



DPC: 23/30433275 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 27 November 2023

Origin: International

Latest date for receipt of comments: 20 January 2024

Project No. 2021/00269

Responsible committee: IST/33/3 Security Evaluation, Testing and Specification

Interested committees:

Title: Draft BS ISO/IEC 19790 Information technology - Security techniques - Security requirements for cryptographic modules.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 20 January 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 19790

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Voting begins on:
2023-11-27

Voting terminates on:
2024-02-19

Information technology — Security techniques — Security requirements for cryptographic modules

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

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number
ISO/IEC DIS 19790:2023(E)
Documents
AVA Document Sharing Hub
© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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.....	v
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	17
5 Cryptographic module security levels	18
5.1 Security Level 1.....	18
5.2 Security Level 2.....	18
5.3 Security Level 3.....	18
5.4 Security Level 4.....	19
6 Functional security objectives	20
7 Security requirements	20
7.1 General.....	20
7.2 Cryptographic module specification	24
7.2.1 Cryptographic module specification general requirements	24
7.2.2 Types of cryptographic modules	24
7.2.3 Cryptographic boundary	24
7.2.4 Module operations	25
7.3 Cryptographic module interfaces	27
7.3.1 Cryptographic module interfaces general requirements.....	27
7.3.2 Types of interfaces	27
7.3.3 Definition of interfaces.....	27
7.3.4 Plaintext trusted path	28
7.3.5 Protected internal paths.....	29
7.4 Roles, services, and authentication.....	29
7.4.1 Roles, services, and authentication general requirements.....	29
7.4.2 Roles	29
7.4.3 Services	30
7.4.4 Authentication.....	31
7.5 Software/Firmware security	33
7.6 Operational environment	35
7.6.1 Operational environment general requirements	35
7.6.2 Clause applicability	36
7.6.3 Operating system requirements for modifiable operational environments	37
7.7 Physical security.....	39
7.7.1 Physical security embodiments	39
7.7.2 Physical security general requirements.....	40
7.7.3 Physical security requirements for each physical security embodiment	42
7.7.4 Environmental failure protection/testing	44
7.8 Non-invasive security.....	45
7.9 Sensitive security parameter management	46
7.9.1 Sensitive security parameter management general requirements.....	46
7.9.2 Random bit generators	46
7.9.3 Sensitive security parameter generation	47
7.9.4 Automated Sensitive security parameter establishment	47
7.9.5 Sensitive security parameter entry and output	47
7.9.6 Sensitive security parameter storage.....	48
7.9.7 Sensitive security parameter zeroisation.....	48
7.10 Self-tests.....	49
7.10.1 Self-test general requirements	49
7.10.2 Pre-operational self-tests.....	50
7.10.3 Conditional self-tests	51

7.11	Life-cycle assurance	53
7.11.1	Life-cycle assurance general requirements.....	53
7.11.2	Configuration management	54
7.11.3	Design	54
7.11.4	Finite state model	54
7.11.5	Development	55
7.11.6	Vendor testing.....	56
7.11.7	Delivery and operation	57
7.11.9	Guidance documents	58
7.12	Mitigation of other attacks	58
Annex A	(normative) Documentation requirements	60
A.1	Purpose.....	60
A.2	Items.....	60
A.2.1	General.....	60
A.2.2	Cryptographic module specification	60
A.2.3	Cryptographic module interfaces	61
A.2.4	Roles, services, and authentication	61
A.2.5	Software/Firmware security.....	61
A.2.6	Operational environment	61
A.2.7	Physical security	62
A.2.8	Non-invasive security.....	62
A.2.9	Sensitive security parameter management	62
A.2.10	Self-tests	63
A.2.11	Life-cycle assurance	63
A.2.12	Mitigation of other attacks	65
Annex B	(normative) Cryptographic module security policy.....	66
B.1	General.....	66
B.2	Items.....	66
B.2.1	General.....	66
B.2.2	Cryptographic module specification	66
B.2.3	Cryptographic module interfaces	67
B.2.4	Roles, services, and authentication	67
B.2.5	Software/Firmware security.....	68
B.2.6	Operational environment	68
B.2.7	Physical security	68
B.2.8	Non-invasive security.....	69
B.2.9	Sensitive security parameters management	69
B.2.10	Self-tests	70
B.2.11	Life-cycle assurance	70
B.2.12	Mitigation of other attacks	70
Annex C	(normative) Approved security functions.....	71
C.1	Purpose.....	71
C.1.1	Cryptographic algorithms	71
C.1.2	Other security functions	72
Annex D	(normative) Approved sensitive security parameter generation and establishment methods.....	73
D.1	Purpose.....	73
D.1.1	Sensitive security parameter generation	73
D.1.2	Key establishment methods	73
Annex E	(normative) Approved authentication mechanisms	74
E.1	Purpose.....	74
E.1.1	Entity authentication	74
E.1.2	Authentication strength and rate limiting methods	74
E.1.3	Password protection methods	75
Annex F	(normative) Approved non-invasive attack mitigation test metrics	76
F.1	Purpose.....	76
F.2	Non-invasive attack mitigation test metrics	76

