BS EN ISO/IEC 19790:2020

Incorporating corrigenda June 2016 and December 2020

BSI Standards Publication

Information technology — Security techniques — Security requirements for cryptographic modules

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 19790:2020

National foreword

This British Standard is the UK implementation of EN ISO/IEC 19790:2020. It is identical to ISO/IEC 19790:2012. It supersedes BS ISO/IEC 19790:2012, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information security, cybersecurity and privacy protection.

A list of organizations represented on this committee can be obtained on request to its committee manager.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 16461 9

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2012.

Amendments/corrigenda issued since publication

Date	Text affected
30 June 2016	Implementation of ISO corrected text 15 December 2015: see ISO foreword for details
30 April 2020	This corrigendum renumbers BS ISO/IEC 19790:2012 as BS EN ISO/IEC 19790:2020
31 December 2020	Implementation of CEN correction notice 9 December 2020: modification of CEN title page and European foreword

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 19790:2020

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 19790

March 2020

ICS 35.030

English version

Information technology - Security techniques - Security requirements for cryptographic modules (ISO/IEC 19790:2012, including corrected version 2015-12)

Technologies de l'information - Techniques de sécurité - Exigences de sécurité pour les modules cryptographiques (ISO/IEC 19790:2012, y compris version corrigée 2015-11)

Informationstechnik - Sicherheitstechniken - Sicherheitsanforderungen für kryptografische Module (ISO/IEC 19790:2012, einschließlich korrigierte Fassung 2015-12)

This European Standard was approved by CEN on 2 March 2020.

This European Standard was corrected and reissued by the CEN-CENELEC Management Centre on 09 December 2020.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

© 2020 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

Ref. No. EN ISO/IEC 19790:2020 E

AVA Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 19790:2020

European foreword

The text of ISO/IEC 19790:2012, including corrected version 2015-12 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 19790:2020 by Technical Committee CEN/CLC/JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2020, and conflicting national standards shall be withdrawn at the latest by September 2020.

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

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 19790:2012, including corrected version 2015-12 has been approved by CEN as EN ISO/IEC 19790:2020 without any modification.

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 19790:2020

Contents

Page

1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviated terms 15
5 Cryptographic module security levels 15
5.1 Security Level 1 15
5.2 Security Level 2 16
5.3 Security Level 3 16
5.4 Security Level 4 17
6 Functional security objectives 17
7 Security requirements 18
7.1 General 18
7.2 Cryptographic module specification 20
7.2.1 Cryptographic module specification general requirements 20
7.2.2 Types of cryptographic modules 20
7.2.3 Cryptographic boundary 21
7.2.4 Modes of operations 22
7.3 Cryptographic module interfaces 23
7.3.1 Cryptographic module interfaces general requirements 23
7.3.2 Types of interfaces 24
7.3.3 Definition of interfaces 24
7.3.4 Trusted channel 25
7.4 Roles, services, and authentication 25
7.4.1 Roles, services, and authentication general requirements 25
7.4.2 Roles 26
7.4.3 Services 26
7.4.4 Authentication 28
7.5 Software/Firmware security 29
7.6 Operational environment 31
7.6.1 Operational environment general requirements 31
7.6.2 Operating system requirements for limited or non-modifiable operational environments 33
7.6.3 Operating system requirements for modifiable operational environments 33
7.7 Physical security 35
7.7.1 Physical security embodiments 35
7.7.2 Physical security general requirements 37
7.7.3 Physical security requirements for each physical security embodiment 39
7.7.4 Environmental failure protection/testing 42
7.8 Non-invasive security 43
7.9 Sensitive security parameter management 44
7.9.1 Sensitive security parameter management general requirements 44
7.9.2 Random bit generators 44
7.9.3 Sensitive security parameter generation 44
7.9.4 Sensitive security parameter establishment 45
7.9.5 Sensitive security parameter entry and output 45
7.9.6 Sensitive security parameter storage 46

Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: BS EN ISO/IEC 19790:2020

7.9.7 Sensitive security parameter zeroisation 46
7.10 Self-tests 47
7.10.1 Self-test general requirements 47
7.10.2 Pre-operational self-tests 47
7.10.3 Conditional self-tests 48
7.11 Life-cycle assurance 50
7.11.1 Life-cycle assurance general requirements 50
7.11.2 Configuration management 51
7.11.3 Design 51
7.11.4 Finite state model 51
7.11.5 Development 52
7.11.6 Vendor testing 53
7.11.7 Delivery and operation 54
7.11.8 End of life 54
7.11.9 Guidance documents 54
7.12 Mitigation of other attacks 55

