

2024

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - ČSN  
Ochrana biometrických informací ISO/IEC 24745

36 9887

Information security, cybersecurity and privacy protection - Biometric information protection

Securité de l'information, cybersécurité et protection de la vie privée - Protection des informations biométriques

Tato norma je českou verzí mezinárodní normy ISO/IEC 24745:2022. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 24745:2022. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 30136 dosud nezavedena

Související ČSN

ČSN EN ISO/IEC 2382-37 (36 9001) Informační technologie - Slovník - Část 37: Biometrika

ČSN ISO/IEC 9796 (soubor) (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovou zprávy

ČSN ISO/IEC 9797-1 (36 9782) Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MACs) - Část 1: Mechanismy používající blokovou šifru

ČSN ISO/IEC 9797-3 (36 9782) Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC) - Část 3: Mechanismy používající univerzální hašovací funkci

ČSN ISO/IEC 19785-4 (36 9864) Informační technologie - Společný rámec formátů biometrické výměny - Část 4: Specifikace formátu bezpečnostního bloku

ČSN EN ISO/IEC 19790:2020 (36 9879) Informační technologie - Bezpečnostní techniky - Bezpečnostní požadavky na kryptografické moduly

ČSN ISO/IEC 19792 (36 9858) Informační technologie - Bezpečnostní techniky - Hodnocení bezpečnosti biometriky

ČSN ISO/IEC 19794 (36 9860) Informační technologie - Formáty výměny biometrických dat

ČSN EN ISO/IEC 24760-1 (36 9716) Bezpečnost IT a soukromí - Rámec pro řízení identit - Část 1: Terminologie a pojmy

ČSN EN ISO/IEC 29100:2015 (36 9705) Informační technologie - Bezpečnostní techniky - Rámec soukromí

ČSN ISO/IEC 30107-2 (36 9862) Informační technologie - Detekce biometrického prezentačního útoku - Část 2: Datové formáty

ČSN ISO/IEC 30107-3 (36 9862) Informační technologie - Detekce biometrického prezentačního útoku - Část 3: Testování a podávání zpráv

ČSN ISO/IEC 30107-4 (36 9862) Informační technologie - Detekce biometrického prezentačního útoku - Část 4: Profil pro testování mobilních zařízení

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v člancích „Informace o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Pro účely této normy je anglický termín „guidance“ přeložen jako „pokyn“ vzhledem k jeho používání v oblasti IT a v návaznosti na vydané normy z oblasti IT. Český ekvivalent „návod“ je vzhledem ke kontextu nevhodný a v praxi se v souvislosti s normami „Bezpečnosti IT“ nepoužívá.

Pro účely této normy byly použity následující anglické termíny v původní podobě, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu:

Hill climbing, nonce, Person-in-the-middle.

Upozornění na národní poznámky

Do normy byla k terminologickému heslu 3.27 doplněna upřesňující národní poznámka.

ICS 35.030

Obsah

	Strana
Předmluva.....	5
Úvod.....	6
<b>1</b> ..... Předmět normy.....	7
<b>2</b> ..... Citované dokumenty.....	7
<b>3</b> ..... Termíny, definice a zkrácené termíny.....	7
<b>4</b> ..... Zkrácené termíny.....	12
<b>5</b> ..... Biometrické systémy.....	12
<b>5.1</b> ..... Obecně.....	12
<b>5.2</b> ..... Provoz biometrického systému.....	13
<b>5.3</b> ..... Biometrické reference a odkazy na identitu (IR).....	15
<b>5.4</b> ..... Biometrické systémy a systémy managementu identit.....	15

5.5.....	Osobně identifikovatelné informace (PII) a soukromí.....	16
5.6.....	Společenská hlediska.....	16
6.....	Bezpečnostní aspekty biometrického systému.....	16
6.1.....	Bezpečnostní požadavky pro biometrické systémy na ochranu biometrických informací.....	16
6.1.1.....	Důvěrnost.....	16
6.1.2.....	Integrita.....	17
6.1.3.....	Obnovitelnost a revokovatelnost.....	17
6.1.4.....	Dostupnost.....	17
6.2.....	Bezpečnostní hrozby a protiopatření v biometrických systémech.....	18
6.2.1.....	Hrozby komponentám biometrických systémů a protiopatření.....	18
6.2.2.....	Hrozby a protiopatření během přenosu biometrických informací.....	19
6.2.3.....	Obnovitelné biometrické reference jako technologie protiopatření.....	20
6.3.....	Bezpečnost datových záznamů obsahujících biometrické informace.....	21
6.3.1.....	Bezpečnost zpracování biometrických informací v jednotlivé databázi.....	21
6.3.2.....	Bezpečnost zpracování biometrických informací v oddělených databázích.....	23
7.....	Management soukromí biometrických informací.....	24