Annex G (normative) Module secure development, manufacturing and operation..... 77

G.1 Purpose..... 77

G.1.1 Secure Development 77

G.1.2 Manufacturing Security 77

G.1.3 Operations Security..... 77

Bibliography 78

Foreword

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

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27.

This third edition cancels and replaces the second edition, (ISO/IEC 19790:2012 Corrigendum 1), and has technically revised clauses, subclauses, tables, figures and annexes, including:

- Clause 3 Terms and definitions - this clause has been refined and updated to reflect changes in requirements in section 7
- Clause 4 Abbreviated terms – this clause has been refined and updated to reflect changes in requirements in section 7
- Clause 5 Cryptographic module security levels – this clause has been refined and updated to reflect major changes in requirements and structure in section 7
- Clause 6 Functional security objectives – language in this clause has been refined and modernized
- Clause 7 Security requirements – although the main structure of this clause remains the same, requirements have been reworded and rearranged for clarity. New requirements have been added, and redundant or unnecessary requirements removed.
- Annex A Documentation requirements - this Annex has been updated to reflect changes in requirements in section 7
- Annex B Cryptographic module security policy - this Annex has been updated to reflect changes in requirements in section 7
- Annex C Approved security functions - this Annex has been restructured and updated with recently published standards
- Annex D - Approved security functions - this Annex has been restructured and updated with recently published standards

- Annex E - Approved authentication mechanisms - this Annex has been updated with recently published standards as well as examples of rate limiting methods.
- Annex F- Approved non-invasive attack mitigation test metrics – this Annex has been updated with the inclusion of ISO/IEC 1785
- New Annex G on module secure development, manufacturing and operation

Introduction

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

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

The overall security rating or the security level within each area of a cryptographic module must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilised and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilise cryptographic modules provide an acceptable level of security for the given application and environment. Since each authority is responsible for selecting which approved security functions are appropriate for a given application, compliance with this 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.

BLANK PAGE

Information technology — Security techniques — Security requirements for cryptographic modules

1 Scope

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

Compliance to 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. Guidance contained in the module's security policy outlines the modules strengths and limitations, and is expected to be followed for any given deployment.

2 Normative references

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

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

3 Terms and definitions

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

3.1 access control list

ACL

list of permissions to grant access to an object

3.2 administrator guidance

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

3.3 automated

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

3.4 approval authority

an organisation or authority able to evaluate and/or approve security functions

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

3.5

approved data authentication technique

approved method providing assurance that the originator of the data is as claimed. Approved data authentication techniques may include the use of an approved digital signature, approved message authentication code or approved keyed hash (e.g. HMAC). Approved data authentication techniques are specified in Annex C

3.6

approved integrity technique

approved method of verifying whether or not data has been corrupted or modified. Approved integrity techniques may be keyed, and can include approved hash, message authentication code or a digital signature algorithm. Approved integrity techniques are specified in Annex C

3.7

approved process

a set of interrelated functions that includes at least one approved security function specified in Annex C, which references Annex D and Annex E, and may include non-cryptographic functions, or non-approved security functions which are not security relevant to the processes operation

EXAMPLE A banking transaction, a compression service that includes encryption, etc.

3.8

approved service

a service which includes at least one approved security function or process, and can include non-security relevant functions or processes

NOTE Security relevant but non-approved security functions or processes are excluded from approved services.

