

2021

Bezpečnost informací – Kritéria a metodika
pro hodnocení bezpečnosti biometrických systémů –
Část 1: Rámec

ČSN
ISO/IEC 19989-1

36 9859

Information security – Criteria and methodology for security evaluation of biometric systems –
Part 1: Framework

Sécurité de l'information – Critères et méthodologie pour l'évaluation de la sécurité des systèmes
biométriques –
Partie 1: Cadre

Tato norma je českou verzí mezinárodní normy ISO/IEC 19989-1:2020. 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 19989-1:2020. 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 2382:2008 nezavedena

ISO/IEC 2382-37:2017 zavedena v ČSN ISO/IEC 2382-37:2018 (36 9001) Informační technologie –
Slovník – Část 37: Biometrika

ISO/IEC 15408-1:2009 zavedena v ČSN EN ISO/IEC 15408-1:2013 (36 9789) Informační
technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a obecný
model

ISO/IEC 15408-2:2008 zavedena v ČSN EN ISO/IEC 15408-2:2010 (36 9789) Informační
technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní
funkční komponenty

ISO/IEC 15408-3:2008 zavedena v ČSN EN ISO/IEC 15408-3:2010 (36 9789) Informační
technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty
bezpečnostních záruk

ISO/IEC 18045:2008 zavedena v ČSN EN ISO/IEC 18045:2020 (36 9805) Informační technologie –

Souvisící ČSN

ČSN ISO/IEC 19792:2016 (36 9858) Informační technologie – Bezpečnostní techniky – Hodnocení bezpečnosti biometricky

ČSN ISO/IEC 19795-1 (36 9861) Informační technologie – Testování a hodnocení výkonnosti biometrik – Část 1: Principy a základní struktura

ČSN ISO/IEC 30107-1:2019 (36 9862) Informační technologie – Detekce biometrického prezentačního útoku – Část 1: Rámec

ČSN ISO/IEC 30107-3:2019 (36 9862) Informační technologie – Detekce biometrického prezentačního útoku – Část 3: Testování a podávání zpráv

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).

Upozornění na národní poznámky

Do kapitoly 7 byla doplněna národní poznámka upozorňující na nesprávné označení třídy FPT.

Vypracování normy

Zpracovatel: Prof. Ing., Dipl. Ing. Martin Drahanský, Ph.D., IČO 73840602

Technická normalizační komise: TNK 42 Výměna dat

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

ICS 35.030

Obsah

Strana

Předmluva.....	7
Úvod.....	8
1..... Předmět normy.....	9
2..... Citované dokumenty.....	9
3..... Termíny a definice.....	9
4..... Zkratky a zkrácené termíny.....	11
5..... Obecné poznámky.....	12
6..... Zranitelnosti v biometrických systémech a hodnocení bezpečnosti.....	12
6.1..... Kategorizace běžných zranitelností biometrických systémů.....	12
6.2..... Biometrický systém a detekce prezentačního útoku.....	15
6.3..... Kategorizace TOE ve vztahu k typu hodnocení.....	16
6.3.1... Hodnocení výkonnosti biometrického	

rozpoznávání.....	16
6.3.2... Hodnocení	
PAD.....	17
7..... Rozšířené bezpečnostní funkční komponenty pro třídu FPT: Ochrana	
TSF.....	17
7.1.....	
Obecně.....	17
7.2..... Detekce prezentačního útoku	
(FPT_PAD).....	17
7.2.1... Chování	
rodiny.....	17
7.2.2... Vyrovnání	
komponent.....	17
7.2.3... Správa	
FPT_PAD.1.....	17
7.2.4... Audit	
FPT_PAD.1.....	18
7.2.5... FPT_PAD.1 Detekce prezentačního	
útoku.....	18
7.3..... Biometrické zachycení s detekcí prezentačního útoku	
(FPT_BCP).....	18
7.3.1... Chování	
rodiny.....	18
7.3.2... Vyrovnání	
komponent.....	18
7.3.3... Správa	
FPT_BCP.1.....	19
7.3.4... Správa	
FPT_BCP.2.....	19

