

Informační technologie - Bezpečnostní techniky -
Hodnocení bezpečnosti biometrie

ČSN
ISO/IEC 19792
36 9858

Information technology - Security techniques - Security evaluation of biometrics

Technologies de l'information - Techniques de sécurité - Cadre de la sécurité pour l'évaluation et le test de la technologie biométrique

Tato norma je českou verzí mezinárodní normy ISO/IEC 19792:2009. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 19792:2009. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 19795-1:2006 zavedena v ČSN ISO/IEC 19795-1:2008 (36 9861) Informační technologie - Testování a hodnocení výkonnosti biometrie - Část 1: Principy a základní struktura

Souvisící ČSN

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

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

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

Vypracování normy

Zpracovatel: Ing. Alena Höningová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 19792

Hodnocení bezpečnosti biometriky První vydání

2009-08-01

ICS 35.040

Obsah

Strana

Předmluva 6

1 Předmět normy 7

2 Shoda 7

3 Citované dokumenty 8

4 Termíny a definice 8

4.1 Obecně 8

4.2 Biometrické systémy 9

4.3 Biometrické procesy 10

4.4 Chybovosti 12

4.5 Statistické definice 13

5 Zkrácené termíny 13

6 Hodnocení bezpečnosti 13

6.1 Přehled 13

6.2 Metodika 14

7 Chybovost biometrických systémů 15

7.1 Úvod 15

7.2 Koncept – Testování chybovosti souvisící s bezpečností 15

7.2.1 Popis systému (Krok 1) 15

7.2.2 Prohlášení dodavatele (Krok 2) 16

7.2.3	Přezkoumání prohlášení dodavatele (Krok 3)	16
7.2.4	Test dodavatele a vyhodnocení testu dodavatele (Krok 4 a 5)	17
7.2.5	Nezávislé testování (Krok 6)	21
8	Posouzení zranitelností	21
8.1	Úvod	21
8.2	Posouzení zranitelností	22
8.2.1	Přehled	22
8.2.2	Přehled hrozeb pro biometrické systémy	23
8.2.3	Další zranitelnosti	23
8.3	Obecné zranitelnosti biometrických systémů	23
8.3.1	Úvod	23
8.3.2	Limity výkonnosti	23
8.3.3	Artefakt biometrických charakteristik	24
8.3.4	Modifikace biometrických charakteristik	25
8.3.5	Obtížnost utajení biometrických charakteristik	26
8.3.6	Podobnost způsobená pokrevními vztahy	26
8.3.7	Speciální biometrické charakteristiky	27
8.3.8	Uměle vytvořené biometrické vzorky typu vlk	28
8.3.9	Nepřátelské prostředí	29
8.3.10	Procedurální zranitelnosti v celém procesu registrace	29
8.3.11	Únik a úprava biometrických dat	30
9	Soukromí	30
9.1	Přehled	30
9.1.1	Ochrana dat	31
9.1.2	Svázání aplikací	31
9.1.3	Deaktivace účtu biometrických referenčních dat	31
9.1.4	Deregistrace	31

Příloha A (informativní) Referenční model biometrického systému 32

A.1 Úvod 32

A.2 Referenční model 32

A.3 Subsystémy a komponenty 32

A.4 Biometrické funkce 35

A.5 Provozní podmínky a podmínky okolního prostředí biometrického systému 36

Bibliografie 37

Odmítnutí odpovědnosti za manipulaci s PDF souborem

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, pokud nejsou typy písma, které jsou vloženy, používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytvoření tohoto souboru PDF lze najít ve Všeobecných informacích, které se vztahují k souboru; parametry, na jejichž základě byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členská organizace ISO mohly používat.

V málo pravděpodobném případě, že vznikne problém, který se týká souboru, informujte o tom Ústřední sekretariát ISO na níže uvedené adrese.



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2009

Veškerá práva vyhrazena. Není-li specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně pořizování fotokopií nebo zveřejnění na internetu nebo intranetu, bez předchozího písemného svolení. O písemné svolení lze požádat buď přímo ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 19792 vypracovala společná technická komise ISO/IEC JTC1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

1 Předmět normy

Tato mezinárodní norma specifikuje subjekty, které budou předmětem hodnocení bezpečnosti biometrického systému.

Pokrývá pro biometriku specifické aspekty a principy, které mají být zvažovány během hodnocení bezpečnosti biometrického systému. Nezabývá se nebiometrickými aspekty, které mohou utvářet část celkového hodnocení bezpečnosti systému používajícího biometrické technologie (například požadavky na databáze nebo komunikační kanály).

Cílem této mezinárodní normy není definovat jakoukoliv konkrétní metodologii pro hodnocení bezpečnosti biometrických systémů, ale místo toho se zaměřuje na základní požadavky. Požadavky v této mezinárodní normě jako takové jsou nezávislé na jakémkoliv hodnotícím nebo certifikačním schématu a bude nutné je začlenit do kontextu konkrétního schématu a upravit je předtím, než budou v tomto kontextu použity.

Tato mezinárodní norma definuje různé oblasti, které je důležité vzít v úvahu v průběhu hodnocení bezpečnosti biometrického systému. Tyto oblasti jsou reprezentovány následujícími kapitolami této mezinárodní normy:

- kapitoly 4 a 5 této mezinárodní normy podávají přehled všech použitých termínů, definic a akronymů,
- kapitola 6 zavádí celkový koncept hodnocení bezpečnosti biometrického systému,
- kapitola 7 popisuje statistické aspekty chybovostí týkajících se bezpečnosti,
- kapitola 8 se zabývá posouzením zranitelnosti biometrických systémů a
- kapitola 9 popisuje hodnocení aspektů soukromí.

Tato mezinárodní norma je důležitá pro komunity hodnotitelů i vývojářů.

- Specifikuje požadavky na hodnotitele a poskytuje návod k provádění hodnocení bezpečnosti biometrického systému.
- Slouží k informování vývojářů o požadavcích na hodnocení biometrické bezpečnosti, aby je tak pomohla připravit pro hodnocení bezpečnosti.

Ačkoliv je tato mezinárodní norma nezávislá na jakémkoliv specifickém schématu hodnocení, mohla by sloužit jako rámec pro vývoj konkrétních metodologií hodnocení a testování k integrování požadavků pro biometrická hodnocení do existujících schémat hodnocení a certifikací.

Tato mezinárodní norma se odvolává na další biometrické normy, které také využívá, zejména normy pro testování a podávání zpráv o biometrické výkonnosti z ISO/JTC1 SC 37. Tyto normy byly upraveny dle nutnosti pro specifické požadavky hodnocení biometrické bezpečnosti.

Konec náhledu - text dále pokračuje v placené verzi ČSN.