3.9

approved security function

security functions that are referenced in Annex C, which references Annex D and Annex E

3.10

asymmetric algorithm or technique

cryptographic algorithm or technique referenced in Annex C, which references Annex D, that uses two related transformations; a public transformation (defined by the public key) and a private transformation (defined by the private key)

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

3.11

attestation

process used to allow an entity outside the boundary of the cryptographic module to securely verify the identity and other physical or logical characteristics of the cryptographic module using an attestation record, and conforming to attestation standards and methods listed in Annex G

3.12

attestation record

record that is generated by and retrievable from a cryptographic module that supports the attester service. The attestation record contains measurement details about software, firmware or hardware 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, registers, and fuse values

3.13

attester service

service that a cryptographic module may support that requires the module to support an identity and the generation of attestation records

3.14**authentication data**

data entered into the module by the operator, used to authenticate the operator to the module. Authentication data is transient and is considered a temporary CSP. During an authentication attempt, authentication data is submitted to the module as:

- a data input by the operator (e.g. a password, PIN, cryptographic key or equivalent); or
- the result of a method/process involving operator related information (e.g. the signing of a challenge with a private key, insertion of a physical key, processing of biometric data)

3.15**authorised**

when an operator has authority to assume a specific role and perform a corresponding set of services

3.16**biometric**

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

3.17**bitstream**

a series of instructions parsed by the FPGA on start-up to configure its internal logic and is considered a highly customised form of executable code

3.18**certificate**

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

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

3.19**compromise**

unauthorised disclosure, modification, substitution, or use of critical security parameters, the unauthorised modification or substitution of public security parameters, or the loss of integrity or availability of the cryptographic module itself, which may result in the unintended bypass of security functions supported by the module

3.20**conditional self-test**

test performed by a cryptographic module when the conditions specified for the test occur

3.21**confidential**

intending that information is not made available or disclosed to unauthorised 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 24765:2010 3.770 1.]

3.23**configuration management system****CMS**

set of procedures and tools (including their documentation) used by a vendor to develop and maintain configurations of modules during its life-cycle

3.24

control information

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

3.25

control input

control information that is input into a cryptographic module or disjoint components of a hybrid module

3.26

control input interface

vendor identified interface(s) for which all control information is input into the cryptographic module

3.27

control output

control information that is output from a cryptographic module or disjoint component of a hybrid module to be used as control input into another cryptographic module or disjoint component of a hybrid module.

3.28

control output interface

vendor identified interface(s) for which all control information is output from the cryptographic module

3.29

critical security parameter

CSP

security related information whose unauthorised access, use, disclosure, modification and substitution can compromise the security of a cryptographic module

EXAMPLE Secret and private cryptographic keys, authentication or verifier data such as passwords or PINs.

NOTE A CSP can be plaintext or encrypted.

3.30

crypto officer

an operator that accesses a cryptographic module in order to perform cryptographic initialisation or management functions of a cryptographic module (e.g. module initialisation, management of SSPs and auditing)

3.31

cryptographic algorithm

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

NOTE 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, software or firmware components) of the cryptographic module

3.33

cryptographic bypass

the ability of a service to partially or wholly circumvent a cryptographic function or process

3.34

cryptographic hash function

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

3.35**cryptographic key****key**

sequence of symbols that controls the operation of a cryptographic transformation

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

3.36**cryptographic module****module**

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

3.37**cryptographic module security policy****security policy**

precise specification of the security rules under which a cryptographic module shall operate, including the rules derived from the requirements of this document and additional rules imposed by the module or validation authority

NOTE See Annex B.

3.38**cryptographic operation**

implementation of one or more cryptographic algorithms in the module

3.39**data input interface**

vendor identified interface(s) for which all input data is input into the cryptographic module

3.40**data output interface**

vendor identified interface(s) for which all output data is output from the cryptographic module

3.41 data path

physical or logical route over which data passes

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

3.42**debugging technique**

method used to halt or alter the execution of the module to analyse malfunctions, using interfaces or tools that can modify objects in memory e.g. including executable code, in a way that may bypass security controls

NOTE Security controls are considered to be any feature of the executable code required to meet the functional requirements of this document.

3.43**degraded operation**

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

3.44**digital signature**

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

3.45

direct entry

entry of an SSP or key component into a cryptographic module, using a device such as a keyboard or number pad

3.46

disjoint signature

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

3.47

electronic entry

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

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

3.48

encompassing signature

single signature for an entire set of code

3.49

encrypted CSP

a CSP that has been encrypted using an approved security function

3.50

entity

person, group, device or process

3.51

entropy

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

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

3.52

environmental failure protection

EFP

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

3.53

environmental failure testing

EFT

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

3.54

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

3.55

executable form

form of the code in which the software or firmware is managed and controlled completely by the operational environment of the module and does not require compilation

3.56**factory state**

default settings consistent with how the module left the factory

3.57**fault injection**

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

3.58**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

3.59**firmware**

code that is executed in a non-modifiable or limited operational environment

3.60**firmware module**

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

3.61**functional specification**

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

3.62**functional testing**

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

3.63**hard****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; physically toughened; rugged, and durable

NOTE

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

3.64**hardware**

physical equipment/elements

3.65**hardware module**

module whose cryptographic boundary is specified at a hardware perimeter. Firmware, which may also include an operating system, may be included within this hardware cryptographic boundary

NOTE

Bitstreams contain 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, 7.10.2.2, and 7.10.3.4 as noted.