<b>7.1.....</b>	<b>Hrozby pro soukromí biometrických informací.....</b>	<b>24</b>
<b>7.2.....</b>	<b>Požadavky a směrnice pro soukromí biometrických informací.....</b>	<b>25</b>
<b>7.2.1.....</b>	<b>Nevratnost.....</b>	<b>25</b>
<b>7.2.2.....</b>	<b>Nepropojitelnost.....</b>	<b>25</b>
<b>7.2.3.....</b>	<b>Důvěrnost.....</b>	<b>25</b>
<b>7.3.....</b>	<b>Management soukromí životního cyklu biometrických informací.....</b>	<b>25</b>

<b>7.3.1.....</b>	
Shromažďování.....	
.....	25
<b>7.3.2.....</b>	Přenos (zpřístupnění informací třetí straně).....
	26
<b>7.3.3.....</b>	
Použití.....	
.....	26
<b>7.3.4.....</b>	
Uložení.....	
.....	26
<b>7.3.5.....</b>	
Uchovávání.....	
.....	27
<b>7.3.6.....</b>	Archivování a zálohování dat.....
	27
<b>7.3.7.....</b>	
Odstranění.....	
.....	27
<b>7.4.....</b>	Povinnosti vlastníka biometrického systému.....
	27
<b>8.....</b>	Modely aplikací biometrických systémů a bezpečnost.....
	28
<b>8.1.....</b>	Modely aplikací biometrických systémů.....
	28
<b>8.2.....</b>	Bezpečnost v každém modelu biometrické aplikace.....
	29
<b>8.2.1.....</b>	
Obecně.....	
.....	29
<b>8.2.2.....</b>	Model A - Uložení na serveru a porovnání na serveru.....
	29
<b>8.2.3.....</b>	Model B - Uložení na tokenu a porovnání na serveru.....
	31
<b>8.2.4.....</b>	Model C - Uložení na serveru a porovnání na

klientovi.....	32
<b>8.2.5.....</b> Model D - Uložení na klientovi a porovnání na klientovi.....	34
<b>8.2.6.....</b> Model E - Uložení na tokenu a porovnání na klientovi.....	35
<b>8.2.7.....</b> Model F - Uložení na tokenu a porovnání na tokenu.....	37
<b>8.2.8.....</b> Model G - Distribuované uložení na tokenu a serveru, porovnání na serveru.....	38
<b>8.2.9.....</b> Model H - Distribuované uložení na tokenu a na klientovi, porovnání na klientovi.....	39
<b>8.2.10...</b> Model I - Uložení na serveru, distribuované porovnání.....	40
<b>8.2.11...</b> Model J - Uložení na tokenu, distribuované porovnání.....	42
<b>8.2.12...</b> Model K - Distribuované uložení, distribuované porovnání.....	43
<b>Příloha A</b> (informativní) Bezpečné provázání a použití oddělených DB <sub>IR</sub> a DB <sub>BR</sub> .....	45
<b>Příloha B</b> (informativní) Rámec pro obnovitelné biometrické reference (RBR).....	48
<b>Příloha C</b> (informativní) Příklady technologií pro ochranu biometrických informací.....	51
<b>Příloha D</b> (informativní) Používání biometrického vodoznaku.....	53
<b>Příloha E</b> (informativní) Ochrana biometrických informací pomocí rozdělení informací.....	55
<b>Příloha F</b> (informativní) Výběr modelů biometrických aplikací.....	56
Bibliografie.....	58



© ISO/IEC 2022

Veškerá práva vyhrazena. Žádná část této publikace nesmí být, není-li specifikováno jinak nebo nepožaduje-li se to v souvislosti s její implementací, reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopíí nebo zveřejňování na internetu nebo intranetu, bez předchozího písemného souhlasu. O souhlas lze požádat buď ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

ISO copyright office

CP 401 · Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Tel.: + 41 22 749 01 11

E-mail: [copyright@iso.org](mailto:copyright@iso.org)

Web: [www.iso.org](http://www.iso.org)

Publikováno ve Švýcarsku



# Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezi-národních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnících ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnících ISO/IEC, část 2 (viz [www.iso.org/directives](http://www.iso.org/directives) nebo [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz [www.iso.org/patents](http://www.iso.org/patents)) nebo v seznamu patentových prohlášení obdržených IEC (viz [patents.iec.ch](http://patents.iec.ch)).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), viz [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html). V IEC viz [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 24745:2011), které bylo technicky zrevidováno.

