Security level 4 introduces multi-factor authentication requirements for operator authentication.

At security level 4 a cryptographic module is required to include special environmental protection features, designed to detect voltage and temperature boundaries and zeroize all plaintext CSPs, plaintext PSPs and plaintext key components. This provides a reasonable assurance that the module will not be affected in a manner that can compromise the security of the module, when it is operating outside of the normal temperature and voltage range.

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

Security level 4 requires manually established cryptographic keys to be encrypted or to utilize a plaintext trusted path with a split-knowledge procedure for entry or output.

Security level 4 is not offered in all clauses of this document for software and hybrid software cryptographic modules.

The design of a security level 4 module is verified by the correspondence between both pre- and post-state conditions and the functional specification. Security level 4 also requires that, after delivery, the authorized operator be authenticated using vendor-provided operator related information.

# 6 Functional security objectives

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

a) employ and correctly implement the approved security functions for the protection of sensitive information;

b) protect a cryptographic module from unauthorized operation or use;

c) prevent the unauthorized disclosure of the contents of the cryptographic module, including CSPs;

d) prevent the unauthorized and undetected modification of the cryptographic module, approved security functions, including the unauthorized modification, substitution, insertion, and deletion of SSPs;

e) provide indications of the operational state of the cryptographic module;

f) ensure that the cryptographic module performs properly when executing approved services;

g) detect errors in the operation of the module and prevent the compromise of SSPs resulting from these errors; and

h) ensure the proper design, delivery and implementation of the cryptographic module.

# 7 Security requirements

## 7.1 General

This clause specifies the security requirements that cryptographic modules shall [AS01.01] follow. 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;

— mitigation of other attacks.

Table 1 summarizes the content in each of these areas.

A cryptographic module shall [AS01.02] be tested against the requirements of each area addressed in this clause. The cryptographic module level shall [AS01.03] be independently determined 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 level that reflects the highest-security level for which the module fulfils all 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 level commensurate with the overall security rating.

In addition to receiving independent levels for each of the security areas, a cryptographic module will also receive an overall security rating.

Many of the security requirements of this document include specific documentation requirements that are summarized in Annexes A and B. All documentation, including copies of the user and installation manuals, design specifications, and life-cycle documentation shall [AS01.04] be provided for a cryptographic module that undergoes independent testing.

Annexes C, D, E, F and G provide references to approved security functions, approved sensitive security parameter generation and establishment methods, approved authentication mechanisms, approved non-invasive attack mitigation test metrics and module secure development, manufacturing and operation.

**Table 1 — Summary of areas covered by 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 operation. Description of cryptographic module, including all hardware, software, and firmware components. All services provide status information to indicate when the service utilizes an approved security function or process in an approved manner. | | | |
| **Cryptographic module interfaces** | Required and optional interfaces.<br>Specification of all interfaces. | | Plaintext trusted path. | |
| **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 identity-based authentication. |
| **Software/firmware security** | Approved integrity technique.<br>Defined module interface. | Approved digital signature or keyed message authentication code-based integrity test. | Approved digital signature-based integrity test. | |
| | | Executable code. | | |
| | EDC-based or approved integrity test for firmware within either hardware module or disjoint hardware components of hybrid module. | | | |
| | A limited operational environment may support a secure container. | | | |
| **Operational environment** | Non-modifiable, limited or modifiable.<br>Control of SSPs. | Non-modifiable, limited.<br>The requirements in 7.6.3 are not applicable if the module is security level 2, 3 or 4 in 7.7. | | |
| | | Modifiable.<br>Role-based or discretionary access control.<br>Audit mechanism. | Not supported. | |
| **Physical security** | Production-grade elements. | Tamper evidence.<br>Opaque or translucent covering or enclosure. | Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing. EFP or EFT. | A hard, opaque removal-resistant coating or strong enclosure, or full enclosure in a tamper detection and response envelope. |
| **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. | |

**Table 1** *(continued)*

| | | Security level 1 | Security level 2 | Security level 3 | Security level 4 |
|---|---|---|---|---|---|
| **Sensitive security parameter management** | | Random bit generators, SSP generation, establishment, entry and output, storage and zeroization. | | | |
| | | Automated SSP transport or SSP agreement using approved methods. | | | |
| | | Manually established SSPs may be entered or output in plaintext form.<br>Plaintext CSPs and key components may be entered and output from software and hybrid software modules provided that the module does not output them from the OE. | | Manually established cryptographic keys may be entered or output in either encrypted form, or via a plaintext trusted path, optionally using split-knowledge procedures. | Manually established cryptographic keys may be entered or output in either encrypted form, or using a plaintext trusted path with split-knowledge procedures |
| | | Zeroization of plaintext CSPs, plaintext PSPs, and plaintext key components by operator procedure or via a service provided by the cryptographic module. | Zeroization of plaintext CSPs, plaintext PSPs, and plaintext key components via a service provided by the cryptographic module. | | Zeroization of all plaintext and encrypted CSPs and PSPs via a service provided by the cryptographic module. |
| **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. | | | |
| | | Periodic self-test | | Automated periodic self-test.<br>Error log protected against unauthorized modification and substitution. | |
| **Life-cycle Assurance** | **Configuration management** | Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout the life cycle. | | 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.<br>Hardware high-level descriptive language. | | Documentation annotated with pre-conditions upon entry into module components and post-conditions expected to be true when components are completed. |
| | **Vendor testing** | Functional testing. | | Low-level testing. | |
| | **Delivery and operation** | Initialization procedures. | Delivery procedures. | | Operator authentication using vendor provided operator related information. |
| | **Attestation** | A module may optionally support an attestation service to counter substitution attacks. Attestation standards are listed in Annex G. | | | |
| | **End of life** | Procedures for secure sanitisation. | | Procedures for secure destruction. | |
| | **Guidance** | Administrator and non-administrator guidance. | | | |

**Table 1** *(continued)*

| | Security level 1 | Security level 2 | Security level 3 | Security level 4 |
|---|---|---|---|---|
| **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 [AS02.01] be a set of hardware, software, firmware, or some combination thereof, which at a minimum, implements a defined cryptographic service employing an approved security function as specified in Annex C, or process, and is contained within a defined cryptographic boundary.

The documentation for cryptographic module specification specified in A.2.1 shall [AS02.02] be provided.

### 7.2.2 Types of cryptographic modules

A cryptographic module shall [AS02.03] be defined as either a hardware module, firmware module, hybrid firmware module, software module, or hybrid software module.

For hardware, firmware or hybrid firmware modules, the applicable physical security and non-invasive security requirements specified in 7.7 and 7.8 shall [AS02.04] apply.

For software modules and hybrid software modules executing in a modifiable operational environment, the physical security requirements specified in 7.7 are optional.

### 7.2.3 Cryptographic boundary

#### 7.2.3.1 Cryptographic boundary general requirements

A cryptographic boundary shall [AS02.05] 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 document shall [AS02.06] apply to all security functions, processes and components within the module's cryptographic boundary. The cryptographic boundary shall [AS02.07], at a minimum, encompass all security relevant security functions, processes and components of a cryptographic module as defined in Clause 7. Non-security relevant security functions, processes or components may be included within the cryptographic boundary. Non-security relevant security functions, processes or components may also be used in approved services. Non-security relevant security functions, processes or components which are used in approved services shall [AS02.08] be implemented in a manner so as to not interfere or compromise the approved operation of the cryptographic module.

The defined name of a cryptographic module shall [AS02.09] 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 [AS02.10] have, at a minimum, specific versioning information representing the distinct individual hardware and software or firmware components as applicable.

Hardware and either software or firmware components within the cryptographic boundary may be excluded from the requirements of this document. The excluded hardware, software or firmware components shall [AS02.11] be implemented in such a manner to not interfere or compromise the approved secure operation of the cryptographic module. Any excluded hardware, software or firmware residing within the module's cryptographic boundary shall [AS02.12] be specified in accordance with Annex A and listed in the module security policy in accordance with Annex B.

#### 7.2.3.2 Definitions of cryptographic boundary

The cryptographic boundary of a hardware cryptographic module shall [AS02.13] delimit and identify:

a) the set of hardware elements which may include:

   1) physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between elements;

   2) active electrical elements such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc; and

   3) physical structures, such as enclosures, potting or encapsulation materials, connectors and interfaces.

b) a limited or non-modifiable OE;

c) firmware, which may include an operating system; and

d) other element types not listed in a), b) or c), (e.g. configuration files for a CPLD).

The cryptographic boundary of a software cryptographic module shall [AS02.14] delimit and identify:

e) the set of executable files or other files that constitute the cryptographic module; and

f) 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 [AS02.15] delimit and identify:

g) the set of executable files or other files that constitute the cryptographic module; and

h) 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 [AS02.16]:

i) be the composite of the module's hardware component and the disjoint software or firmware component(s); and

j) include the collection of all ports and interfaces from each component.

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

### 7.2.4 Module operations

#### 7.2.4.1 Module operations general requirements

The operator shall [AS02.17] be able to operate the module utilizing approved services. An approved service shall [AS02.18] be defined as a service that includes at least one approved security function or process and can include non-security relevant functions or processes.

Non-approved security functions and processes shall not [AS02.19] be utilized by the operator in an approved service unless the non-approved security function or process is not security relevant to the approved process or service's operation (e.g. a non-approved security function or non-approved generated key may be used to obfuscate data or CSPs but the result is considered plaintext and provides no security relevant functionality until it is protected with an approved security function).

#### 7.2.4.2 Normal operation

Normal operation is where the entire set of approved security functions, services or processes are available and, where supported, can be configured.

CSPs shall [AS02.20] be exclusive between approved and non-approved services (e.g. not shared or accessed). CSPs may be accessible by both approved and non-approved services where it can be demonstrated that shared access cannot weaken the security of the CSP or increase its risk of compromise. The output of an approved random bit generator (RBG) may be provided to a non-approved algorithm, security function or process without the zeroization of the RBG seed, as long as the seed cannot be accessed by a non-approved service.

The module's security policy shall [AS02.21] define the complete set of services: approved, non-approved and non-security related.

Each service shall [AS02.22] provide an output indicator upon completion of the service to indicate whether the service executed an approved security function or process, or not.

If a singular service provides different outcomes based on the services configurable parameter setting, the output indicator in AS02.22 should reflect the particular parameter setting utilized upon the services execution.

NOTE AS02.22 is intended to provide an automated auditable indicator of usage of executable approved services.

EXAMPLE 1 A single encryption service utilizes different key strengths depending on an input parameter setting. The output indicator in AS02.22 reflects whether or not the parameter is set to an approved key strength.

EXAMPLE 2 A single encryption service simultaneously outputs both an encrypted result using an approved security function and a result based on a non-security relevant, non-approved security function. Since at least one output utilizes an approved security function, the output indicator in AS02.22 would indicate that an approved security function is executed. Examples of such implementations include double encryption, where the module relies on only one of the two layers of encryption to secure the data in an approved manner, or a protocol that uses a non-approved function but where that function does not affect the overall security of that protocol.

EXAMPLE 3 A single encryption service outputs an encrypted result using an approved security function or a result based on a non-approved security function, depending on which security function is requested by the operator (e.g. a digital signature service where a parameter selects among underlying hashes, at least one approved and at least one non-approved). The output indicator in AS02.22 only indicates when the approved security function is executed.

EXAMPLE 4 A single encryption service outputs a result using an approved security function in combination with a non-approved security function (e.g. a digital signature using a non-approved hash function). The output indicator in AS02.22 does not indicate that an approved function has been used.

EXAMPLE 5 The output indicator is a singular bit indicating whether the service executed an approved security function or process (e.g. a logical "1" for an approved security function or process and a logical "0" for all others).

#### 7.2.4.3 Degraded operation

A cryptographic module may be designed to support degraded operation if the module enters the error state. For a cryptographic module to operate in degraded operation, the following shall [AS02.23] apply:

a) degraded operation shall [AS02.24] be entered only after exiting an error state;

b) the module shall [AS02.25] provide status information when re-configured and degraded operation entered;

c) the mechanism or process that failed shall [AS02.26] be isolated;

d) all applicable conditional cryptographic algorithm self-tests shall [AS02.27] be performed prior to the first operational use of the cryptographic algorithm after entering degraded operation; and

e) services shall [AS02.28] provide an indicator if attempts are made to use the mechanism or process that failed.

The error state in AS02.24 may either impact the full module or be localized to the mechanism or process isolated in AS02.26. Where a localized error is used, it shall [AS02.29] be shown that the target error cannot impact other approved services running outside the isolated mechanism or process.

The cryptographic module shall [AS02.30] remain in degraded operation until the cryptographic module has repeated pre-operational test self-tests covering either the entire module or the failed isolated mechanisms and processes. When only a subset of pre-operational self-tests are re-run ahead of exiting degraded operation, it shall [AS02.31] be demonstrated why it was not necessary to re-run the excluded self-tests. 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 passes all the pre-operational self-tests while in degraded operation, the module shall [AS02.32] exit degraded operation. If the cryptographic module fails the pre-operational self-tests while in degraded operation, the module shall [AS02.33] enter an error state.

## 7.3 Cryptographic module interfaces

### 7.3.1 Cryptographic module interfaces general requirements

A cryptographic module shall [AS03.01] 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 [AS03.02] 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).

The documentation for cryptographic module interfaces specified in A.2.2 shall [AS03.03] be provided.

### 7.3.2 Types of interfaces

a) Hardware module interface: 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.

b) Software or firmware module interface: 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.

c) Hybrid software or hybrid firmware module interface: 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 Categories of interfaces

A cryptographic module's interfaces shall [AS03.04] be categorized into one or more of the following seven interface categories ("input" and "output" are indicated from the perspective of the module):

a) Data input interface: All input data shall [AS03.05] enter via the data input interface. Input data may be accepted by the module through the data input interface while the module is performing self-tests as defined in 7.10.

NOTE 1 Not applicable if a module does not receive data (e.g. module only generates random bit streams as an output).

b) Data output interface: All output data shall [AS03.06] exit via the data output interface. All output data shall [AS03.07] be inhibited while the cryptographic module is in an error state, and also inhibited while performing pre-operational self-tests as specified in 7.10.3, and zeroization as specified in 7.9.7.

NOTE 2 Not applicable if a module only outputs status or control information.

c) Control input interface: All control input shall [AS03.08] enter via the control input interface.

d) Control output interface: All control output shall [AS03.09] exit via the control output interface. All control output shall [AS03.10] be inhibited when the cryptographic module is in an error state unless exceptions are specified and documented in the security policy.

NOTE 3 Not applicable if a module does not output control information.

e) Status output interface: All status output shall [AS03.11] exit via the status output interface.

f) Maintenance interface: All physical and logical interfaces to the cryptographic module, which are utilized when in the maintenance role shall [AS03.12] be defined.

NOTE 4 Not applicable if a module does not implement a maintenance role.

g) Power interface: All external power shall [AS03.13] enter or exit via a power interface.

The cryptographic module shall [AS03.14] distinguish between data, control information and power for input to the module, and between data, control information, status information and power for output from the module.

The cryptographic module specification shall [AS03.15], unambiguously, specify format of input data and control information, including length restrictions for all variable length inputs. The cryptographic module shall [AS03.16] confirm that all inputs conform to the specifications in AS03.15.

EXAMPLE Examples of techniques used to confirm inputs include:

a) checking received parameter values to ensure that the lengths of parameters received match the ranges expected by the module and where they cannot exceed any allocated buffers when copied from input buffers to other regions of memory allocated internal to the module;

b) checking enumerated values to ensure a received command parameter matches supported options expected;

c) checking address ranges and sizes supplied for any read requests received to ensure that these can only reference authorized memory and where read lengths from an address do not exceed the permitted region that can be read;

d) where commands to a module have dependencies ahead of execution, checking that these dependencies have been met ahead of execution (e.g. where execution of a given command requires registers to have been set based on a prior module event, ensuring that the required event has occurred ahead of processing the requested command).

NOTE 5 Validation performed depends on the implementation technology used by the cryptographic module and on where a number of the checks (identified in the Example above) are performed automatically for memory-safe implementation languages.

NOTE 6 The list provided in the Example is not exhaustive and is provided as an example of potential validation only. Checks expected for a given module depend on the module and its implementation technology.

### 7.3.4 Plaintext trusted path

#### 7.3.4.1 general

A plaintext trusted path is a link established between the cryptographic module and a sender or receiver to securely communicate plaintext CSPs and key components without using encryption. A plaintext trusted path protects against eavesdropping, as well as physical or logical tampering by unauthorized operators or 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 end point.

Authentication to the plaintext trusted path itself is not required.

#### 7.3.4.2 Security levels 1 and 2

For security levels 1 and 2, there are no requirements for a plaintext trusted path.

#### 7.3.4.3 Security level 3

For security level 3:

a) for the transmission of plaintext CSPs and key components between the cryptographic module and the sender or receiver's end point, the cryptographic module shall [AS03.17] implement a plaintext trusted path;

b) the plaintext trusted path shall [AS03.18] prevent unauthorized modification, substitution, and disclosure along the communication link;

c) the physical ports used for the plaintext trusted path shall [AS03.19] be used only for the plaintext trusted path and be physically separated from all other ports, or the logical interfaces used for the plaintext trusted path shall [AS03.20] be logically separated from all other interfaces;

d) identity-based authentication shall [AS03.21] be employed for all services utilizing the plaintext trusted path; and

e) a status indicator shall [AS03.22] be provided when the plaintext trusted path is in use.

#### 7.3.4.4 Security level 4

In addition to the requirements of security level 3, multi-factor identity-based authentication or other authentication methods, as specified for security level 4 in Annex E, shall [AS03.23] be employed for all services utilizing the plaintext trusted path.

### 7.3.5 Protected internal paths

A module may have protected internal paths between ICs within the cryptographic boundary of multiple-chip modules, i.e. they are logically protected, but not physically protected by a potting material or enclosure. At security levels 2, 3, and 4, protected internal paths shall [AS03.24] employ approved cryptographic algorithms to provide confidentiality and integrity of security relevant data and controls.

## 7.4 Roles, services, and authentication

### 7.4.1 Roles, services, and authentication general requirements

A cryptographic module shall [AS04.01] support authorized 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 [AS04.02] internally maintain the separation of the roles assumed by each operator and the corresponding services. An operator is not required to assume an authorized 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 can be required within a cryptographic module to authenticate an operator accessing the module, and to verify that the operator is authorized to assume the requested role and perform the services within the role.

The documentation for roles, services and authentication specified in A.2.3 shall [AS04.03] be provided.

### 7.4.2 Roles

A cryptographic module shall [AS04.04], at a minimum, support a crypto officer role. The crypto officer role shall [AS04.05] be assumed to perform cryptographic initialization or management functions and general security services (e.g. module initialization, management of CSPs, PSPs and auditing).

A cryptographic module may support a user role. If the cryptographic module supports a user role, then the user role shall [AS04.06] 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 physical or logical maintenance services (e.g. opening service covers or performing certain diagnostics). All plaintext CSPs, plaintext PSPs and plaintext key components shall [AS04.07] be zeroized when entering and when exiting the maintenance role.

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

### 7.4.3 Services

#### 7.4.3.1 Services general requirements

Services shall [AS04.08] refer to all operations or functions that can be performed by a module. Service inputs shall [AS04.09] consist of all data or control inputs to the module that initiate or obtain specific services, operations or functions. Service outputs shall [AS04.10] 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 [AS04.11] result in a service output.

A cryptographic module shall [AS04.12] provide the following services to operators:

a) Show module's versioning information: The cryptographic module shall [AS04.13] output the name or module identifier, and the versioning information that can be correlated with a validation record (e.g. hardware and either software or firmware versioning information).

b) Show status: The cryptographic module shall [AS04.14] 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 [AS04.15] perform the pre-operational self-tests and conditional self-tests as specified in 7.10.

d) Perform approved security functions: The cryptographic module shall [AS04.16] perform at least one approved security function as specified in 7.2.

e) Perform zeroization: The cryptographic module shall [AS04.17] perform zeroization of the parameters as specified in 7.9.7.

A cryptographic module may provide other services (e.g. audit), operations or functions, both approved and non-approved, in addition to the services specified in a) to e). 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 Cryptographic bypass

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, and (as a result of module configuration or operator intervention) can also output the item in a non-protected form, then a bypass capability shall [AS04.18] be defined.

If a cryptographic module implements a bypass capability, then:

a) the operator shall [AS04.19] assume an authorized role before configuring the bypass capability;

b) two independent internal actions shall [AS04.20] be required by the module to activate the capability to prevent the inadvertent bypass of plaintext data due to a single error. The two independent internal actions shall [AS04.21] modify firmware, software, or hardware behaviour (or a combination) that is dedicated to mediating 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 [AS04.22] show its 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 are encrypted);

   2) is activated and the module is exclusively providing services without cryptographic processing (e.g. plaintext data are 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 can be encrypted or not, depending on the configuration of each channel).

#### 7.4.3.3 Re-authentication bypass

Re-authentication bypass is a configuration of the module that allows it to perform cryptographic operations and other approved security functions, or SSP management techniques which cannot compromise the security of the module, without re-authentication by the operator. The re-authentication bypass shall [AS04.23] only be enabled by the crypto officer. This configuration alongside any authentication state for operators may be preserved over resetting, rebooting or power cycling of the module.

If a cryptographic module implements a re-authentication bypass, then:

a) two independent internal actions shall [AS04.24] be required by the module to prevent inadvertent enabling of the re-authentication bypass due to a single error. The two independent internal actions shall [AS04.25] modify firmware, software or hardware behaviour (or a combination) that is dedicated to mediating the re-authentication bypass (e.g. two different software, firmware or hardware flags are set, one of which may be user-initiated); and

b) the module shall [AS04.26] show its status to indicate whether the re-authentication bypass is activated.

#### 7.4.3.4 Software/Firmware loading

If a cryptographic module has the capability of loading its software, firmware or bitstream components from an external source, then the following requirements shall [AS04.27] apply:

a) the security policy shall [AS04.28] specify that, by policy, the operator may only load software, firmware or bitstream validated by a certification body prior to loading to maintain validation, except when loaded into a secure container meeting the requirements of 7.5;

b) the software/firmware load test specified in 7.10.4.4 shall [AS04.29] be performed before the loaded code can be executed;

c) the cryptographic module shall [AS04.30] withhold execution of any loaded or modified approved security functions until after the pre-operational self-tests specified in 7.10.3 have been successfully executed. Pre-operational self-tests performed may cover either the full module or the loaded or modified code. Where pre-operational self-tests only cover the loaded or modified code, it shall [AS04.31] be demonstrated why the excluded self-tests are not re-run; and

d) the modules versioning information shall [AS04.32] be modified to represent the addition or update of the newly loaded software or firmware. This requirement does not apply when loaded firmware is contained within a secure container meeting the requirements of 7.5.

