

STN	Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Požiadavky na testovanie kryptografických modulov	STN ISO/IEC 24759 97 4125
------------	--	---

Information security, cybersecurity and privacy protection
Test requirements for cryptographic modules

Sécurité de l'information, cybersécurité et protection de la vie privée
Exigences d'essai pour modules cryptographiques

Táto slovenská technická norma obsahuje anglickú verziu medzinárodnej normy ISO/IEC 24759: 2025 a má postavenie oficiálnej verzie.

This Slovak standard includes the English version of the International standard ISO/IEC 24759: 2025 and has the status of the official version.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN ISO/IEC 24759 z augusta 2021 v celom rozsahu.

142386

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2026
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.

Anotácia

Toto štvrté vydanie ruší a nahrádza tretie vydanie (ISO/IEC 24759: 2017), ktoré bolo technicky revidované.

Hlavné zmeny sú nasledovné:

- bola doplnená nová terminológia;
- AS, VE a TE boli aktualizované v súlade s ISO/IEC 19790: 2025; a
- VE a TE boli opravené alebo aktualizované s cieľom zlepšiť efektívnosť.

V oblasti informačných technológií existuje neustále rastúca potreba používať kryptografické mechanizmy, napríklad na ochranu údajov pred neoprávneným prístupnením alebo manipuláciou, na autentifikáciu entít a na zabezpečenie nepopierateľnosti. Bezpečnosť a spoľahlivosť takýchto mechanizmov priamo závisí od kryptografických modulov, v ktorých sú implementované.

Norma ISO/IEC 19790 stanovuje štyri vzostupné, kvalitatívne úrovne bezpečnostných požiadaviek určené na pokrytie širokého rozsahu potenciálnych aplikácií a prostredí. Kryptografické techniky sú totožné pre všetky štyri bezpečnostné úrovne definované v tomto dokumente. Bezpečnostné požiadavky pokrývajú oblasti týkajúce sa návrhu a implementácie kryptografického modulu. Tieto oblasti zahŕňajú:

- špecifikáciu kryptografického modulu;
- rozhrania kryptografického modulu;
- roly, služby a autentifikáciu;
- bezpečnosť softvéru/firmvéru;
- prevádzkové prostredie;
- fyzickú bezpečnosť;
- neinvazívnu bezpečnosť;
- správu citlivých bezpečnostných parametrov;
- samočinné testy;
- zabezpečenie životného cyklu; a
- zmierňovanie iných útokov.

Tento dokument špecifikuje skúšobné požiadavky pre kryptografické moduly zhodné s ISO/IEC 19790: 2025.

Tento dokument špecifikuje metódy, ktoré majú používať skúšobné laboratóriá na overenie, či kryptografický modul spĺňa požiadavky stanovené v ISO/IEC 19790: 2025. Metódy boli vypracované tak, aby počas skúšobného procesu poskytovali vysoký stupeň objektivity a aby zabezpečili konzistentnosť medzi skúšobnými laboratóriami.

Tento dokument tiež špecifikuje informácie, ktoré sú dodávatelia povinní poskytnúť skúšobným laboratóriám ako podporné dôkazy na preukázanie zhody ich kryptografických modulov s požiadavkami stanovenými v ISO/IEC 19790: 2025.

Dodávatelia môžu tento dokument použiť aj na overenie, či ich kryptografické moduly spĺňajú požiadavky stanovené v ISO/IEC 19790: 2025 ešte pred podaním žiadosti o skúšanie v skúšobnom laboratóriu.

Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2025 ISO/IEC, ref. č. ISO/IEC 24759: 2025 E.

Normatívne referenčné dokumenty

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN možno získať na webovej stránke www.unms.sk.

ISO/IEC 19790: 2025 dosiaľ neprijatá

ISO/IEC 20085-1 prijatá ako STN ISO 20085-1 IT bezpečnostné metódy. Požiadavky na testovacie nástroje a metódy kalibrácie testovacích nástrojov na použitie pri testovaní neinvazívnych techník zmierňovania útokov v kryptografických moduloch. Časť 1: Testovacie nástroje a metódy (97 4106)

ISO/IEC 20085-2 prijatá ako STN ISO/IEC 20085-2 IT bezpečnostné metódy. Požiadavky na testovacie nástroje a metódy kalibrácie testovacích nástrojov na použitie pri testovaní neinvazívnych techník zmierňovania útokov v kryptografických moduloch. Časť 2: Skúšobné kalibračné metódy a prístroje (97 4106)

ISO/IEC 20543 dosiaľ neprijatá

Vypracovanie

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

ISO/IEC 24759:2025(en)