Annex A (normative) Documentation requirements 56
A.1 Purpose 56
A.2 Items 56
A.2.1 General 56
A.2.2 Cryptographic module specification 56
A.2.3 Cryptographic module interfaces 57
A.2.4 Roles, services, and authentication 57
A.2.5 Software/Firmware security 57
A.2.6 Operational environment 58
A.2.7 Physical security 58
A.2.8 Non-invasive security 58
A.2.9 Sensitive security parameter management 58
A.2.10 Self-tests 59
A.2.11 Life-cycle assurance 60
A.2.12 Mitigation of other attacks 61

Annex B (normative) Cryptographic module security policy 62
B.1 General 62
B.2 Items 62
B.2.1 General 62
B.2.2 Cryptographic module specification 62
B.2.3 Cryptographic module interfaces 63
B.2.4 Roles, services, and authentication 63
B.2.5 Software/Firmware security 64
B.2.6 Operational environment 64
B.2.7 Physical security 64
B.2.8 Non-invasive security 65
B.2.9 Sensitive security parameters management 65
B.2.10 Self-tests 66
B.2.11 Life-cycle assurance 66
B.2.12 Mitigation of other attacks 66

Annex C (normative) Approved security functions 67
C.1 Purpose 67
C.1.1 Block ciphers 67
C.1.2 Stream ciphers 67
C.1.3 Asymmetric algorithms and techniques 67
C.1.4 Message authentication codes 67
C.1.5 Hash functions 67
C.1.6 Entity authentication 68

Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: BS EN ISO/IEC 19790:2020

C.1.7 Key management 68
C.1.8 Random bit generation 68

Annex D (normative) Approved sensitive security parameter generation and establishment methods 69
D.1 Purpose 69
D.1.1 Sensitive security parameter generation 69
D.1.2 Sensitive security parameter establishment methods 69

Annex E (normative) Approved authentication mechanisms 70
E.1 Purpose 70
E.1.1 Authentication mechanisms 70

Annex F (normative) Approved non-invasive attack mitigation test metrics 71
F.1 Purpose 71
F.1.1 Non-invasive attack mitigation test metrics 71

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

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

This corrected version of Technical corrigendum 1 to ISO/IEC 19790:2012 cancels and replaces the first edition (ISO/IEC 19790:2012/Cor 1:2015), incorporating the same technical revisions and miscellaneous editorial corrections showing in **red** text instead of black underlining:

— 3.21: The term "cryptographic boundary" is corrected;

— 3.80: The term "non-security relevant" is corrected;

— 3.108: The term "self-test" is corrected;

— 7.2.2: The requirements **[02.04]**, **[02.05]** and **[02.06]** are corrected;

— 7.2.4.3: The requirement **[02.31]** is corrected;

— 7.3.3: The requirement **[03.14]** is corrected;

— 7.5: The requirements **[05.06]** and **[05.07]** are added. The requirements **[05.08]**, **[05.13]** and **[05.17]** through **[05.23]** are corrected;

— 7.6.3: The requirement **[06.06]** is corrected;

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

- 7.8: The requirement **[08.04]** is corrected;
- 7.9.1: The requirement **[09.04]** is corrected;
- 7.9.7: The requirement **[09.37]** is corrected;
- 7.10.2.2: The requirement **[10.17]** is corrected;
- 7.11.5: The requirement **[11.26]** is corrected;
- 7.11.7: The requirement **[11.35]** is corrected;
- 7.11.9: The requirement **[11.38]** is corrected;
- A.2.5: The requirements of the 1st and 2nd bullets are corrected;
- A.2.7: The requirement of the 3rd bullet is corrected;
- A.2.10: The requirement of the 4th bullet is corrected;
- B.2.4: The requirement of the 9th bullet is corrected;
- B.2.5: The requirement of the 1st bullet is corrected;
- B.2.7: The requirement of the 2nd level 6th bullet is corrected;
- D.1: Duplicate text is removed;
- D.1.2: The reference to ISO/IEC 15946-3 is removed;
- E.1: Duplicate text is removed; and
- F.1: Duplicate text is removed.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

Introduction

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

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

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

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

— physical and environmental controls;

— access controls;

— software development;

— backup and contingency plans; and

— information and data controls.

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

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

Information technology — Security techniques — Security requirements for cryptographic modules

1 Scope

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

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

2 Normative references

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

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

3 Terms and definitions

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

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

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

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

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

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

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

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

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

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

NOTE A CSP can be plaintext or encrypted.