3.66

hash value

output of a cryptographic hash function

3.67

hybrid module

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

NOTE Hybrid firmware modules and hybrid software modules are the sub-categories of hybrid module.

3.68

hybrid firmware module

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

3.69

hybrid software module

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

3.70

input data

all data (except control data entered via the control input interface) that is input to and processed by a cryptographic module (including plaintext data, ciphertext data, SSPs, and status information from another module)

3.71

integrity

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

3.72

interface

logical interface

logical entry or exit point of a cryptographic module that provides access to the module for logical information flows. Logical interfaces are separated into seven categories: data input interface, data output interface, control input interface, control output interface, status output interface, maintenance interface, and power interface

3.73

key agreement

key establishment procedure where the resulting key 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

3.74

key component

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

3.75

key loading device

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

NOTE The use of a key 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 that is designed to accept only controlled changes by an operator to the module components, the computing platform, or the operating system

3.78**low-level testing**

testing of the individual components or group of components of the cryptographic module and their physical ports and logical interfaces

3.79**maintenance interface**

all physical and logical interfaces to the cryptographic module which are utilised when in the maintenance role

3.80**maintenance role**

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

EXAMPLE

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

3.81**manual**

requiring human operator manipulation

3.82**message authentication code****MAC**

a cryptographic checksum on data that uses a symmetric key which provides data source confirmation and the detection of integrity against both accidental and intentional modifications

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 that is useful in determining a worst-case estimate of sample entropy

3.85**modifiable operational environment**

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

3.86**multi-factor authentication**

authentication of an operator using at least two independent authentication factors. All authentication data is verified by the cryptographic module

NOTE 1 An authentication factor is operator related information that resides outside the module, is used as proof of identity, and may include a method/process to produce varying or short-lived authentication data from the operator related information.

NOTE 2 Independent authentication factor categories for human operators include: something known, such as a secret password, something possessed, such as a physical key or token, and a physical property, such as a biometric.

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 the user and/or other non-administrative roles for operating the cryptographic module

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

3.89

non-invasive attack

attack that uses side-channels (information gained from the physical implementation) emitted by the module.

NOTE Examples of side channels include power consumption, electromagnetic emissions and computation time.

3.90

non-modifiable operational environment

operational environment that is designed to not accept firmware changes

3.91

non-security relevant

implemented in a manner to not interfere or compromise the approved secure operation of the cryptographic module

3.92

normal operation

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

3.93

opaque

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

3.94

operational environment

OE

operating system, where applicable (including virtual machine(s) and runtime environment, when applicable), and hardware platform required for the cryptographic module to operate

NOTE This may include, where applicable, integrated circuits, processors, libraries, memory management, process control, device drivers for hardware, power supplies and enclosures.

3.95

operational state

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

3.96

operator

an entity external to the module that exercises the module's services via the provided interfaces [where entity means an individual (person), organization, device, process or another module]

3.97**output data**

All data (except status data output via the status output interface and control data output via the control output interface) that is output from a cryptographic module (including plaintext data, ciphertext data, and SSPs)

3.98**overall security rating**

the minimum security level of the independent security levels received in all security area

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

3.100**password**

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

EXAMPLE Letters, numbers, and other symbols.

3.101**personal identification number****PIN**

numeric code used to authenticate an identity or to verify access authorisation

3.102**physical protection**

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

3.103**plaintext**

unencrypted, or obfuscated by non-approved methods

3.104**plaintext trusted path**

protected communication link established between the cryptographic module and a sender or receiver to securely communicate plaintext CSPs and key components without using cryptography

NOTE A plaintext trusted path protects against eavesdropping, as well as physical or logical tampering by unwanted operators or entities between the module's defined input or output ports and along the communication link with the intended endpoint without using cryptographic methods.

3.105**port**

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

3.106**power**

electrical power that is input to or output from a cryptographic module

3.107

power interface

vendor identified interface(s) for which power is input to or output from a cryptographic module

3.108

pre-operational self-test

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

3.109

private key

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

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

3.110

production-grade

product, element or software that has been tested to meet operational specifications

3.111

protected internal path

interfaces between ICs within the cryptographic boundary in a multi-chip module using approved cryptographic methods to protect the confidentiality and integrity of the data

3.112

public key

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

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

3.113

public key certificate

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

3.114

public (asymmetric) key algorithm

cryptographic algorithm that uses two related keys, a public key and a private key

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

3.115

public security parameter

PSP

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

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

NOTE A PSP is considered protected if it cannot be modified or substituted without detection by the cryptographic module.

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 meant to slow down and render impractical automated guessing attacks on authentication data

EXAMPLE Rate limiting methods can be, but are not limited to, 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

3.119**role**

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

NOTE One or more services 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 granting access to an object

NOTE An object can be data, a service, or other.

3.121**runtime environment**

environment in which a program or application is executed

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

3.122**salted password**

a password to which unique data has been added ahead of creating the stored password hash

3.123**secret key**

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

3.124**secure container**

isolated execution space internal to the cryptographic module's physical enclosure where firmware can execute in a manner such that the module is protected against the secure container firmware interfering or compromising the cryptographic module

NOTE 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 clause 7.5.

3.125**secure container firmware**

firmware executing within a secure container

3.126**security function**

cryptographic algorithms together with modes of operation, such as block ciphers, stream ciphers, symmetric or asymmetric key algorithms, message authentication codes, hash functions, random bit generators, etc. or other security functions such as entity authentication, SSP generation and establishment, etc.

3.127

security level

well-defined set of security requirements in a security area

3.128

security relevant

function of the module that if bypassed, modified or substituted can ultimately contribute to the potential compromise of the cryptographic module

NOTE 1 This term is not the inverse of non-security relevant as covered separately.

NOTE 2 Security relevant considered as applicable within this scope of this document.

3.129

seed

secret value used to initialise a random bit generator

3.130

self-test

pre-operational or conditional test executed by the cryptographic module

3.131

sensitive security parameters

SSP

critical security parameters (CSP) and public security parameters (PSP)

3.132

service

operation and/or function that can be performed by a cryptographic module invoked by an external operator

3.133

service input

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

3.134

service output

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

3.135

single-chip cryptographic module

physical embodiment in which a single integrated circuit (IC) chip may be used as a standalone device or may be embedded within an enclosure or a product that may not be physically protected

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

NOTE 1 The enclosure may include non-IC components that are security relevant and require physical protection.

NOTE 2 The enclosure may include other excluded IC components.

3.136

software

code that is executed in a modifiable operational environment

3.137

software module

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

3.138**software/firmware integrity test**

self-test(s) performed on the software or firmware components of a cryptographic module to ensure integrity of those components

3.139**software/firmware load test**

conditional self-test performed on software or firmware components after the components have been introduced into the module boundary, and which must pass successfully before the new components can be executed by the cryptographic module

3.140**split knowledge**

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

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

3.141**SSP establishment**

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

NOTE 1 SSP establishment includes SSP agreement, SSP transport and SSP entry or output.

NOTE 2 Automated SSP establishment can include generation and derivation.

3.142**SSP generation**

process of creating an SSP within the cryptographic module

3.143**SSP transport**

process of transferring an SSP from one entity to another entity using approved cryptographic methods

3.144**status information**

output signals, indicators (e.g. error indicator), and status data (including return codes and physical indicators such as visual (display, indicator lamps), audio (buzzer, tone, ring), and mechanical (vibration)) used to indicate the status of a cryptographic module

3.145**status output**

status information that is output from a cryptographic module

3.146**status output interface**

vendor identified interface(s) for which all status output is output from the cryptographic module

3.147**strong**

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

3.148**symmetric cryptographic technique**

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

3.149

tamper detection

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

3.150

tamper evidence

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

3.151

tamper response

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

3.152

temporary SSP

an SSP that, after its use to perform an approved function, is no longer needed

NOTE Temporary SSPs are commonly ephemeral in nature and used only for a single cryptographic operation and then cleared.

3.153

translucent

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

3.154

trust anchor

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

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

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

3.155

user

an operator that accesses a cryptographic module in order to perform general security services, including cryptographic operations and other approved security functions

3.156

validated

assurance of tested conformance by a validation authority

3.157

validation authority

entity that will validate the testing results for conformance to this document

3.158

vendor

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

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

3.159

verifier data

data used by the module to verify the correct authentication data was entered into the module by operators authenticating themselves to the module. Verifier data resides inside the cryptographic module (or its OE should the OE implement the authentication mechanism per 7.6.3 Level 2), until updated or zeroised. It may have been generated inside or outside the module. Verifier data is an SSP