### 7.4.4 Authentication

#### 7.4.4.1 Authentication general requirements

Authentication mechanisms implemented within a cryptographic module authenticate an operator attempting to access the module. They also verify that the operator is authorized 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 [AS04.33] require that one or more roles either be implicitly or explicitly selected by the operator and shall [AS04.34] 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 [AS04.35] authenticate the assumption of any role that was not previously authenticated for that operator.

NOTE This assertion avoids privilege escalation.

b) Identity-based authentication: If identity-based authentication mechanisms are supported by a cryptographic module, the module shall [AS04.36] require that the operator be individually and uniquely

identified, shall [AS04.37] require that one or more roles either be implicitly or explicitly selected by the operator, and shall [AS04.38] authenticate the identity of the operator and that the operator is authorized to assume the selected role or set of roles. The authentication of the identity of the operator, selection of roles, and the authorization of the assumption of the selected roles may be combined. If a cryptographic module permits an operator to change roles, then the module shall [AS04.39] verify the authentication of the identified operator to assume any role that was not previously authenticated and the authorization of the identified operator to assume any role that was not previously authorized.

A cryptographic module may permit an authenticated operator to perform all services allowed within an authorized role or can 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 [AS04.40] require the operator to be authenticated, unless the re-authentication bypass is enabled. This requirement is not applicable if authentication status is not maintained (e.g. when the cryptographic module requires authentication for each service).

Authentication data within a cryptographic module shall [AS04.41] be protected against unauthorized use, disclosure, modification, and substitution. Verifier data within a cryptographic module shall [AS04.42] be protected against unauthorized use, disclosure, modification and substitution if it is considered a CSP, or shall [AS04.43] be protected against unauthorized modification and substitution if it is considered a PSP. Approved security functions may be used as part of the authentication mechanism.

The initialization of authentication mechanisms can warrant special treatment. If a cryptographic module does not contain the verifier data required to authenticate the operator for the first time the module is accessed, then other authentication methods (e.g. procedural controls) shall [AS04.44] be used to control access to the module and initialize the authentication mechanisms. If default verifier data are used to control access to the approved security functions and processes of the module, then on first-time authentication, new verifier data shall [AS04.45] be configured for use in subsequent authentication attempts by each role or identity. This requirement shall [AS04.46] be enforced by the module. This default verifier data are not required to meet the zeroization requirements of 7.9.7.

The authentication mechanism may be a group of mechanisms of different authentication properties that jointly meet the requirements of 7.4.4.

The following general authentication requirements apply to all modules at security level 2 or above in this clause:

c) The module shall [AS04.47] implement an approved authentication mechanism as referenced in Annex E.

d) The strength of the approved authentication mechanism shall [AS04.48] be specified in the security policy in accordance with Annex B.

e) If the cryptographic module uses security functions to authenticate the operator, then those security functions shall [AS04.49] be approved security functions.

f) For each attempt to use the approved authentication mechanism, the module shall [AS04.50] meet the strength of the authentication objective. For multiple attempts to use the approved authentication mechanism, the module shall [AS04.51] use a rate limiting method to meet the strength of the authentication objective.

g) The approved authentication mechanism shall [AS04.52] be met by the module's implementation and not rely on documented procedural controls or security rules (e.g. password size restrictions). Configuration of authentication mechanisms by the crypto officer is permitted prior to or when initializing an uninitialized role. This is permitted provided that configured authentication mechanisms for initialized roles cannot be bypassed based on this action.

h) For a software or hybrid software cryptographic module at security level 2 in 7.6.3, the operating system may implement the authentication mechanism at security level 2 or 3 (see 7.4). If the operating system implements the authentication mechanism, then the authentication mechanism shall [AS04.53] meet the requirements in 7.4.4 that are applicable to the claimed security level of the authentication mechanism.

i) Feedback of authentication data to an operator shall [AS04.54] be obscured during the authentication process to anyone other than the operator (e.g. when entering a password, individual characters are not displayed long enough for anyone other than the operator to see them). Non-significant characters may be displayed in place of the actual authentication data.

j) Feedback provided to an operator during an attempted authentication shall [AS04.55] prevent weakening of the authentication mechanism strength beyond the required authentication strength.

#### 7.4.4.2 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 [AS04.56] require that the operator either implicitly or explicitly select one or more roles.

#### 7.4.4.3 Security level 2

For security level 2, a cryptographic module shall [AS04.57] at a minimum employ role-based authentication to control access to the module.

#### 7.4.4.4 Security level 3

For security level 3, a cryptographic module shall [AS04.58] employ identity-based authentication mechanisms to control access to the module.

#### 7.4.4.5 Security level 4

In addition to the requirements at security level 3, a cryptographic module shall [AS04.59] employ multi-factor identity-based authentication mechanisms or another authentication method that meets security level 4 requirements in Annex E.

### 7.5 Software/firmware security

#### 7.5.1 Software/firmware security general requirements

A cryptographic module is defined as either a hardware, software, firmware or hybrid module (see 7.2.2). The requirements of this clause shall [AS05.01] apply to software, firmware or bitstream 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 document.

The public or secret key used for an approved integrity technique may reside within the module code and is not considered an SSP when considering zeroization.

A module with a limited OE may implement a controlled secure container at an internally defined boundary, that may include non-validated executable firmware. The secure container shall [AS05.02] be controlled to prevent the non-validated executable firmware within the secure container from interfering or compromising the cryptographic module. The following requirements shall [AS05.03] apply:

a) the software/firmware load test specified in 7.10.4.4 shall [AS05.04] be performed by the module before the firmware that is loaded into the secure container can be executed;

b) the boundary of the module with the secure container firmware shall [AS05.05] be defined;

c) the interfaces provided by the module to the secure container firmware shall [AS05.06] be defined (e.g. all interfaces that the module provides to the secure container to allow data and control input and output, status etc. to the module's external interfaces from the executing firmware in the secure container);

d) the services provided by the module to the secure container firmware shall [AS05.07] be defined;

e) all roles of the module that have access to the secure container firmware shall [AS05.08] be defined.

The documentation for software/firmware security specified in A.2.4 shall [AS05.09] be provided.

### 7.5.2 Security level 1

The following requirements shall [AS05.10] apply to software, firmware, or bitstream components of a cryptographic module for security level 1:

a) all software, firmware, or bitstream shall [AS05.11] be in a form that satisfies the requirements of this document without modification prior to installation;

b) for software and firmware modules and the disjoint software or firmware components of a hybrid module:

   1) a cryptographic mechanism using an approved integrity technique shall [AS05.12] be applied to all software and firmware components within the module's defined cryptographic boundary in one of the following ways:

      a) by the cryptographic module itself; or

      b) by another validated cryptographic module utilizing an approved service.

c) for firmware or bitstream components of a hardware cryptographic module and the firmware or bitstream components within a disjoint hardware component of a hybrid cryptographic module:

   1) a cryptographic mechanism using an approved integrity technique or an error detection code (EDC) shall [AS05.13] be applied to all firmware or bitstream 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 [AS05.14] be at least 16 bits in length.

d) 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 [AS05.15] enter the error state. The integrity test may consist of a single encompassing message authentication code; EDC; signature; or multiple disjoint authentication codes, EDCs or signatures of which failure of any disjoint authentication code, EDC or signature shall [AS05.16] cause the module to enter the error state. The expected referenced output of the integrity test mechanism may be considered data and not subject to the integrity test. The temporary value(s) generated during the integrity test of the module's software or firmware should be zeroized from the module upon completion of the integrity test;

e) an operator shall [AS05.17] be able to perform the integrity test on demand. Acceptable means to invoke the software/firmware integrity test on demand are: a provided service, resetting, rebooting, or power cycling;

f) all data and control inputs, and data, control and status outputs of the cryptographic module and services shall [AS05.18] be directed through a defined module interface;

g) if software, firmware, or bitstream is loaded and is associated, bound to, modifies or is an executable requisite of the validated module, then the software/firmware load test is applicable and shall [AS05.19] be performed by the validated module.

### 7.5.3 Security level 2

In addition to the requirements of security level 1, the following requirements shall [AS05.20] apply to software and firmware modules or the disjoint software and firmware components of a hybrid module for security level 2:

a) code shall [AS05.21] only be in executable form;

b) there shall [AS05.22] be no services or control settings via the module interface to allow the operator to initiate or perform debugging techniques when operational;

c) an approved digital signature or keyed message authentication code shall [AS05.23] 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 [AS05.24] enter the error state.

### 7.5.4 Security levels 3 and 4

In addition to the requirements of security levels 1 and 2, the following requirements shall [AS05.25] apply to software and firmware modules or the disjoint software and firmware components of a hybrid module for security levels 3 and 4:

a) a cryptographic mechanism using an approved digital signature shall [AS05.26] 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 [AS05.27] enter the error state; and

b) the digital signature technique may consist of a single encompassing signature or multiple disjoint signatures; failure of the verification of the single signature or any disjoint signature shall [AS05.28] cause the module to enter the error state. The private signing key shall [AS05.29] reside outside the module.

## 7.6 Operational environment

### 7.6.1 Operational environment general requirements

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 operational environment within the module consisting of an operating system which allows the execution of internal firmware. The operating system is considered to include, when applicable, the virtual machine(s) (system 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:

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

b) limited - this operational environment is designed or configured in a manner to allow controlled modification by an operator to the module components, the computing platform, or the operating system. This environment can 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) modifiable - this operational environment refers to an operational environment that may be reconfigured to add, delete or modify functionality and 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 an operator can load and execute software (e.g. a word processor) that is not part of the defined software or hybrid software module.

Hardware, firmware and hybrid firmware modules shall [AS06.01] use a non-modifiable or limited operational environment.

Software modules and hybrid software modules shall [AS06.02] use a modifiable operational environment.

A modifiable operational environment has the following characteristics:

d) Functions may be added or modified within the operational environment. It is possible that those functions will interfere with the operation of the cryptographic module unless such interference is prohibited by the operational environment;

e) Access to SSPs requires the use of the defined interfaces of the cryptographic module. Access to SSPs from outside the trusted part of the operational environment without using the defined interfaces of the cryptographic module is not permitted.

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 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 can 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 Table 2.

**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 document. | Limited |
| A computing platform that allows the loading of code without meeting the software loading requirements of this document. | 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 operational environment, the controlling components, which maintain the non-modifiable or limited operational environment, may include attributes of the computing platform, the operating system or the cryptographic module itself.

Code that is executed in a non-modifiable or limited operational environment is referred to as firmware within this document. Code that is executed in a modifiable operational environment is referred to as software within this document.

### 7.6.2 Clause applicability

If the operational environment is non-modifiable and the module is security level 1 in 7.7, the operating system requirements in 7.6.3 security level 1 shall [AS06.03] apply.

If the operational environment is a limited operational environment and the module is security level 1 in 7.7, the operating system requirements in 7.6.3 security level 1 shall [AS06.04] apply.

If the operational environment is a modifiable operational environment, the requirements in 7.6.3 shall [AS06.05] apply.