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

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

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

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

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

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

Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: BS EN ISO/IEC 19790:2020

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

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

3.26
cryptographic module security policy
security policy
precise specification of the security rules under which a cryptographic module shall operate, including the rules derived from the requirements of this International Standard and additional rules imposed by the module or validation authority

NOTE See Annex B

3.27
data path
physical or logical route over which data passes

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

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

3.29
differential power analysis
DPA
analysis of the variations of the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to cryptographic operation

3.30
digital signature
data appended to, or a cryptographic transformation of a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery (e.g. by the recipient)

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

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

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

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

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

3.35
encompassing signature
single signature for an entire set of code

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

3.37
entity
person, group, device or process

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

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

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

3.40
environmental failure testing
EFT
use of specific methods to provide reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions outside of the module's normal operating range

3.41
error detection code
EDC
value computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data

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

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

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

3.44
finite state model
FSM
mathematical model of a sequential machine that is comprised of a finite set of input events, a finite set of output events, a finite set of states, a function that maps states and input to output, a function that maps states and inputs to states (a state transition function), and a specification that describes the initial state

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

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

3.46
firmware module
module that is composed solely of firmware

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

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

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

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

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

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

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

3.53
hash value
output of a cryptographic hash function

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

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

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

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

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

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

3.60
ISO/IEC adopted
security function that is either:

— specified in an ISO/IEC standard, or

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

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

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

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

NOTE The use of a key loader requires human manipulation.

Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: BS EN ISO/IEC 19790:2020

3.64
key management
administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy

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

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

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

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

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

3.69
manual
requiring human operator manipulation

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

EXAMPLE A Hash Based Message Authentication Code

3.71
microcode
processor instructions that correspond to an executable program instruction

EXAMPLE Assembler code

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

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

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

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

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

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

EXAMPLE Adapters and expansion boards

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

EXAMPLE Encrypting routers or secure radios

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

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

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

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

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

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

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

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

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

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

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

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

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

EXAMPLE Silicon dioxide or phosphorus glass

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

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

EXAMPLE Letters, numbers, and other symbols

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

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

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

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

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

3.94
private key
key of an entity's asymmetric key pair, which should only be used by that entity

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

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

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

NOTE 1 In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key can only be available to all members of a pre-specified group.

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

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

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

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

3.99
public security parameter
PSP
security related public information whose modification can compromise the security of a cryptographic module

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

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

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

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

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

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

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

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

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

3.105
secret key
cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public

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

NOTE See Annex C

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

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

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

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

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

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

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

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

3.115
single-chip cryptographic module
physical embodiment in which a single integrated circuit (IC) chip may be used as a standalone device or may be embedded within an enclosure or a product that may not be physically protected

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

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

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

3.117
software module
module that is composed solely of software

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

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

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

3.120
split knowledge
process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key

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

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

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

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

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

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

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

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

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

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

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

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

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

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

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

3.131
validated
assurance of tested conformance by a validation authority

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

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

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

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

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

4 Abbreviated terms

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

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

5 Cryptographic module security levels

The following subclauses provide an overview of the four security levels. Common examples, given to illustrate how the requirements might be met, are not intended to be restrictive or exhaustive. Within this document, references to a *module* shall be interpreted as a *cryptographic module*. The cryptographic techniques are identical over the four security levels. Each security level levies increasing levels of security requirements for the protection of the module itself (e.g. access and knowledge of internal components and operation) and SSPs contained and controlled within the module. Each security requirement is identified by a **shall [xx.yy]** where **xx** indicates the clause and **yy** is a numeric index within the clause.

5.1 Security Level 1

Security Level 1 provides a baseline level of security. Basic security requirements are specified for a cryptographic module (e.g. at least one approved security function or approved sensitive security parameter establishment method shall be used). Software or firmware modules may operate in a non-modifiable, limited or modifiable operating

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020

environment. No specific physical security mechanisms are required in a Security Level 1 hardware cryptographic module beyond the basic requirement for production-grade components. Non-invasive mitigation methods or mitigation of other attacks which are implemented are documented. Examples of a Security Level 1 cryptographic module is a hardware encryption board found in a personal computer (PC) or a cryptographic toolkit executing in a handheld device or general purpose computer.

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

5.2 Security Level 2

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

Tamper-evident coatings or seals are placed on a module so that the coating or seal must be broken to attain physical access to SSPs within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorised physical access.

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

Security Level 2 allows a software cryptographic module to be executed in a modifiable environment that implements role-based access controls or, at the minimum, a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions through access control lists (e.g. ACLs), and with the capability of assigning each user to more than one group, and that protects against unauthorised execution, modification, and reading of cryptographic software.

5.3 Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 provides additional requirements to mitigate the unauthorised access to SSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at direct physical access, use or modification of the cryptographic module and probing through ventilation holes or slits. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroise all CSPs when the removable covers/doors of the cryptographic module are opened.

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

Security Level 3 requires manually established plaintext CSPs to be encrypted, utilise a trusted channel or use a split knowledge procedure for entry or output.

Security Level 3 also protects a cryptographic module against a security compromise due to environmental conditions outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defences. A cryptographic module is required to either include special environmental protection features designed to detect when the voltage and temperature boundaries are exceeded and zeroise CSPs, or to undergo rigorous environmental failure testing to provide

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 19790:2020