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	2
5 Document organization	2
5.1 General	2
5.2 Assertions and security requirements	3
5.3 Assertions with cross references	3
6 Security requirements	4
6.1 General	4
6.2 Cryptographic module specification	5
6.2.1 Cryptographic module specification general requirements	5
6.2.2 Types of cryptographic modules	5
6.2.3 Cryptographic boundary	6
6.2.4 Module operations	16
6.3 Cryptographic module interfaces	23
6.3.1 Cryptographic module interfaces general requirements	23
6.3.2 Categories of interfaces	26
6.3.3 Plaintext trusted path	35
6.3.4 Protected internal paths	38
6.4 Roles, services, and authentication	39
6.4.1 Roles, services, and authentication general requirements	39
6.4.2 Roles	40
6.4.3 Services	41
6.4.4 Authentication	49
6.5 Software/firmware security	59
6.5.1 Software/firmware security general requirements	59
6.5.2 Security level 1	62
6.5.3 Security level 2	67
6.5.4 Security levels 3 and 4	68
6.6 Operational environment	69
6.6.1 Operational environment general requirements	69
6.6.2 Clause applicability	70
6.6.3 Operating system requirements for modifiable operational environments	71
6.7 Physical security	83
6.7.1 Physical security embodiments	83
6.7.2 Physical security general requirements	84
6.7.3 Physical security requirements for each physical security embodiment	95
6.7.4 Environmental failure protection/testing	100
6.7.5 Environmental failure protection features	100
6.7.6 Environmental failure testing procedures	101
6.8 Non-invasive security	104
6.8.1 Non-invasive security general requirements	104
6.8.2 Security levels 1 and 2	104
6.8.3 Security level 3	105
6.8.4 Security level 4	105
6.9 Sensitive security parameter management	106
6.9.1 Sensitive security parameter management general requirements	106
6.9.2 Random bit generators	108
6.9.3 Sensitive security parameter generation	110
6.9.4 Automated sensitive security parameter establishment	110

ISO/IEC 24759:2025(en)

6.9.5	Sensitive security parameter entry and output.....	111
6.9.6	Sensitive security parameter storage.....	117
6.9.7	Sensitive security parameter zeroization.....	118
6.10	Self-tests.....	122
6.10.1	Self-test general requirements.....	122
6.10.2	Security levels 3 and 4.....	126
6.10.3	Pre-operational self-tests.....	127
6.10.4	Conditional self-tests.....	130
6.11	Life-cycle assurance.....	143
6.11.1	Life-cycle assurance general requirements.....	143
6.11.2	Configuration management.....	143
6.11.3	Design.....	145
6.11.4	Finite state model.....	145
6.11.5	Development.....	149
6.11.6	Vendor testing.....	155
6.11.7	Delivery and operation.....	157
6.11.8	Guidance documents.....	160
6.12	Mitigation of other attacks.....	161
6.12.1	Mitigation of other attacks general requirements.....	161
6.12.2	Security levels 1, 2 and 3.....	161
6.12.3	Security level 4.....	161
7	Documentation requirements.....	162
7.1	Purpose.....	162
7.2	Items.....	163
7.2.1	Cryptographic module specification.....	163
7.2.2	Cryptographic module interfaces.....	164
7.2.3	Roles, services, and authentication.....	164
7.2.4	Software/Firmware security.....	165
7.2.5	Operational environment.....	165
7.2.6	Physical security.....	166
7.2.7	Non-invasive security.....	167
7.2.8	Sensitive security parameter management.....	167
7.2.9	Self-tests.....	169
7.2.10	Life-cycle assurance.....	169
7.2.11	Mitigation of other attacks.....	171
8	Cryptographic module security policy.....	172
8.1	General.....	172
8.2	Items.....	173
8.2.1	General.....	173
8.2.2	Cryptographic module specification.....	174
8.2.3	Cryptographic module interfaces.....	175
8.2.4	Roles, services, and authentication.....	175
8.2.5	Software/Firmware security.....	176
8.2.6	Operational environment.....	177
8.2.7	Physical security.....	178
8.2.8	Non-invasive security.....	179
8.2.9	Sensitive security parameters management.....	179
8.2.10	Self-tests.....	180
8.2.11	Life-cycle assurance.....	180
8.2.12	Mitigation of other attacks.....	181
	Bibliography.....	182

ISO/IEC 24759:2025(en)

Foreword

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

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

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

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

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

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

This fourth edition cancels and replaces the third edition (ISO/IEC 24759:2017), which has been technically revised.

The main changes are as follows:

- new terminology has been added;
- ASs, VEs and TEs have been updated according to ISO/IEC 19790:2025; and
- VEs and TEs have been corrected or updated to improve efficiency.

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

ISO/IEC 24759:2025(en)

Introduction

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

ISO/IEC 19790 provides four increasing, qualitative levels of security requirements intended to cover a wide range of potential applications and environments. The cryptographic techniques are identical over the four security levels defined in this document. The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include:

- cryptographic module specification;
- cryptographic module interfaces;
- roles, services and authentication;
- software/firmware security;
- operational environment;
- physical security;
- non-invasive security;
- sensitive security parameter management;
- self-tests;
- life-cycle assurance; and
- mitigation of other attacks.

This document specifies the test requirements for cryptographic modules conforming to ISO/IEC 19790:2025.

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

1 Scope

This document specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2025. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.

This document also specifies the information that vendors are required to provide testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790:2025.

Vendors can also use this document to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:2025 before applying to a testing laboratory for testing.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

ISO/IEC 19790:2025, *Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules*

ISO/IEC 20085-1, *IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques*

ISO/IEC 20085-2, *IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 2: Test calibration methods and apparatus*

ISO/IEC 20543, *Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN