

STN P	Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Požiadavky na spôsobilosť laboratórií na testovanie a hodnotenie bezpečnosti IT Časť 2: Testovanie podľa ISO/IEC 19790 (ISO/IEC TS 23532-2: 2021)	STN P CEN/CLC ISO/IEC/TS 23532-2 97 4164
------------------	--	--

Information security, cybersecurity and privacy protection
Requirements for the competence of IT security testing and evaluation laboratories
Part 2: Testing for ISO/IEC 19790

Sécurité de l'information, cybersécurité et protection de la vie privée
Exigences relatives aux compétences des laboratoires d'essais et d'évaluation de la sécurité TI
Partie 2: Essais pour l'ISO/IEC 19790

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre
Anforderungen an die Kompetenz von Prüf- und Evaluierungsstellen für IT-Sicherheit
Teil 2: Prüfung für ISO/IEC 19790

Táto predbežná slovenská technická norma je slovenskou verzou CEN/CLC ISO/IEC/TS 23532-2: 2024.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN P CEN/CLC ISO/IEC/TS 23532-2 má rovnaké postavenie, ako majú oficiálne verzie.

This prestandard is the Slovak version of CEN/CLC ISO/IEC/TS 23532-2: 2024.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN P CEN/CLC ISO/IEC/TS 23532-2 has the same status as the official versions.

**Táto predbežná slovenská technická norma je určená na overenie. Prípadné pripomienky pošlite
do septembra 2026 Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.**

Nahradenie predchádzajúcich dokumentov

Táto predbežná slovenská technická norma nahrádza anglickú verziu STN P CEN/CLC ISO/IEC/TS 23532-2
z februára 2025 v celom rozsahu.

141414

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2025
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii
v znení neskorších predpisov.

Národný predhovor

Obrázky a matematické výrazy v tejto STN P sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2021 ISO/IEC, ref. č. ISO/IEC TS 23532-2: 2021 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 a TNI možno získať na webovom sídle www.unms.sk.

ISO/IEC 17000 prijatá ako STN EN ISO/IEC 17000 Posudzovanie zhody. Slovník a všeobecné zásady (ISO/IEC 17000) (01 5202)

ISO/IEC 17025: 2017 prijatá ako STN EN ISO/IEC 17025: 2018 Všeobecné požiadavky na kompetentnosť skúšobných a kalibračných laboratórií (ISO/IEC 17025: 2017) (01 5253)

ISO/IEC 19790 prijatá ako STN EN ISO/IEC 19790 Informačné technológie. Bezpečnostné metódy. Bezpečnostné požiadavky na kryptografické moduly (ISO/IEC 19790) (36 9781)

ISO/IEC 19896-1 prijatá ako STN EN ISO/IEC 19896-1 IT bezpečnostné metódy. Požiadavky na kompetentnosť testerov a hodnotiteľov informačnej bezpečnosti. Časť 1: Úvod, koncepty a všeobecné požiadavky (ISO/IEC 19896-1) (97 4138)

ISO/IEC 19896-2 prijatá ako STN EN ISO/IEC 19896-2 IT bezpečnostné metódy. Požiadavky na kompetentnosť testerov a hodnotiteľov informačnej bezpečnosti. Časť 2: Požiadavky na znalosti, zručnosti a efektívnosť pre testerov ISO/IEC 19790 (ISO/IEC 19896-2) (97 4138)

Vypracovanie

Spracovateľ: SynCo, s.r.o., Bratislava, Ing. Lenka Gondová

Technická komisia: TK 37 Informačné technológie

**TECHNICKÁ ŠPECIFIKÁCIA
TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION****CEN/CLC ISO/IEC/TS 23532-2**

September 2024

ICS 35.030

**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia
Požiadavky na spôsobilosť laboratórií na testovanie a hodnotenie bezpečnosti IT
Časť 2: Testovanie podľa ISO/IEC 19790
(ISO/IEC TS 23532-2: 2021)**

Information security, cybersecurity and privacy protection
Requirements for the competence of IT security testing and evaluation laboratories
Part 2: Testing for ISO/IEC 19790
(ISO/IEC TS 23532-2: 2021)

Sécurité de l'information, cybersécurité et protection
de la vie privée
Exigences relatives aux compétences des laboratoires
d'essais et d'évaluation de la sécurité TI
Partie 2: Essais pour l'ISO/IEC 19790
(ISO/IEC TS 23532-2: 2021)

Informationssicherheit, Cybersicherheit und
Schutz der Privatsphäre
Anforderungen an die Kompetenz von Prüf-
und Evaluierungsstellen für IT-Sicherheit
Teil 2: Prüfung für ISO/IEC 19790
(ISO/IEC TS 23532-2: 2021)

Túto technickú špecifikáciu (CEN/TS) schválil CEN 16. septembra 2024 na predbežné používanie.

Obdobie platnosti tejto CEN/TS je obmedzené spočiatku na tri roky. Členovia CEN a CENELEC budú po dvoch rokoch požiadaní o predloženie pripomienok súvisiacich najmä s otázkou, či sa má CEN/TS zmeniť na európsku normu.

Členovia CEN a CENELEC sú povinní oznámiť existenciu tejto technickej špecifikácie CEN/TS takým istým spôsobom ako EN a vhodnou formou sprístupniť túto CEN/TS na národnej úrovni. Do konečného rozhodnutia o možnej konverzii CEN/TS na EN je možné ponechať v platnosti (paralelne s CEN/TS) aj rozporné národné normy.

Členmi CEN a CENELEC sú národné normalizačné organizácie Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

CEN

Európsky výbor pre normalizáciu
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

CENELEC

Európsky výbor pre normalizáciu v elektrotechnike
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Riadiace stredisko CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

Obsah

strana

Európsky predhovor	6
Úvod	7
1 Predmet	8
2 Normatívne odkazy	8
3 Termíny a definície	8
4 Všeobecné požiadavky	9
4.1 Nestrannosť	9
4.2 Dôvernosť	10
5 Štrukturálne požiadavky	10
6 Požiadavky na zdroje	11
6.1 Všeobecne	11
6.2 Pracovníci	12
6.3 Priestory a podmienky prostredia	13
6.4 Zariadenie	15
6.5 Metrologická nadväznosť	18
6.6 Externe poskytované produkty a služby	19
7 Požiadavky na proces	20
7.1 Preskúmanie požiadaviek, tendrov a zmlúv	20
7.2 Výber, verifikácia a validácia metód	21
7.2.1 Výber a verifikácia metód	21
7.2.2 Validácia metód	22
7.3 Odber vzoriek	22
7.4 Zaobchádzanie s predmetmi skúšania alebo kalibrácie	23
7.5 Technické záznamy	23
7.6 Hodnotenie neistoty merania	24
7.7 Zabezpečenie platnosti výsledkov	24
7.8 Oznamovanie výsledkov	24
7.8.1 Všeobecne	24
7.8.2 Spoločné požiadavky na správy (o skúškach, o kalibráciách alebo o odbere vzoriek)	25
7.8.3 Špecifické požiadavky na protokoly o skúškach	26
7.8.4 Špecifické požiadavky na kalibračné certifikáty	26
7.8.5 Protokoly o odbere vzoriek – špecifické požiadavky	26
7.8.6 Oznamovanie vyhlásení o zhode	26
7.8.7 Oznamovanie názorov a interpretácií	26
7.8.8 Dodatky k správam	26
7.9 Sťažnosti	27
7.10 Nezhodná práca	27
7.11 Riadenie údajov a manažérstvo informácií	27

8	Požiadavky na systém manažérstva.....	28
8.1	Možnosti.....	28
8.1.1	Všeobecne.....	28
8.1.2	Možnosť A	28
8.1.3	Možnosť B.....	28
8.2	Dokumentovanie systému manažérstva (možnosť A)	28
8.3	Riadenie dokumentov systému manažérstva (možnosť A).....	29
8.4	Riadenie záznamov (možnosť A).....	29
8.5	Opatrenia na zvládanie rizík a príležitostí (možnosť A)	29
8.6	Zlepšovanie (možnosť A)	29
8.7	Nápravné opatrenia (možnosť A)	30
8.8	Interné audity (možnosť A)	30
8.9	Preskúmania manažmentom (možnosť A).....	30
Príloha A	(informatívna) – Metrologická nadväznosť	31
Príloha B	(informatívna) – Možnosti systému manažérstva.....	32
Príloha C	(informatívna) – Vzťah noriem pri testovaní kryptografických modulov	33
Literatúra		34

Európsky predhovor

Text ISO/IEC TS 23532-2: 2021 vypracovala technická komisia ISO/IEC JTC 1 *Informačné technológie* medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako CEN/CLC ISO/IEC/TS 23532-2: 2024 technickou komisiou CEN-CENELEC/JTC 13 *Kybernetická bezpečnosť a ochrana údajov*, ktorej sekretariát je v DIN.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. CEN-CENELEC nezodpovedá za identifikáciu ktoréhokoli alebo všetkých takýchto patentových práv.