7.3.5... Audit	
FPT_BCP.1.....	
.....	19
7.3.6... Audit	
FPT_BCP.2.....	
.....	19
7.3.7... FPT_BCP.1 Kontrola zachycení biometrických vzorků	
.....	19
7.3.8... FPT_BCP.2 Biometrické zachycení s nízkou mírou selhání	
.....	19
8..... Rozšířené bezpečnostní funkční komponenty pro třídu FIA: Identifikace a autentizace	
.....	20
8.1.....	
Obecně.....	
.....	20

8.2..... Registrace biometrické reference (FIA_EBR).....	20
8.2.1... Chování rodiny.....	20
8.2.2... Vyrovnání komponent.....	20
8.2.3... Správa FIA_EBR.1.....	20
8.2.4... Správa FIA_EBR.2.....	20
8.2.5... Audit FIA_EBR.1.....	21
8.2.6... Audit FIA_EBR.2.....	21
8.2.7... FIA_EBR.1 Kontrola biometrických vzorků pro registraci.....	21
8.2.8... FIA_EBR.2 Biometrická registrace s nízkou mírou selhání registrace.....	21
8.3..... Biometrická verifikace (FIA_BVR).....	21
8.3.1... Chování rodiny.....	21
8.3.2... Vyrovnání komponent.....	22
8.3.3... Správa FIA_BVR.1.....	22
8.3.4... Správa FIA_BVR.2.....	

.....	22
8.3.5... Správa	
FIA_BVR.3.....	
.....	22
8.3.6... Správa	
FIA_BVR.4.....	
.....	22
8.3.7... Audit	
FIA_BVR.1.....	
.....	22
8.3.8... Audit	
FIA_BVR.2.....	
.....	23
8.3.9... Audit	
FIA_BVR.3.....	
.....	23
8.3.10 Audit	
FIA_BVR.4.....	
.....	23
8.3.11 FIA_BVR.1 Biometrická verifikace s vysokou	
výkonností.....	23
8.3.12 FIA_BVR.2 Načasování autentizace uživatelů s biometrickou	
verifikací.....	23
8.3.13 FIA_BVR.3 Autentizace uživatele s biometrickou verifikací před jakoukoli	
akcí.....	24
8.3.14 FIA_BVR.4 Biometrická verifikace nepřijímající nástroje prezentačního	
útku.....	24
8.4..... Biometrická identifikace	
(FIA_BID).....	24
8.4.1... Chování	
rodiny.....	
.....	24
8.4.2... Vyrovnání	
komponent.....	
.....	24
8.4.3... Správa	
FIA_BID.1.....	
.....	25

8.4.4... Správa	
FIA_BID.2.....	
.....	25
8.4.5... Správa	
FIA_BID.3.....	
.....	25
8.4.6... Správa	
FIA_BID.4.....	
.....	25
8.4.7... Audit	
FIA_BID.1.....	
.....	25
8.4.8... Audit	
FIA_BID.2.....	
.....	25
8.4.9... Audit	
FIA_BID.3.....	
.....	25
8.4.10 Audit	
FIA_BID.4.....	
.....	25
8.4.11 FIA_BID.1 Biometrická identifikace s vysokou	
výkonností.....	26
8.4.12 FIA_BID.2 Načasování biometrické	
identifikace.....	26
8.4.13 FIA_BID.3 Biometrická identifikace před jakoukoli	
akcí.....	26
8.4.14 FIA_BID.4 Biometrická verifikace nepřijímající nástroje prezentačního	
útku.....	26
9..... Doplnkové činnosti k ISO/IEC 18045 ve třídě APE: Hodnocení profilu	
ochrany.....	27
10..... Doplnkové činnosti k ISO/IEC 18045 ve třídě ASE: Bezpečnostní	
cíl.....	27
11..... Doplnkové činnosti k ISO/IEC 18045 ve třídě ADV:	
Vývoj.....	28
11.1.... Doplnkové činnosti k bezpečnostní architektuře	
ADV_ARC.....	28

