



SLOVENSKI STANDARD
oSIST prEN ISO/IEC 19790:2020
01-januar-2020

Informacijska tehnologija - Varnostne tehnike - Varnostne zahteve za kriptografske module (ISO/IEC 19790:2012)

Information technology - Security techniques - Security requirements for cryptographic modules (ISO/IEC 19790:2012)

Informationstechnik - Sicherheitstechniken - Sicherheitsanforderungen für kryptografische Module (ISO/IEC 19790:2012)

Technologies de l'information - Techniques de sécurité - Exigences de sécurité pour les modules cryptographiques (ISO/IEC 19790:2012)

Ta slovenski standard je istoveten z: prEN ISO/IEC 19790

ICS:

35.030 Informacijska varnost IT Security

oSIST prEN ISO/IEC 19790:2020 en

INTERNATIONAL
STANDARD

ISO/IEC
19790

Second edition
2012-08-15

Corrected version
2015-12-15

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO/IEC 19790:2020

<https://standards.iteh.ai/catalog/standards/sist/0bd04ea3-f89b-4b1e-8367-603ab1d3989a/sist-en-iso-iec-19790-2020>



Reference number
ISO/IEC 19790:2012(E)

© ISO/IEC 2012

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO/IEC 19790:2020

<https://standards.iteh.ai/catalog/standards/sist/0bd04ea3-f89b-4b1e-8367-603abd3989a/sist-en-iso-iec-19790-2020>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents	Page
1	Scope1
2	Normative references1
3	Terms and definitions1
4	Abbreviated terms15
5	Cryptographic module security levels15
5.1	Security Level 115
5.2	Security Level 216
5.3	Security Level 316
5.4	Security Level 417
6	Functional security objectives17
7	Security requirements18
7.1	General18
7.2	Cryptographic module specification20
7.2.1	Cryptographic module specification general requirements20
7.2.2	Types of cryptographic modules20
7.2.3	Cryptographic boundary21
7.2.4	Modes of operations22
7.3	Cryptographic module interfaces23
7.3.1	Cryptographic module interfaces general requirements23
7.3.2	Types of interfaces24
7.3.3	Definition of interfaces24
7.3.4	Trusted channel25
7.4	Roles, services, and authentication25
7.4.1	Roles, services, and authentication general requirements25
7.4.2	Roles26
7.4.3	Services26
7.4.4	Authentication28
7.5	Software/Firmware security29
7.6	Operational environment31
7.6.1	Operational environment general requirements31
7.6.2	Operating system requirements for limited or non-modifiable operational environments33
7.6.3	Operating system requirements for modifiable operational environments33
7.7	Physical security35
7.7.1	Physical security embodiments35
7.7.2	Physical security general requirements37
7.7.3	Physical security requirements for each physical security embodiment39
7.7.4	Environmental failure protection/testing42
7.8	Non-invasive security43
7.9	Sensitive security parameter management44
7.9.1	Sensitive security parameter management general requirements44
7.9.2	Random bit generators44
7.9.3	Sensitive security parameter generation44
7.9.4	Sensitive security parameter establishment45
7.9.5	Sensitive security parameter entry and output45
7.9.6	Sensitive security parameter storage46

ISO/IEC 19790:2012(E)

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

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

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO/IEC 19790:2020

<https://standards.iteh.ai/catalog/standards/sist/0bd04ea3-f89b-4b1e-8367-603ab1d3989a/sist-en-iso-iec-19790-2020>

ISO/IEC 19790:2012(E)

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;

- 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 19790:2012(E)

Introduction

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

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

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

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

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

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

Information technology — Security techniques — Security requirements for cryptographic modules

1 Scope

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

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

2 Normative references

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

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

3 Terms and definitions

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

3.1

access control list

ACL

list of permissions to grant access to an object

3.2

administrator guidance

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

3.3

automated

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

ISO/IEC 19790:2012(E)**3.4****approval authority**

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

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

3.5**approved data authentication technique**

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

3.6**approved integrity technique**

approved hash, message authentication code or a digital signature algorithm

3.7**approved mode of operation**

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

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

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

3.8**approved security function**

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

3.9**asymmetric cryptographic technique**

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

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

3.10**biometric**

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

3.11**bypass capability**

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

3.12**certificate**

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

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

3.13**compromise**

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

3.14**conditional self-test**

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

3.15**confidentiality**

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

3.16**configuration management system****CMS**

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

3.17**control information**

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

3.18**critical security parameter****CSP**

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

EXAMPLE
anchors

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.

ISO/IEC 19790:2012(E)**3.24****cryptographic key component
key component**

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

3.25**cryptographic module
module**

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

3.26**cryptographic module security policy
security policy**

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

NOTE See Annex B

3.27**data path**

physical or logical route over which data passes

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

3.28**degraded operation**

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

3.29**differential power analysis****DPA**

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

3.30**digital signature**

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

3.31**direct entry**

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

3.32**disjoint signature**

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

3.33**electromagnetic emanations****EME**

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

3.34**electronic entry**

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

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

3.35**encompassing signature**

single signature for an entire set of code

3.36**encrypted key**

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

3.37**entity**

person, group, device or process

3.38**entropy**

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

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

3.39**environmental failure protection****EFP**

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

3.40**environmental failure testing****EFT**

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

3.41**error detection code****EDC**

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

3.42**executable form**

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

3.43**fault induction**

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