Akákoli'vek spätná väzba a otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu používateľov. Kompletný zoznam týchto orgánov je na webovom sídle CEN a CENELEC.

V súlade s vnútornými predpismi CEN-CENELEC sú túto európsku normu povinné prevziať národné normalizačné organizácie týchto krajín: Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

Oznámenie o schválení

Text ISO/IEC TS 23532-2: 2021 schválil CEN-CENELEC ako CEN/CLC ISO/IEC/TS 23532-2: 2024 bez akýchkoľvek modifikácií.

Úvod

Laboratóriá, ktoré vykonávajú skúšky zhody s normou ISO/IEC 19790 a požiadavkami na skúšky v norme ISO/IEC 24759, môžu využívať a vyžadovať zhodu s normou ISO/IEC 17025: 2017. V norme ISO/IEC 17025: 2017 sa uvádzajú všeobecné požiadavky pre širokú škálu skúšobných a kalibračných laboratórií, aby mohli preukázať, že pracujú kompetentne a sú schopné vytvárať platné výsledky.

Laboratóriá, ktoré vykonávajú takéto validácie, majú osobitné požiadavky na spôsobilosť podľa normy ISO/IEC 19790, ktoré im umožnia získať platné výsledky.

Poskytnutím ďalších podrobností a doplnkových požiadaviek k norme ISO/IEC 17025: 2017, ktoré sú špecifické pre laboratóriá na testovanie a hodnotenie informačnej bezpečnosti, tento dokument uľahčí spoluprácu a lepšiu zhodu a harmonizáciu medzi laboratóriami a inými orgánmi. Tento dokument môžu používať krajiny a akreditačné orgány ako súbor požiadaviek na posudzovanie a akreditáciu laboratórií.

Tento dokument je v záujme uľahčenia implementácie číslovaný rovnako ako norma ISO/IEC 17025: 2017. Doplnujúce požiadavky sú uvedené ako články, ktoré dopĺňajú normu ISO/IEC 17025: 2017.

1 Predmet

Tento dokument rozširuje a dopĺňa postupy a všeobecné požiadavky uvedené v norme ISO/IEC 17025: 2017 pre laboratória vykonávajúce skúšky na základe noriem ISO/IEC 19790 a ISO/IEC 24759.

2 Normatívne odkazy

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).

ISO/IEC 17000 *Conformity assessment – Vocabulary and general principles*. [Posudzovanie zhody. Slovník a všeobecné zásady.]

ISO/IEC 17025: 2017 *General requirements for the competence of testing and calibration laboratories*. [Všeobecné požiadavky na kompetentnosť skúšobných a kalibračných laboratórií.]

ISO/IEC 19790 *Information technology – Security techniques – Security requirements for cryptographic modules*. [Informačné technológie. Bezpečnostné metódy. Bezpečnostné požiadavky na kryptografické moduly.]

ISO/IEC 19896-1 *IT security techniques – Competence requirements for information security testers and evaluators – Part 1: Introduction, concepts and general requirements*. [IT bezpečnostné metódy. Požiadavky na kompetentnosť testerov a hodnotiteľov informačnej bezpečnosti. Časť 1: Úvod, koncepty a všeobecné požiadavky.]

ISO/IEC 19896-2 *IT security techniques – Competence requirements for information security testers and evaluators – Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers*. [IT bezpečnostné metódy. Požiadavky na kompetentnosť testerov a hodnotiteľov informačnej bezpečnosti. Časť 2: Požiadavky na znalosti, zručnosti a efektívnosť pre testerov ISO/IEC 19790.]

koniec náhľadu – text ďalej pokračuje v platenej verzii STN