11.2.... Doplnkové činnosti k funkční specifikaci	
ADV_FSP.....	28
11.2.1 Doplnkové činnosti k hodnocení dílčí činnosti	
ADV_FSP.1.....	28
11.2.2 Doplnkové činnosti k hodnocení dílčí činnosti	
ADV_FSP.2.....	29
11.2.3 Doplnkové činnosti k hodnocení dílčí činnosti	
ADV_FSP.3.....	30
11.2.4 Doplnkové činnosti k hodnocení dílčí činnosti	
ADV_FSP.4.....	31
11.3.... Doplnkové činnosti k návrhu TOE	
ADV_TDS.....	32
11.3.1 Doplnkové činnosti k hodnocení dílčí činnosti	
ADV_TDS.1.....	32
11.3.2 Doplnkové činnosti k hodnocení dílčí činnosti	
ADV_TDS.2.....	32
11.3.3 Doplnkové činnosti k hodnocení dílčí činnosti	
ADV_TDS.3.....	33
12..... Doplnkové činnosti k ISO/IEC 18045 ve třídě AGD: Dokumenty s návody.....	33
12.1.... Doplnkové činnosti k provozní uživatelské příručce	
AGD_OPE.....	33
12.2.... Doplnkové činnosti k přípravným postupům	
AGD_PRE.....	34
13..... Doplnkové činnosti k ISO/IEC 18045 ve třídě ALC: Podpora životního cyklu.....	34
13.1.... Doplnkové činnosti k podpoře životního cyklu	
ALC_CMS.....	34
13.2.... Doplnkové činnosti k dodání	
ALC_DEL.....	35
13.3.... Doplnkové činnosti k nápravě závad	
ALC_FLR.....	35
14..... Doplnkové činnosti k ISO/IEC 18045 ve třídě ATE: Testy.....	35
14.1.... Doplnkové činnosti k funkčním testům	

ATE_FUN.....	35
14.2.... Doplnkové činnosti k nezávislému testování	
ATE_IND.....	36
14.2.1	
Obecně.....	36
14.2.2 Doplnkové činnosti k hodnocení dílčí činnosti	
ATE_IND.1.....	36
14.2.3 Doplnkové činnosti k hodnocení dílčí činnosti	
ATE_IND.2.....	37
15..... Doplnkové činnosti k ISO/IEC 18045 ve třídě AVA:	
Zranitelnost.....	38
15.1....	
Obecně.....	38
15.2.... Doplnkové činnosti k analýze zranitelnosti	
AVA_VAN.....	38
15.2.1 Doplnkové činnosti k hodnocení dílčí činnosti	
AVA_VAN.2.....	38
15.2.2 Doplnkové činnosti k hodnocení dílčí činnosti	
AVA_VAN.3.....	40
15.2.3 Doplnkové činnosti k hodnocení dílčí činnosti	
AVA_VAN.4.....	41
Příloha A (informativní) Úvod do základních pojmů	
ISO/IEC 15408.....	42
Příloha B (normativní) Třída FPT: ochrana	
TSF.....	44
Příloha C (normativní) Třída FIA: identifikace	
a autentizace.....	45
Příloha D (informativní) Základní informace o doplňkových činnostech pro hodnocení	
PAD.....	48
Příloha E (informativní) Ostatní obecné	
zranitelnosti.....	53
Příloha F (normativní) Potenciál útoku a odolnost	
TOE.....	55
Bibliografie.....	



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2020

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 fotokopii 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

Web: 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 mezinárodních norem prostřednictvím 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).

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 obdržných ISO (viz www.iso.org/patents) nebo v seznamu patentových prohlášení obdržných IEC (viz <http://patents.iec.ch>).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamena 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), jsou uvedeny na www.iso.org/iso/foreword.html.

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

Seznam všech částí souboru ISO/IEC 19989 lze nalézt na webových stránkách ISO.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na adrese www.iso.org/members.html.