The documentation requirements for the operational environment specified in A.2.5 shall [AS06.06] be provided.

### 7.6.3 Operating system requirements for modifiable operational environments

#### 7.6.3.1 Security level 1

The following requirements apply to operating systems for security level 1:

a) Each instance of a cryptographic module shall [AS06.07] have control over its own SSPs.

b) The operating system shall [AS06.08] 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 of whether these data are 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 operating system shall [AS06.09] be documented in the security policy of the cryptographic module.

c) Processes that are spawned by the cryptographic module shall [AS06.10] be owned by the module and are not owned by external processes/operators.

These requirements cannot be enforced by administrative documentation and procedures and shall [AS06.11] be enforced by the operating system itself.

#### 7.6.3.2 Security level 2

In addition to the requirements of security level 1, for security level 2 an operating system shall [AS06.12] meet the following requirements, or as allowed by the certification body:

a) All cryptographic software, SSPs, control and status information shall [AS06.13] 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 [AS06.14] be configured to protect against unauthorized execution, unauthorized modification and unauthorized reading of SSPs, control and status data;

b) To protect plaintext data, cryptographic software and SSPs, the access control mechanisms of the operating system:

   1) shall [AS06.15] 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;

   2) shall [AS06.16] 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;

   3) shall [AS06.17] 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

   4) shall [AS06.18] 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.

c) The following specifications shall [AS06.19] be consistent with the roles or designated groups' rights and services as defined in the security policy:

   1) When not supporting a maintenance role, the operating system shall [AS06.20] 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);

2) The operating system shall [AS06.21] prevent user processes from gaining either read or write access to SSPs owned by other processes and to system SSPs; and

3) The configuration of the operating system that meets the above requirements shall [AS06.22] be specified in the administrator guidance. The administrator guidance shall [AS06.23] state that the operating system be configured as specified for the module contents to be considered protected.

The identification and authentication mechanism to the operating system shall [AS06.24] meet the requirements of 7.4.4 at security level 2, 3 or 4, and be specified in the module's security policy.

All cryptographic software, SSPs, control and status information shall [AS06.25] be under the control of an operating system. The operating system shall [AS06.26] have, at a minimum, the following attributes:

d) The operating system shall [AS06.27] provide an audit mechanism with the date and time of each audited event. The cryptographic module shall not [AS06.28] include SSPs as part of any audit record;

e) The cryptographic module shall [AS06.29] provide the following events to be recorded by the audit mechanism of the operating system:

1) modifications, accesses, deletions, and additions of cryptographic data and SSPs;

2) addition or deletion of an operator to and from a crypto officer role (if those roles are managed by the cryptographic module);

3) the use of a security-relevant crypto officer function;

4) requests to access verifier data associated with the cryptographic module;

5) the use of an authentication mechanism (e.g. login) associated with the cryptographic module; and

6) explicit requests to assume a crypto officer role.

f) The cryptographic module may record some or all events specified in e) with its own audit mechanism; regardless, all audit requirements in AS06.29 shall [AS06.30] be recorded, either by the operating system, module or a combination of both. The audit mechanism of the operating system shall [AS06.31] be capable of auditing the following operating system related events:

1) all operator read or write accesses to audit data stored in the audit trail;

2) access to files used by the cryptographic module to store cryptographic data or SSPs;

3) addition or deletion of an operator to and from a crypto officer role (if those roles are managed by operating system);

4) requests to use verifier data management mechanisms (if verifier data associated with the cryptographic module is managed by the operating system);

5) attempts to use the plaintext trusted path function and whether the request was granted, when plaintext trusted path is supported at this security level; and

6) identification of the initiator and target of a plaintext trusted path, when the plaintext trusted path is supported at this security level.

g) The operating system shall [AS06.32] 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 requirements specified in 7.6.3.2 shall [AS06.33] be permitted at security level 2. The audit record should be protected against unauthorized modification through the use of an approved security function.

## 7.7 Physical security

### 7.7.1 Physical security embodiments

A cryptographic module shall [AS07.01] employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module when installed.

All hardware, firmware, data elements and SSPs within the cryptographic boundary shall [AS07.02] be physically protected as specified for the target physical security level. A software or software component of a hybrid software cryptographic module is not subject to the physical security requirements of this document.

The requirements of 7.7 shall [AS07.03] be applicable to hardware and firmware modules, and hardware and firmware components of hybrid modules.

Physical security requirements are specified for two 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.

b) Multiple-chip cryptographic modules are physical embodiments in which two or more IC chips are interconnected.

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

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

d) during an access attempt where appropriate immediate actions is taken by the cryptographic module to protect SSPs and deter unauthorized use or modification of the module.

In the case of multiple-chip cryptographic modules, interconnected ICs may employ protected internal paths to protect security relevant data and controls passed between IC within cryptographic module boundary.

The requirements of 7.7 do not apply to excluded elements or interconnections.

Table 3 summarizes the physical security requirements: both general requirements and the two 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 |
|---|---|---|---|
| **Security level 1** | Production-grade elements.<br>Standard passivation.<br>Operator-initiated or automatic zeroization when accessing the maintenance interface. | No additional requirements. | |
| **Security level 2** | Evidence of tampering.<br>Opaque or translucent within the visible spectrum.<br>Prevent direct observation through holes and slits. | Tamper-evident encapsulating material, enclosure or package. | Entirely coated or enclosed in a tamper-evident material that may include doors or removable covers (excluding protected internal paths).<br>Tamper-evident seals or pick-resistant locks for doors or removable covers. |
| **Security level 3** | Tamper response and zeroization circuitry on doors and removable covers.<br>Automatic zeroization when accessing the maintenance interface.<br>Prevent probing through holes or slits. EFP or EFT for temperature and voltage. | Hard tamper-evident coating or within a strong enclosure or package with removal or penetration resistance. | Hard coating or within a strong enclosure with removal or penetration resistance (excluding protected internal paths). |
| **Security level 4** | EFP for temperature and voltage.<br>Protection from fault injection. | Resistance to peeling, prying or dissolving of hard coating or strong enclosure or package;<br>or<br>Tamper detection and response with zeroization capability. | Resistance to peeling, prying or dissolving of hard coating or strong enclosure. All exposed security relevant inter-IC connections are protected internal paths;<br>or<br>Tamper detection and response envelope with zeroization capability. |

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

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

The documentation for physical security specified in A.2.6 shall [AS07.04] be provided.

### 7.7.2 Physical security general requirements

#### 7.7.2.1 Physical security general requirements for all security levels

The following requirements shall [AS07.05] apply to all physical embodiments:

a) documentation shall [AS07.06] specify the physical embodiment of the cryptographic module;

b) whenever zeroization is performed for physical security purposes, the zeroization shall [AS07.07] occur in a sufficiently small time period so as to prevent the recovery of the zeroized SSP between the time of detection and the actual zeroization;

c) 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 authorized individual), then:

   1) a maintenance interface shall [AS07.08] be defined;

2) the maintenance interface shall [AS07.09] include all physical access paths to the contents of the cryptographic module, including any removable covers or doors; and

3) any removable covers or doors included within the maintenance interface shall [AS07.10] be safeguarded using the appropriate physical security mechanisms.

#### 7.7.2.2 Security level 1

The following requirements shall [AS07.11] apply to all cryptographic modules for security level 1:

a) the cryptographic module shall [AS07.12] consist of production-grade elements 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

b) when performing physical maintenance, zeroization shall [AS07.13] be performed either automatically by the cryptographic module or initiated by the operator.

EXAMPLE An example of performing maintenance for an IC is placing it into a test mode where internal memory or registers can be read or modified using methods that bypass controls that would be normally required for the module to meet the applicable requirements of this document.

#### 7.7.2.3 Security level 2

In addition to the general requirements for security level 1, the following requirements shall [AS07.14] apply to all cryptographic modules for security level 2:

a) The cryptographic module shall [AS07.15] either be:

1) entirely coated in a tamper evident material (excluding the protected internal paths); or

2) include an enclosure that may include doors or removable covers (excluding the protected internal paths).

EXAMPLE 1 Suitable coatings include epoxy resin and hard plastics.

EXAMPLE 2 Suitable container materials include metals and hard plastics.

b) If the module is in an enclosure containing doors or removable covers, then the doors or covers shall [AS07.16] be locked with pick-resistant mechanical locks employing physical or logical keys or shall [AS07.17] be protected with tamper-evident seals (e.g. evidence tape or holographic seals);

c) the cryptographic module shall [AS07.18] provide tamper evidence (e.g. on the cover, enclosure, coating, package, or seal) to provide detectable evidence of attempts to modify or access the module;

d) the tamper-evident material, coating, enclosure or package shall [AS07.19] either be opaque or translucent within the visible spectrum (i.e. light of wavelength range of 400 nm to 750 nm) to prevent the gathering of information about the internal operations of the critical areas of the module; and

e) if the cryptographic module contains ventilation holes or slits, then the module shall [AS07.20] be constructed in a manner to prevent the gathering of information of the module's internal construction or elements by direct visual observation using artificial light sources in the visual spectrum of the module's internal construction or elements.

#### 7.7.2.4 Security level 3

In addition to the general requirements for security levels 1 and 2, the following requirements shall [AS07.21] apply to all cryptographic modules for security level 3:

a) the module shall [AS07.22] be covered (excluding the protected internal paths) with a hard, opaque tamper-evident coating, enclosure or package to ensure that attempts at physical removal or penetration of the coating using non-chemical methods shall [AS07.23] have a high probability of causing serious damage to the cryptographic module;

b) if the cryptographic module contains any doors or removable covers or if a maintenance access interface is defined, then the module shall [AS07.24] contain tamper response and zeroization capability.

c) any tamper response and zeroization capability shall [AS07.25] immediately zeroize all plaintext CSPs, plaintext PSPs and plaintext key components when a tamper event is detected (e.g. a door is opened, a cover is removed, an internal tamper sensor is triggered such as a breach of a tamper detection envelope, or when the maintenance interface is accessed);

d) if a module supports a tamper response and zeroization capability, the tamper response and zeroization capability shall [AS07.26] remain operational while plaintext CSPs, plaintext PSPs and plaintext key components are contained within the cryptographic module. Zeroization triggered by the detection of a tamper event shall [AS07.27] be performed by the module without external module power and before the internal module power is insufficient for the module's zeroization circuitry to function;

e) if the cryptographic module contains ventilation holes or slits, then the module shall [AS07.28] be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g. prevent probing by a single articulated probe);

f) strong or hard conformal or non-conformal enclosures, coatings or potting materials shall [AS07.29] maintain strength and hardness characteristics over the module's intended temperature range of operation, storage and distribution; and

g) if tamper evident seals are employed, they shall [AS07.30] be uniquely numbered or independently identifiable (e.g. uniquely numbered evidence tape or uniquely identifiable holographic seals).

#### 7.7.2.5 Security level 4

In addition to the general requirements for security levels 1, 2, and 3, the following requirement shall [AS07.31] apply to all cryptographic modules for security level 4:

a) the cryptographic module shall [AS07.32] provide protection from fault injection. The fault injection mitigation techniques and the mitigation metrics employed shall [AS07.33] 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 for security levels 1, 2, 3 and 4, the following requirements shall [AS07.34] apply to single-chip cryptographic modules for security level 4:

a) the removal-resistant coating or strong enclosure shall [AS07.35] have solvency characteristics such that dissolving the coating or strong enclosure has a high probability of seriously damaging the module (i.e. the module will not function and be irreparably damaged); or

b) the module shall [AS07.36] provide a tamper detection envelope with tamper detection circuitry that shall [AS07.37] detect tampering by means such as cutting, drilling, milling, grinding, burning, melting, or dissolving of the single-chip module coating or package to a sufficient extent that would allow access to or modification of SSPs, or would result in unauthorized use or modification of the module.

#### 7.7.3.2 Multiple-chip cryptographic modules

In addition to the general physical security requirements for security levels 1, 2, 3 and 4 specified in 7.7.2, the following requirements shall [AS07.38] apply to multiple-chip cryptographic modules for security level 4:

a) All inter component interfaces carrying security relevant data and controls shall [AS07.39] be either a protected internal path or be fully enclosed in a tamper detection envelope with tamper detection circuitry.

b) All components shall [AS07.40] either be covered with a hard, opaque removal-resistant coating, strong enclosure, or be fully enclosed in a tamper detection envelope.

c) Where a tamper detection envelope is used, it shall [AS07.41] detect tampering by means such as cutting, drilling, milling, grinding, burning, melting, or dissolving of the module's enclosure to a sufficient extent that would allow access to or modification of SSPs, or would result in unauthorized use or modification of the module.

d) Where a hard opaque removal-resistant coating or strong enclosure is used, the material shall [AS07.42] have hardness and adhesion characteristics such that attempting to peel or pry the coating or strong enclosure from the module will have a high probability of resulting in serious damage to the module (i.e. the module will not function and be irreparably damaged).

e) Where a hard opaque removal-resistant coating or strong enclosure is used, the material shall [AS07.43] have solvency characteristics such that dissolving the coating or strong enclosure will have a high probability of dissolving or seriously damaging the module (i.e. the module will not function and be irreparably damaged).

f) Where a tamper detection envelope is used, the cryptographic module shall [AS07.44] contain tamper response and zeroization capability that continuously monitor the tamper detection envelope.

g) Where a tamper detection envelope is used, the cryptographic module on detection of tampering, shall [AS07.45] immediately zeroize all plaintext CSPs, plaintext PSPs and plaintext key components.

### 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 or unusual environmental conditions can be provided by having the module employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT).

#### 7.7.4.2 Security levels 1 and 2

The module is not required to employ EFP features or undergo EFT.

#### 7.7.4.3 Security level 3

The module shall [AS07.46] either employ EFP features or undergo EFT.

#### 7.7.4.4 Security level 4

The module shall [AS07.47] employ EFP features.

### 7.7.5 Environmental failure protection features

EFP features shall [AS07.48] 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 cryptographic module.

The cryptographic module shall [AS07.49] 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 [AS07.50] either:

a) shutdown the module to prevent further operation; or

b) immediately zeroize all plaintext CSPs, plaintext PSPs and plaintext key components.

### 7.7.6 Environmental failure testing procedures

EFT shall [AS07.51] 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 cryptographic module.

EFT shall [AS07.52] 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 [AS07.53] the security of the cryptographic module be compromised.

The temperature range to be tested shall [AS07.54] be from a temperature within the normal operating temperature range to the lowest (i.e. coldest) temperature outside of the normal operating range that results in the module either failing or entering an error state. The temperature range shall [AS07.55] also be from a temperature within the normal operating temperature range to the highest (i.e. hottest) temperature outside of the normal operating range that results in the module either failing or entering an error state. The temperature range to be tested shall [AS07.56] be from −100 °C to 200 °C; however, the test shall [AS07.57] be interrupted as soon as either the module fails or the module enters an error state. Temperature shall [AS07.58] be monitored internally at the sensitive elements and critical devices and not just at the module's cryptographic boundary.

The voltage range tested shall [AS07.59] be gradually decreasing from a voltage within the normal operating voltage range to a lower voltage outside of the normal voltage range that results in the module either failing or entering an error state. The voltage range tested shall [AS07.60] also be gradually increasing from a voltage within the normal operating voltage range to a higher voltage outside of the normal voltage range that results in the module either failing or entering an error state.

## 7.8 Non-invasive security

### 7.8.1 Non-invasive security general requirements

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 document are referenced in Annex F.

Requirements AS08.01 to AS08.06 are not applicable if the cryptographic module vendor does not claim non-invasive attack mitigation techniques to protect the module's plaintext CSPs from non-invasive attacks referenced in Annex F.

If no vendor claims are made, the vendor's public documentation should reflect that no claims have been made regarding non-invasive attack mitigation techniques.

The requirements in 7.8 are applicable if the cryptographic module implements at least one non-invasive attack mitigation technique to protect the module's plaintext CSPs 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 [AS08.01] meet the requirements in 7.12.

A module may implement a combination of mitigation techniques that are addressed in this subclause and mitigation techniques addressed in 7.12.

The documentation for non-invasive security specified in A.2.7 shall [AS08.02] be provided.

### 7.8.2 Security levels 1 and 2

For security levels 1 and 2, documentation shall [AS08.03] specify all of the mitigation techniques employed to protect the module's SSPs from the non-invasive attacks referenced in Annex F. Documentation shall [AS08.04] include evidence of the effectiveness of each of the attack mitigation techniques.

### 7.8.3 Security level 3

In addition to the requirements for security levels 1 and 2, the cryptographic module shall [AS08.05] be tested to meet the approved non-invasive attack mitigation test metrics for security level 3 as referenced in Annex F.

### 7.8.4 Security level 4

In addition to the requirements for security levels 1 and 2, the cryptographic module shall [AS08.06] 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

SSPs consist of CSPs and PSPs. The security requirements for SSP management encompass the entire life cycle of SSPs employed by the module. SSP management includes RBGs, SSP generation, SSP establishment, SSP entry/output, SSP storage, and plaintext CSP and PSP zeroization.

Encrypted CSPs refer to CSPs that are encrypted using an approved security function, as specified in Annex C. CSPs encrypted or obfuscated using non-approved security functions are considered unprotected within the scope of this document.

CSPs shall [AS09.01] be protected within the module from unauthorized access, use, disclosure, modification, and substitution.

PSPs shall [AS09.02] be protected within the module against unauthorized modification and substitution.

A module shall [AS09.03] 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.

Authentication data, verifier data that are not PSPs, RBG state information and intermediate key generation values shall [AS09.04] be considered as CSPs.

Hash values of passwords shall [AS09.05] be considered as CSPs unless they were generated using an approved password protection method (e.g. salt and hash) as specified in Annex E, in which case the hash values of passwords shall [AS09.06] be considered PSPs. When a hash function is used on passwords/PINs, whether it is on its own or as part of an approved password protection method in Annex E, then an approved hash algorithm as listed in Annex C shall [AS09.07] be used.

EXAMPLE 1 Verifier data that is a CSP includes a passwords, biometrics data reference, or their hash.

EXAMPLE 2 Verifier data that is a PSP includes public keys, user public key certificates, or hash values of salted passwords.

The documentation for sensitive security parameter management specified in A.2.8 shall [AS09.08] 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 requires random values, then an approved RBG shall [AS09.09] be used to provide these values.

Entropy input used to seed an approved RBG shall [AS09.10] 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 initialize the deterministic RBG) shall [AS09.11] 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 shall [AS09.12] be generated using approved sensitive security parameter generation methods listed in Annex D.

### 7.9.4 Automated sensitive security parameter establishment

Automated SSP establishment shall [AS09.13] use an approved method listed in Annex D.

### 7.9.5 Sensitive security parameter entry and output

#### 7.9.5.1 Sensitive security parameter entry and output general requirements

SSPs may be manually entered 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 operational environment). If SSPs are manually entered or output from a module, the entry or output shall [AS09.14] be through the defined module interfaces.

All cryptographically protected SSPs, entered or output from the module shall [AS09.15] be protected using an approved security function, as specified in Annex C.

PSPs may be entered or output from a cryptographic module in plaintext form. For SSPs which are directly entered manually, the entered values may be temporarily displayed to allow visual verification and to improve accuracy for the operator. If encrypted SSPs are directly entered manually into the module, then the plaintext values of the SSPs shall not [AS09.16] be displayed. Except for authentication data, manually directly entered (plaintext or encrypted) SSPs shall [AS09.17] be verified during entry into a module for accuracy using the conditional manual entry test specified in 7.10.4.5.

To prevent the inadvertent output of sensitive information, two independent internal actions shall [AS09.18] be required by the module in order to output any plaintext CSP; this requirement does not apply if AS09.22 is applicable.

For electronic entry or output via a wireless connection, CSPs and key components shall [AS09.19] be encrypted. Cryptographic keys established wirelessly using automated methods shall [AS09.20] use an approved method listed in Annex D.

If the cryptographic module employs split-knowledge procedures for cryptographic keys entry or output, at least two key components shall [AS09.21] be required by the module to reconstruct the original cryptographic key.

#### 7.9.5.2 Security levels 1 and 2

Plaintext cryptographic keys (when using manual entry or output, either directly or electronically), plaintext key components, plaintext verifier data 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 and key components may be entered or output from the module in plaintext form; in this case, the module shall not [AS09.22] output the CSPs and key components from the operational environment.

#### 7.9.5.3 Security level 3

Cryptographic keys, key components from split-knowledge procedures, and non-key CSPs entered or output from the cryptographic module using direct entry or electronic methods shall [AS09.23] either be encrypted or using a plaintext trusted path that meet security level 3 requirements in 7.3.4.

When entering or outputting key components from split-knowledge procedures, the module shall [AS09.24] authenticate each operator (i.e. each distinct key component importer or exporter) separately with an authentication that meets security level 3 requirements in 7.4.4.

#### 7.9.5.4 Security level 4

Cryptographic keys entered or output from the cryptographic module shall [AS09.25] either be encrypted or entered using split-knowledge procedures.

Key components from split-knowledge procedures and non-key CSPs shall [AS09.26] be entered or output from the module either encrypted or by a plaintext trusted path that meets security level 4 requirements in 7.3.4.

For key components entered or outputted as part of split-knowledge procedures, the module shall [AS09.27] authenticate each operator (i.e. each distinct key component importer/exporter) separately with an authentication that meets security level 4 requirements in 7.4.4.

### 7.9.6 Sensitive security parameter storage

A module shall [AS09.28] associate every SSP stored within the module with the entity (e.g. operator, role, or process) to which the SSP is assigned.

NOTE SSPs stored within the module are protected as part of AS09.01 and AS09.02.

### 7.9.7 Sensitive security parameter zeroization

#### 7.9.7.1 Sensitive security parameter zeroization general requirements

A module shall [AS09.29] provide methods to zeroize all plaintext CSPs, plaintext PSPs and plaintext key components within the module. Temporarily stored SSPs, key components and other stored values owned by the module should be zeroized when they are no longer required for future use. Inhibition of the data output interface is not a requirement when performing routine zeroization of temporary SSPs. Inhibition is exclusively required when zeroization is being performed in response to a user request or tamper event. The requirement to inhibit data output during zeroization is intended so that the target SSP to be zeroized (or derivation of these keys) are not exported or used in a way that can compromise the security of the SSP after the zeroization event is triggered. Zeroization of a subset of SSPs selected by the user outside the zeroization service does not require inhibition of the data output interface. Unless otherwise indicated, this clause does not apply to zeroization in response to tamper.

A zeroized SSP or key component shall not [AS09.30] be retrievable or reusable, including in response to tamper.

Except at security level 4, zeroization of encrypted CSPs, encrypted PSPs and encrypted key components is not required. Zeroization of CSPs, PSPs and key components otherwise physically or logically protected within an additional embedded validated module (meeting the requirements of this document) is not required. The goal of security level 4 zeroization, which requires the zeroization of all CSPs, PSPs and key components, whether protected or not, is to return the module to a factory state, i.e. the state it was in when shipped to the customer.

Zeroization of factory state PSPs is not required at any level.

Parameters used solely for self-test purposes as defined in 7.10 are not required to meet zeroization requirements.

Due to their purpose and the consequences of zeroization, some SSPs may be exempt from the zeroization requirements of AS04.07, AS04.17, AS07.13, AS07.25, AS07.45, AS07.50 and AS09.39. An exempt SSP may be used by services offered by the module that contribute to the security of the module where its compromise does not directly compromise user data, privacy or other SSPs which protect user data or privacy.

Where compromise of SSP can be shown to not directly compromise user data, physical destruction as a zeroization method is permitted at all levels.

#### 7.9.7.2 Security level 1

Zeroization may be performed procedurally by the module operator, and independent of the module's control (e.g. reformatting of a hard drive or the atmospheric destruction of a module during re-entry). If zeroization is performed procedurally, the security policy shall [AS09.31] provide instructions on how to perform the procedure, such that all plaintext CSPs, plaintext PSPs and plaintext key components are zeroized.

#### 7.9.7.3 Security levels 2 and 3

The cryptographic module shall [AS09.32] perform the zeroization of plaintext CSPs, plaintext PSPs and plaintext key components (e.g. overwriting with all zeros or all ones or with random data). When zeroizing plaintext CSPs or plaintext PSPs, or both in response to a user request or tamper, the module shall not [AS09.33] overwrite them with other plaintext CSPs or user PSPs, including in response to tamper. Temporary SSPs shall [AS09.34] be zeroized when they are no longer required, however, in this case AS09.35 and AS03.07 are not applicable.

The module shall [AS09.35] provide an output status indication when the zeroization of plaintext CSPs, plaintext PSPs and plaintext key components is complete, including in response to tamper.

NOTE If zeroization is performed as a result of a tamper event, it is possible that the module does not report an output status indicator if the module is no longer in an operational state.

An output status indicator is not required when temporary SSPs and other stored values owned by the module are zeroized.

#### 7.9.7.4 Security level 4

In addition to the requirements of security levels 2, and 3, the following requirements shall [AS09.36] be met:

a) the zeroization shall [AS09.37] be immediate and non-interruptible, and shall [AS09.38] occur in a sufficiently small time period so as to prevent the recovery of the SSP being zeroized between the time zeroization is initiated and the actual zeroization completed, including in response to tamper; and

b) all SSPs shall [AS09.39] be zeroized, including in response to tamper, 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 provide the operator assurance that faults have not been introduced that would prevent the module's correct operation. All self-tests shall [AS10.01] be performed by the module, without external controls, externally provided input test vectors, expected output results, or operator intervention, and regardless of whether the module will operate an approved or non-approved service. The determination of pass or fail shall [AS10.02] be made by the module, without external controls, externally provided input test vectors, expected output results, or operator intervention, and regardless of the module will operate an approved or non-approved service.

The pre-operational self-tests shall [AS10.03] be performed and passed successfully prior to the module providing any data output via the data output interface.

Conditional self-tests shall [AS10.04] be performed when an applicable cryptographic algorithm or process is invoked (i.e. cryptographic algorithms for which self-tests are required).

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

All self-tests identified in the underlying standards in Annex C, Annex D and Annex E shall [AS10.05] be implemented as applicable. All self-tests identified in addition to or in lieu of those specified in the underlying standards in Annex C, Annex D and Annex E shall [AS10.06] be implemented as referenced in Annex C, Annex D and Annex E for each approved security function.

A self-test may be performed as a set of disjoint self-tests.

If a cryptographic module fails a self-test, the module: shall [AS10.07] enter an error state, or shall [AS10.08] behave as specified by the certification body for that particular self-test failure, if that self-test is defined in the underlying standards in Annex C, Annex D and Annex E.

If a cryptographic module fails the conditional manual entry test or the conditional software/firmware load test, and in some cases the conditional critical function test, the module shall [AS10.09] indicate the test failed, but the module is not required to enter an error state, inhibit data output, or cease cryptographic processing.

Entering an error state for a conditional critical function test failure as defined in 7.10.4.7 will be dependent on whether the test is checking the integrity of data from outside the module boundary. In situations where integrity failures are detected for operator or system provided data to the module, it is sufficient for the module to return an error to the calling function or application and reject the data without entering an error state as the detected error is with the supplied data and not the module's ability to function or process data.

The operator of the module shall [AS10.10] be able to determine if the module has entered an error state either by an error indicator output by the module or implicitly through an unambiguous procedure documented in the security policy. The cryptographic module shall not [AS10.11] 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 [AS10.12] utilize 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.

### 7.10.2 Security levels 3 and 4

At security levels 3 and 4, the module shall [AS10.13] maintain an error log that contains at a minimum, the most recent error event (i.e. which self-test failed). The error log shall [AS10.14] be protected against unauthorized modification and substitution.

The documentation for self-tests specified in A.2.9 shall [AS10.15] be provided.

### 7.10.3 Pre-operational self-tests

#### 7.10.3.1 Pre-operational self-test general requirements

The pre-operational self-tests shall [AS10.16] be performed and passed successfully by a cryptographic module:

a) after a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc.);

b) before the primary, secondary, or backup power is applied to the module; and

c) before the module transitions to the operational state.

A cryptographic module shall [AS10.17] perform the following pre-operational self-tests, as applicable:

d) pre-operational software/firmware integrity test;

e) pre-operational bypass test; and

f) pre-operational critical functions test.

#### 7.10.3.2 Pre-operational software/firmware integrity test

All software, firmware and bitstream components within the cryptographic boundary shall [AS10.18] 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 [AS10.19] fail. The pre-operational software/firmware integrity test is not required for any software, firmware or bitstream excluded from the security requirements of this document or for any executable code stored in non-reconfigurable memory.

If a hardware module does not contain firmware or bitstream, the module shall [AS10.20], at a minimum, implement one conditional cryptographic algorithm self-test as specified in 7.10.4.2 as a pre-operational self-test.

The conditional cryptographic algorithm self-test may be satisfied if the cryptographic algorithm is utilized by the approved integrity technique for the pre-operational software/firmware integrity test.

#### 7.10.3.3 Pre-operational bypass test

If a cryptographic module implements a bypass capability, then the module shall [AS10.21] ensure the correct operation of the logic governing activation of the bypass capability by exercising that logic. The module shall [AS10.22] also verify the data path by:

a) setting the bypass switch to provide cryptographic processing and verify that data transferred through the bypass mechanism is cryptographically processed; and

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

#### 7.10.3.4 Pre-operational critical functions test

There may be other security functions critical to the secure operation of a cryptographic module that shall [AS10.23] be tested as a pre-operational test. Documentation shall [AS10.24] specify the pre-operational critical functions that are tested.

### 7.10.4 Conditional self-tests

#### 7.10.4.1 Conditional self-test general requirements

Conditional self-tests shall [AS10.25] 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.

#### 7.10.4.2 Conditional cryptographic algorithm self-test

A cryptographic algorithm self-test shall [AS10.26] be conducted for all approved cryptographic algorithms as referenced in Annex C, which references Annex D.

The conditional cryptographic algorithm self-test shall [AS10.27] be executed prior to the first operational use of the cryptographic algorithm after power-on, a new instantiation of the module or periodic self-test request.

A cryptographic algorithm self-test can 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 [AS10.28] fail.

A cryptographic algorithm self-test that is supported by the module shall [AS10.29], at a minimum, use any approved key length, modulus size, DSA prime, or curve that is supported by the module.

If a cryptographic algorithm specifies multiple modes (e.g. ECB and CBC), at a minimum, one mode shall [AS10.30] be selected for the self-test that is supported by the module. The following are the requirements for self-tests for one-way functions and reversible functions:

a) One-way functions: Input test vector(s) generate output which shall [AS10.31] be identical to expected output [e.g. hashing, keyed hashes, message authentication, RBG (fixed entropy input), SSP agreement].

b) Reversible functions: The forward and reverse function shall [AS10.32] be self-tested before each is separately used (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 [AS10.33] fail.

NOTE The comparison test is continuous and is run every time the two or more independent cryptographic algorithm implementations are executed.

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 self-test for fault detection shall [AS10.34] fail.

EXAMPLE The fault-detection test of the RBG will cover an error of the entropy source being correctly handled inside the implementation of the RBG.

#### 7.10.4.3 Conditional pair-wise consistency test

If a cryptographic module generates asymmetric key pairs, a pair-wise consistency test shall [AS10.35] be performed for every generated asymmetric key pair as referenced in Annex C for the applicable cryptographic algorithm.

NOTE An asymmetric key pair consists of a public and private key.

#### 7.10.4.4 Conditional software/firmware load test

If a cryptographic module has the capability of loading software, firmware or bitstream from an external source, then the following requirements in addition to those in 7.4.3.4 shall [AS10.36] be performed:

a) The cryptographic module shall [AS10.37] implement an approved data authentication technique to verify the authenticity of the software, firmware, or bitstream that is loaded.

NOTE 1 The approved data authentication technique can consist of a single encompassing message authentication code or signature, or multiple disjoint authentication codes or signatures.

b) The reference authentication key shall [AS10.38] be loaded independently in the module prior to the software, firmware, or bitstream loading.

c) The applied approved data authentication technique shall [AS10.39] be successfully verified or the software/firmware load test shall [AS10.40] fail. Loaded software, firmware, or bitstream shall not [AS10.41] be used if the software/firmware load test fails.

d) The software/firmware load test shall [AS10.42] be performed and pass successfully prior to the first execution of any new software, firmware or bitstream components. The software/firmware load test is not required to be performed immediately after software, firmware or bitstream components have been

introduced into the module boundary. A module can delay execution of these tests until first execution of the target new or updated components.

NOTE 2 The software/firmware load test is considered to be inherently performed by performing software/firmware integrity test after introducing the software, firmware or bitstream into the module if all following conditions are met: the software/firmware load test and the software/firmware integrity test use the same cryptographic algorithm, the cryptographic algorithm self-test has been already conducted and successfully completed for this cryptographic algorithm, and software, firmware or bitstream introduced into the module cannot be executed until software/firmware integrity successfully passes.

#### 7.10.4.5 Conditional manual entry test

If SSPs or key components are manually entered directly into a cryptographic module or if an 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 [AS10.43] be performed:

a) The SSP or key components shall [AS10.44] have an EDC applied or shall [AS10.45] be entered using duplicate entries.

When an operator is authenticating, authentication data entered into the module is not required to meet requirements in 7.10.4.5.

If an EDC is used, the EDC shall [AS10.46] be at least 16 bits in length. If the EDC cannot be verified, or the duplicate entries do not match, the test shall [AS10.47] fail.