Hlavní změny oproti předchozímu vydání jsou následující:

- oprava termínů;
- odstranění nevyhovujících požadavků týkajících se jurisdikcí;
- objasnění různých vysvětlení;
- zlepšení požadavků na ochranu biometrických informací s výslovnějším prosazováním nevratnosti a nespojitelnosti;
- doplnění příslušných odkazů na ISO/IEC 30136:2018;
- zavedení nových aplikačních modelů založených na nejnovějších technologiích;

- doplnění příkladů v přílohách.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na

[www.iso.org/members.html](http://www.iso.org/members.html)

a [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

# Úvod

S tím, jak se Internet stává všudypřítomnou součástí každodenního života, jsou prostřednictvím Internetu poskytovány různé služby, např. internetové bankovníctví, zdravotní péče na dálku atd. Aby bylo možné tyto služby poskytovat bezpečným způsobem, je stále kritičtější potřeba autentizačních mechanismů mezi subjekty a poskytovanou službou. Některé z již vyvinutých autentizačních mechanismů zahrnují schémata založená na tokenech, osobních identifikačních a transakčních číslech (PIN/TAN), schémata digitálního podpisu založená na kryptografických systémech s veřejným klíčem a autentizační schémata využívající biometrické techniky.

Biometrika, automatické rozpoznávání jednotlivců na základě jejich behaviorálních a fyziologických charakteristik, zahrnuje technologie rozpoznávání založené např. na obrazu otisku prstu, hlasových vzorech, obrazu duhovky, obrazu obličeje a podobně. Náklady na biometrické techniky se snižují, zatímco jejich spolehlivost se zvyšuje, a jsou nyní přijatelné a životaschopné pro použití jako autentizační mechanismus.

Biometrická autentizace přináší potenciální rozpor mezi ochranou soukromí a zárukou autentizace. Na jedné straně jsou biometrické charakteristiky v ideálním případě neměnnou vlastností spojenou s jednotlivcem a jsou pro něj výrazné. Tato vazba průkazní informace na osobu poskytuje silnou záruku autentizace. Na druhé straně je tato silná vazba také základem obav o soukromí souvisících s používáním biometriky, jako je nezákonné zpracování biometrických dat, a představuje výzvy pro bezpečnost biometrických systémů, aby se zabránilo kompromitaci biometrických referencí (BR). Obvyklé řešení kompromitace autentizační průkazní informace (změna hesla nebo vydání nového tokenu) není pro biometrickou autentizaci obecně dostupné, protože biometrické charakteristiky, které jsou buď vnitřními fyziologickými vlastnostmi nebo rysy chování jednotlivců, je obtížné nebo nemožné změnit. Nanejvýš lze registrovat jinou instanci prstu nebo oka, ale výběr je obvykle omezený. Proto jsou nezbytná vhodná protopatření k zajištění bezpečnosti biometrického systému a soukromí subjektů biometrických dat.

Biometrické systémy obvykle spojují BR s dalšími osobně identifikovatelnými informacemi (PII) pro autentizaci jednotlivců. V tomto případě je takové spojení nutné k zajištění bezpečnosti datového záznamu obsahujícího biometrické informace. Rostoucí propojení BR s jinými PII a sdílení biometrických informací napříč právními jurisdikcemi extrémně ztěžují organizacím zajištění ochrany biometrických informací a dosažení souladu s různými předpisy na ochranu soukromí.

# 1 Předmět normy

Tento dokument se zabývá ochranou biometrických informací v rámci různých požadavků na důvěrnost, integritu a obnovitelnost/odvolatelnost během uchovávání a přenosu. Poskytuje také požadavky a doporučení pro bezpečný management a zpracování biometrických informací v souladu s ochranou soukromí.

Tento dokument specifikuje následující:

- analýzu hrozeb a protiopatření souvisejících s biometrikou a modely aplikací biometrických systémů;
- bezpečnostní požadavky na bezpečné propojení biometrické reference (BR) a odkazu na identitu (IR);
- modely aplikací biometrických systémů s různými scénáři pro ukládání a porovnávání biometrických referencí;
- pokyny pro ochranu soukromí jednotlivce při zpracování biometrických informací.

Tento dokument nezahrnuje obecné záležitosti managementu týkající se fyzické bezpečnosti, bezpečnosti prostředí a managementu klíčů pro kryptografické techniky.

**Konec náhledu - text dále pokračuje v placené verzi ČSN.**