Úvod

Biometrické systémy mohou být zranitelné vůči prezentačním útokům, kdy se útočníci pokoušejí rozvrátit bezpečnostní politiku systému tím, že prezentují své přirozené biometrické charakteristiky nebo artefakty obsahující kopírované nebo předstírané vlastnosti. K prezentačním útokům může dojít během události registrace nebo identifikace/verifikace. Techniky určené k detekci prezentačních artefaktů se obecně liší od technik odvrácení útoků, kde se používají přirozené charakteristiky. Ochrana před prezentačními útoky s přirozenými charakteristikami se obvykle spoléhá na schopnost biometrického systému rozlišovat mezi oprávněnými registrovanými subjekty a útočníky na základě rozdílů mezi jejich přirozenými biometrickými charakteristikami. Tato schopnost je charakterizována výkonností biometrického rozpoznávání systému. Výkonnost biometrického rozpoznávání a detekce prezentačního útoku mají vliv na bezpečnost biometrických systémů. Hodnocení těchto aspektů výkonnosti z hlediska bezpečnosti se proto stane důležitým faktorem při pořizování biometrických produktů a systémů.

Biometrické produkty a systémy sdílejí mnoho vlastností jiných produktů a systémů IT, u kterých se k hodnocení bezpečnosti z pohledu normalizace využívá soubor norem ISO/IEC 15408 a norma ISO/IEC 18045. Biometrické systémy však ztělesňují určité funkce, které vyžadují specializovaná hodnotící kritéria a metodiku, která není řešena souborem ISO/IEC 15408 a ISO/IEC 18045. Tyto se týkají především hodnocení biometrického rozpoznávání a prezentačního útoku. To jsou funkce, kterým se věnuje soubor ISO/IEC 19989.

ISO/IEC 19792 popisuje tyto biometrické aspekty a specifikuje principy, které je třeba vzít v úvahu při hodnocení bezpečnosti biometrických systémů. Nespecifikuje však konkrétní kritéria a metodiku, které jsou nutné pro hodnocení bezpečnosti na základě souboru ISO/IEC 15408.

Soubor ISO/IEC 19989 představuje most mezi principy hodnocení biometrických produktů a systémů definovaných v ISO/IEC 19792 a kritérii a metodickými požadavky pro hodnocení bezpečnosti na základě souboru ISO/IEC 15408. Soubor ISO/IEC 19989 doplňuje soubory ISO/IEC 15408 a ISO/IEC 18045 tím, že poskytuje rozšířené bezpečnostní funkční komponenty spolu s doplňkovými činnostmi souvisejícími s těmito požadavky. Rozšíření požadavků a doplňkových činností nalezených v souboru ISO/IEC 15408 a v ISO/IEC 18045 souvisí s hodnocením biometrického rozpoznávání a prezentačního útoku, které se týkají zejména biometrických systémů.

Tento dokument obsahuje zavedení obecného rámce pro hodnocení bezpečnosti biometrických systémů, včetně rozšířených bezpečnostních funkčních komponent a doplňkové metodiky a hodnotících činností pro hodnotitele. Podrobná doporučení jsou vypracována pro aspekty biometrického rozpoznávání v ISO/IEC 19989-2 a pro aspekty detekce prezentačního útoku v ISO/IEC 19989-3.

V tomto dokumentu se termín „uživatel“ používá k označení termínu „subjekt zachycení“ používaný v biometrice.

1 Předmět normy

Pro hodnocení bezpečnosti výkonnosti biometrického rozpoznávání a detekce prezentačního útoku pro systémy biometrické verifikace a systémy biometrické identifikace tento dokument stanovuje:

- rozšířené bezpečnostní funkční komponenty pro třídy SFR v ISO/IEC 15408-2;
- doplňkové činnosti k metodice uvedené v ISO/IEC 18045 pro třídy SAR dle ISO/IEC 15408-3.

Tento dokument zavádí obecný rámec pro hodnocení bezpečnosti biometrických systémů, včetně rozšířených bezpečnostních funkčních komponent, a doplňkových činností k metodice, což jsou další hodnotící činnosti a návod/

doporučení pro hodnotitele, který má tyto činnosti zpracovat. V tomto dokumentu jsou rozvinuty činnosti doplňkového hodnocení, zatímco podrobná doporučení jsou vypracována v ISO/IEC 19989-2 (pro aspekty biometrického rozpoznávání) a v ISO/IEC 19989-3 (pro aspekty detekce prezentačního útoku). Tento dokument je použitelný pouze pro TOE pro samostatné typy biometrických charakteristik. Je však povolen výběr charakteristiky z více charakteristik v SFR.

Konec náhledu - text dále pokračuje v placené verzi ČSN.