#### 7.10.4.6 Conditional bypass test

If a cryptographic module implements a bypass capability where the services may be provided without cryptographic processing (e.g. transferring plaintext data through the module), then the following suite of bypass tests shall [AS10.48] be performed to ensure that a single point of failure of module components will not result in the unintentional output of plaintext data:

a) a cryptographic module shall [AS10.49] 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;

b) 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 [AS10.50] 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); and

c) if a cryptographic module maintains internal information that governs the bypass capability, then the module shall [AS10.51] verify the integrity of the governing information through an approved integrity technique immediately preceding modification of the governing information, and shall [AS10.52] generate a new integrity value using the approved integrity technique immediately following the modification.

#### 7.10.4.7 Conditional critical functions test

There may be other security functions critical to the secure operation of a cryptographic module that shall [AS10.53] be tested as a conditional self-test.

#### 7.10.4.8 Periodic self-tests

##### 7.10.4.8.1 Security levels 1 and 2

A cryptographic module shall [AS10.54] permit operators to initiate the pre-operational or conditional cryptographic algorithm 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.

#### 7.10.4.8.2 Security levels 3 and 4

In addition to the requirements at security levels 1 and 2, the module shall [AS10.55] repeatedly and automatically, upon a defined time period, without external input or control, perform the pre-operational or conditional cryptographic algorithm self-tests. The time period and any conditions that can result in the interruption of the module's operations during the time to repeat the pre-operational or conditional cryptographic algorithm self-tests shall [AS10.56] be specified in the security policy.

If the module is performing mission critical services that cannot be interrupted and the time period has passed for the initiation of the pre-operational self-tests, the self-tests may be deferred after the time period is passed again.

If the operational time period of a module between resetting, rebooting, or power cycling is sufficiently short, the periodic self-test requirements may be omitted; in this case, the security policy shall [AS10.57] document the expected operational time period of the module, and that periodic self-tests are therefore not required.

NOTE Time is a relative period generated internal to the module. Examples of methods of measuring time periods include clock cycles, counters, or command or operation counts.

## 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 for life-cycle assurance specified in A.2.10 shall [AS11.01] be provided.

### 7.11.2 Configuration management

#### 7.11.2.1 General

A configuration management system is put in place to prevent accidental or unauthorized modifications to, and provide change traceability for, the cryptographic module and related documentation.

#### 7.11.2.2 Security levels 1 and 2

The following requirements shall [AS11.02] apply for security levels 1 and 2:

a) a configuration management system shall [AS11.03] be used for the development of a cryptographic module and module components within the cryptographic boundary, and of associated module documentation;

b) each version of each configuration item (e.g. hardware, software, and firmware components, module HDL, user guidance, security policy) that comprises the module and associated documentation shall [AS11.04] be assigned and labelled with a unique identifier;

c) the configuration management system shall [AS11.05] 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;

d) the vendor shall [AS11.06] protect confidential module documentation from unauthorized access.

#### 7.11.2.3 Security levels 3 and 4

In addition to the requirements for security levels 1 and 2, the configuration items shall [AS11.07] 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 [AS11.08] 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 [AS11.09] be specified using a finite state model (FSM), or equivalent, represented by a state transition diagram and a state transition table and state descriptions. The FSM shall [AS11.10] be sufficiently detailed to demonstrate that the cryptographic module complies with the relevant requirements of this document.

The FSM of a cryptographic module shall [AS11.11] include, as a minimum, the following distinct operational and error states:

a) Power-off state: A state in which the module is powered off. All primary, secondary, or backup power is no longer applied to the module. For a software or firmware module and the software or firmware components of a hybrid module, power-off is the action of terminating the executable image(s) of the software or firmware module or the software or firmware components of a hybrid module.

b) Power-on state: A state in which the module is powered on (after power-off, reset, reboot, cold-start, power interruption) and primary, secondary or backup power is applied to the module. For a software or firmware module and the software or firmware components of a hybrid module, power-on is the action of spawning an executable image of the software or firmware module or the software or firmware components of a hybrid module.

c) General initialization state: A state in which the cryptographic module is undergoing initializing before the module transitions to the approved state.

d) Crypto officer state: A state in which the crypto officer services are performed (e.g. cryptographic initialization, secure administration, and key management) and in which authorized users obtain security services, perform cryptographic operations, or perform other approved functions).

e) CSP entry state (if CSP entry is implemented): A state for entering the CSPs into the cryptographic module.

f) Self-test state: A state in which the cryptographic module is performing self-tests.

g) Error state: A state when the cryptographic module has encountered an error condition (e.g. failed a self-test). There can be one or more error conditions that result in a single module error state. Error states can include “hard” errors that indicate an equipment malfunction and that can require maintenance, service or repair of the cryptographic module, or recoverable “soft” errors that can require initialization or resetting of the module. Recovery from error states shall [AS11.12] be possible, except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.

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

h) Maintenance state. A state assumed to perform physical or logical maintenance services while performing in the maintenance role.

i) 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.

j) Degraded state. A state that supports degraded operation in 7.2.4.3.

k) Quiescent state. A state in which the cryptographic module is dormant (e.g. low power, suspended or in hibernation).

l) User state. A state in which the user services are performed, and in which authorized users obtain security services, perform cryptographic operations, or perform other approved functions).

NOTE Exiting from the quiescent state is not considered transitioning through a power-on state.

### 7.11.5 Development

#### 7.11.5.1 General

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. 7.11.5.2 to 7.11.5.4 specify 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.

#### 7.11.5.2 Security level 1

The following requirements shall [AS11.13] apply to cryptographic modules for security level 1:

a) if a cryptographic module contains software or firmware, the following elements shall [AS11.14] be tracked using the configuration management system: 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;

b) if a cryptographic module contains software or firmware, the source codes shall [AS11.15] be annotated with comments that depict the correspondence of the software or firmware to the design of the module;

c) if a cryptographic module contains hardware, documentation shall [AS11.16] specify the schematics or hardware description language (HDL), or both, as applicable;

d) if a cryptographic module contains hardware, and if HDL is used to specify the hardware, the HDL shall [AS11.17] be annotated with comments that depict the correspondence of the hardware to the design of the module;

e) for software and firmware cryptographic modules and the software or firmware component of a hybrid module:

   1) the result of the approved integrity and data authentication techniques specified in 7.5 and 7.10 shall [AS11.18] be calculated and integrated into the software, firmware or hybrid module by the vendor during the module development;

   2) the cryptographic module documentation shall [AS11.19] specify the compiler, configuration settings and methods to compile the source code into an executable form; and

   3) the cryptographic module shall [AS11.20] be developed using production-grade development tools (e.g. compilers).

#### 7.11.5.3 Security levels 2 and 3

In addition to the requirements for security level 1, the following requirements shall [AS11.21] apply to cryptographic modules for security levels 2 and 3:

a) all software or firmware shall [AS11.22] be implemented using a high-level, non-proprietary language or rationale shall [AS11.23] be provided to justify 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;

b) custom integrated circuits within a cryptographic module shall [AS11.24] be created using methods that support comprehension or analysis, e.g. using a high-level HDL or a schematic for analogue elements;

c) all software or firmware shall [AS11.25] 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; and

d) the module shall [AS11.26] be designed and implemented in a manner that utilizes the requirements as defined in Annex G.

#### 7.11.5.4 Security level 4

In addition to the requirements for security levels 1, 2 and 3, the following requirement shall [AS11.27] apply to cryptographic modules for security level 4:

a) for each cryptographic module hardware, software and firmware component, the documentation shall [AS11.28] 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, or procedure is complete.

### 7.11.6 Vendor testing

#### 7.11.6.1 General

7.11.6.2 and 7.11.6.3 specify 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 according to the functional specifications.

#### 7.11.6.2 Security levels 1 and 2

For security levels 1 and 2, documentation shall [AS11.29] specify the functional testing performed on the cryptographic module.

The vendor shall [AS11.30] use automated security diagnostic tools (e.g. detect buffer overflow) for software or firmware cryptographic modules and the software or firmware component of a hybrid module, or the firmware component of a hardware module.

#### 7.11.6.3 Security levels 3 and 4

In addition to the requirements for security levels 1 and 2, documentation shall [AS11.31] specify the procedures for and the results of low-level testing performed on the cryptographic module.

### 7.11.7 Delivery and operation

#### 7.11.7.1 General

7.11.7.2 to 7.11.7.5 specify the security requirements for the secure delivery, installation and start-up of a cryptographic module, providing assurance that the module is securely delivered to authorized operators, and is installed and initialized in a correct and secure manner.

#### 7.11.7.2 Security level 1

For security level 1, documentation shall [AS11.32] specify the procedures for secure installation, initialization, and start-up of the cryptographic module.

#### 7.11.7.3 Security levels 2 and 3

In addition to the requirement of security level 1, documentation shall [AS11.33] specify the procedures required for maintaining security while distributing, installation and the initialization of versions of a cryptographic module to authorized operators. The procedures shall [AS11.34] specify how to detect tamper during the delivery, installation and initialization of the module to the authorized operators.

#### 7.11.7.4 Security level 4

In addition to the requirements of security levels 1, 2 and 3, the procedures shall [AS11.35] require the authorized operator to be authenticated by the module using the operator specific authentication data provided by the vendor.

#### 7.11.7.5 Attestation

This subclause is not applicable if the cryptographic module vendor does not claim support for the attester service component of attestation for the module.

If no vendor claims are made, the vendor's public documentation should reflect that no claims have been made regarding attestation.

In order to counter substitution attacks on a given cryptographic module, a cryptographic module may support the attester service to aid with both uniquely identifying a target module alongside allowing reporting of the integrity of the module and its configuration.

If the cryptographic module supports the attester service:

a) the attester service shall [AS11.36] be designed and implemented in a manner that complies with applicable standards and requirements for the attester as defined in Annex G; and

b) the module security policy shall [AS11.37] provide guidance to the user on using the module's attester service including how to retrieve any required module cryptographic identity and retrieve attestation records; how to verify the records; and the type of measurements contained within the records returned by the module.

#### 7.11.7.6 End of life

##### 7.11.7.6.1 End of life general requirements

7.11.7.6.2 and 7.11.7.6.3 specify the security requirements when a cryptographic module is no longer deployed or intended for further use by the operator.

The security policy shall [AS11.38] document end of life procedures, provide a summary of end of life procedures, or an external publicly available reference to where the modules end of life procedures can be found.

NOTE Procedures can include multiple methods such as zeroization or physical destruction.

##### 7.11.7.6.2 Security levels 1 and 2

For security level 1 and 2, documentation shall [AS11.39] specify the procedures for secure sanitization of the cryptographic module. Sanitization is the process of removing sensitive information (e.g. CSPs, PSPs, key components, user data) from the module, so that it can then be either distributed to other operators or disposed of.

##### 7.11.7.6.3 Security levels 3 and 4

In addition to the requirement of security levels 1 and 2, documentation shall [AS11.40] specify the procedures required for the secure destruction (e.g. rendering the module inoperable and unrepairable) of the module.

### 7.11.8 Guidance documents

The requirements in this subclause are intended to ensure that all entities using the cryptographic module have adequate guidance and procedures to administer and use the module's approved services.

Guidance documentation consists of administrator and non-administrator guidance.

Administrator guidance shall [AS11.41] specify:

a) 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 or administrative roles, or both;

b) information and procedures required for authentication data and mechanisms, such as for first authentication and the administration of roles, as well as any other guidance required for authentication;

c) procedures on how to administer the cryptographic module; and

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

Non-administrator guidance shall [AS11.42] specify:

e) the approved and non-approved security functions, physical ports, and logical interfaces available to the users of a cryptographic module; and

f) all user responsibilities necessary for the operation of a cryptographic module.

## 7.12 Mitigation of other attacks

### 7.12.1 Mitigation of other attacks general requirements

Susceptibility of a cryptographic module to attacks not defined in this document depends on the module type, implementation, and implementation environment. Such attacks can be of particular concern for cryptographic modules implemented in hostile environments (e.g. where the attackers can be the authorized 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.

Requirements in 7.12 are not applicable if the cryptographic module vendor does not claim mitigation of other attacks.

If no vendor claims are made, the vendors public documentation should reflect that no claims have been made regarding mitigation of other attacks.

The documentation for mitigation of other attacks specified in A.2.11 shall [AS12.01] be provided.

### 7.12.2 Security levels 1, 2 and 3

If a cryptographic module is designed to mitigate one or more specific attack(s) not defined in this document and claimed by the module vendor, then the module's supporting documents shall [AS12.02] 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.

### 7.12.3 Security level 4

In addition to the requirements for security levels 1, 2 and 3, the following requirement shall [AS12.03] apply to cryptographic modules for security levels 4:

a) If the mitigation of specific attacks not defined in this document is claimed, documentation shall [AS12.04] specify the methods used to mitigate the attacks and the methods to test the effectiveness of these mitigation techniques.

# Annex A
(normative)

# Documentation requirements

## A.1 Purpose

This annex specifies the minimum documentation which shall [ASA.01] be required for a cryptographic module that undergoes independent testing.

## A.2 Items

### A.2.1 Cryptographic module specification

The following cryptographic module specifications shall [ASA.02] be documented for security levels 1, 2, 3 and 4:

a) specification of the module type (hardware, software, firmware, hybrid software or hybrid firmware module);

b) specification of the module's cryptographic boundary;

c) specification of the hardware, software and firmware components of the cryptographic module, and description of the physical configuration of the module;

d) specification of hardware, software or firmware components of the cryptographic module that are excluded from the security requirements of Clause 7 and an explanation of the rationale for the exclusion;

e) specification of the physical ports and logical interfaces of a cryptographic module;

f) specification of the manual or logical controls of a cryptographic module, physical or logical status indicators, and applicable physical, logical, and electrical characteristics;

g) 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;

h) block diagram depicting all major hardware elements of a cryptographic module and element interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory and program memory;

i) specification of the design of the hardware, software and firmware of a cryptographic module;

j) specification of all security-related information, including secret and private cryptographic keys (both plaintext and encrypted), authentication data (e.g. passwords, PINs), verifier data, CSPs, PSPs and other protected information (e.g. audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module;

k) specification of how the module supports a degraded operation; and

l) specification of a cryptographic module security policy including the instructions derived from the requirements of Clause 7 and the instructions derived from any additional requirements imposed by the vendor.

### A.2.2 Cryptographic module interfaces

The following cryptographic module specifications shall [ASA.03] be documented for security levels 1, 2, 3 and 4:

a) specification of the data input, data output, control input, control output, status output and power interfaces, both physical and logical; and

b) specification of the exceptions and rationale if the control output interface is not inhibited during the error state.

The following cryptographic module specifications shall [ASA.04] be documented for security levels 3 and 4:

c) specification of the plaintext trusted path interface.

### A.2.3 Roles, services, and authentication

The following cryptographic module specifications shall [ASA.05] be documented for security levels 1, 2, 3 and 4:

a) specification of all authorized roles supported by a cryptographic module;

b) specification of the services, operations, or functions provided by a cryptographic module, both approved and non-approved. For each service, specification of the service input, corresponding service output, and the authorized role(s) in which the service can be performed;

c) specification of any services provided by a cryptographic module for which the operator is not required to assume an authorized role, and how these services do not modify, disclose, or substitute cryptographic keys and other CSPs, or otherwise affect the security of the module;

d) specification of the module's services that show the module's versioning information, show status, perform self-tests, perform approved security functions and perform zeroization;

e) specification of the cryptographic bypass mechanisms;

f) specification of the software or firmware loading mechanisms; and

g) specification of the re-authentication bypass controls and interface.

The following cryptographic module specifications shall [ASA.06] be documented for security levels 2, 3 and 4:

h) specification of the authentication mechanisms supported by a cryptographic module, the types of verifier data required to implement supported authentication mechanisms, the authorized methods used to control access to the module for the first time and initialize the authentication mechanism, and the rate limiting methods of the authentication mechanisms supported by the module, including the rationale supporting the use of multiple authentication mechanisms.

### A.2.4 Software/firmware security

The following cryptographic module specifications shall [ASA.07] be documented for security levels 1, 2, 3 and 4:

a) specification of approved integrity techniques or EDC used;

b) specification of the method for the operator to perform the integrity test on demand.

The following cryptographic module specifications shall [ASA.08] be documented for security levels 2, 3 and 4:

c) specification of the form of the executable code.

### A.2.5 Operational environment

The following cryptographic module specifications shall [ASA.09] be documented for security levels 1 and 2:

a) specification of the operational environment and versioning including, if applicable, the operating system employed by the module;

b) specification of the security policies, settings or restrictions to the configuration of the operating system.

The following cryptographic module specifications shall [ASA.10] be documented for security level 2:

c) administrator guidance documentation to configure the operating system according to the specification requirements and authentication methods.

### A.2.6 Physical security

The following cryptographic module specifications shall [ASA.11] be documented for security levels 1, 2, 3 and 4:

a) specification of the physical embodiment and security level for which the physical security mechanisms of a cryptographic module are implemented. Specification of the physical security mechanisms that are employed by a module; and

b) if a cryptographic module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access, specification of the maintenance interface and how and which SSPs are zeroized when the maintenance interface is accessed.

The following additional cryptographic module specifications shall [ASA.12] be documented for security levels 2, 3 and 4:

c) specification of all protected trusted path, if any, in multiple-chip modules, and the approved cryptographic function used.

The following additional cryptographic module specifications shall [ASA.13] be documented for security level 3:

d) specification of the normal operating ranges of a cryptographic module. Specification of the environmental failure protection features employed by a cryptographic module or specification of the environmental failure tests performed.

The following additional cryptographic module specifications shall [ASA.14] be documented for security level 4:

e) specification of the environmental failure protection features employed by a cryptographic module; and

f) specification of the fault injection mitigation techniques employed.

### A.2.7 Non-invasive security

The following cryptographic module specifications shall [ASA.15] be documented for security levels 1, 2, 3 and 4:

a) specification of the mitigation techniques employed against non-invasive attacks including those specified in Annex F; and

b) evidence of the effectiveness of each of the employed attack mitigation techniques.

### A.2.8 Sensitive security parameter management

The following cryptographic module specifications shall [ASA.16] be documented for security levels 1, 2, 3 and 4:

a) specification of all SSPs employed by a cryptographic module;

b) specification of all RBGs and their usage;

c) specification of minimum entropy required by the module for each entered entropy input parameter;

d) specification of each RBG (approved and non-approved and entropy sources) employed by a cryptographic module;

e) specification of the minimum entropy input and the generation method of the claimed minimum entropy if the entropy input is collected from within the cryptographic boundary of the cryptographic module;

f) specification of each SSP generation method that makes use of an RBG;

g) specification of each SSP generation method employed by a module;

h) specification of each of the key generation methods (approved and non-approved) employed by a cryptographic module;

i) specification of the SSP establishment methods employed by a cryptographic module;

j) specification of the SSP entry and output methods employed by a module;

k) specification of the SSPs stored in the modules;

l) specification of how CSPs are protected from unauthorized access, use, disclosure, modification, and substitution when stored in the module;

m) specification of how PSPs are protected from unauthorized modification and substitution when stored within the module;

n) specification of how the module associates a PSP stored in the module with the entity (operator, role, or process) to which the parameter is assigned;

o) specification of the zeroization method(s) employed by a module, including procedural, and the rationale as to how the method(s) prevent(s) the retrieval and reuse of the zeroized values; and

p) list of SSPs claiming exemption from zeroization requirements, the specific zeroization requirements that are not enforced for each SSP, justification for each SSP of why compromise does not directly compromise user data, privacy, or other SSPs that protect user data or privacy and how the exempt SSPs contribute to the security of the module.

The following additional cryptographic module specifications shall [ASA.17] be documented for security levels 3 and 4:

q) if split-knowledge procedures are used, documentation provided to demonstrate that if knowledge of n components is required to reconstruct the original CSP, then knowledge of any n-1 components provides no information about the original CSP other than the length; and

r) specification of the split-knowledge procedures employed by a module.

### A.2.9 Self-tests

The following cryptographic module specifications shall [ASA.18] be documented for security levels 1, 2, 3 and 4:

a) specification of self-tests performed by a cryptographic module including pre-operational and conditional tests;

b) specification of whether a self-test is being performed on data internal to the module, or data being provided from an external source;

c) specification of the self-test failure status indicator;

d) specification of the error states that a cryptographic module can enter when a self-test fails, and the conditions and actions necessary to exit the error states and resume normal operation of a cryptographic module (e.g. this can include maintenance of the module, re-powering the module, automatic module recovery, entering degraded operation or returning the module to the vendor for servicing). This includes which conditions trigger an error state upon failure of a conditional critical function test;

e) specification of all security functions critical to the secure operation of a cryptographic module and identification of the applicable pre-operational self-tests and conditional self-tests performed by the module; and

f) if a cryptographic module implements a bypass capability, specification of the mechanism or logic governing the switching procedure.

### A.2.10 Life-cycle assurance

The following cryptographic module specifications shall [ASA.19] be documented for security levels 1, 2, 3 and 4:

a) specification of the configuration management system used for the cryptographic module;

b) specification of the supporting documents for the development of the cryptographic module and associated documents provided by the configuration management system;

c) specification of procedures for secure installation, initialization and start-up of a cryptographic module;

d) specification of the correspondence between the design of the hardware and software or firmware components of a cryptographic module, and the cryptographic module's security policy and FSM;

e) if a cryptographic module contains software, specification of the source code for the software, annotated with comments that clearly depict the correspondence of the software to the design of the module;

f) if a cryptographic module contains hardware, specification of either the schematics, or the HDL listings, or both for the hardware as applicable;

g) specification of the FSM (or equivalent) using a state transition diagram and state transition table which include:

   1) the operational and error states of a cryptographic module;

   2) the corresponding transitions from one state to another;

   3) the input events, including data inputs and control inputs, which cause transitions from one state to another; and

   4) the output events, including internal module conditions, data outputs, and status outputs, resulting from transitions from one state to another;

h) specification of the source code for the software or firmware;

i) specification of attestation standards being met by the module;

j) for administrator guidance, specification of:

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

   2) procedures on how to administer the cryptographic module in a secure manner; and

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

k) for non-administrator guidance, specification of:

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

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

The following additional cryptographic module specifications shall [ASA.20] be documented for security levels 2, 3 and 4:

l) specification of a functional specification that informally describes the cryptographic module, the functionality of the cryptographic module, the external physical ports and logical interfaces of the cryptographic module, and the purpose of the physical ports and logical interfaces; and

m) specification of the procedures for maintaining security while distributing and delivering versions of a cryptographic module to authorized operators.