

Informační technologie – Bezpečnostní techniky – Ochrana biometrických informací

ČSN
ISO/IEC 24745
36 9887

Information technology – Security techniques – Biometric information protection

Technologies de l'information – Techniques de sécurité – Protection des informations biométriques

Tato norma je českou verzí mezinárodní normy ISO/IEC 24745:2011. 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 24745:2011. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Souvisící ČSN

ČSN ISO/IEC 19092:2009 (97 9123) Finanční služby – Biometrika – Struktura bezpečnosti

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

ČSN ISO/IEC 9796 (všechny části) (36 9780) Informační technologie – Bezpečnostní techniky – Schémata digitálního podpisu umožňující obnovu zprávy

ČSN ISO/IEC 9797 (všechny části) (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MACs)

ČSN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN ISO/IEC 7816-4:2006 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 4: Organizace, bezpečnost a příkazy pro výměnu

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42 Výměna dat

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 24745
Ochrana biometrických informací První vydání
2011-06-15

ICS 35.040

Obsah

Strana

Předmluva 6

Úvod 7

1 Předmět normy 8

2 Termíny a definice 8

3 Zkrácené termíny 12

4 Biometrické systémy 13

4.1 Úvod k biometrickým systémům 13

4.2 Operace biometrického systému 14

4.3 Biometrické reference a identitní reference 15

4.4 Biometrické systémy a systémy řízení identity 16

4.5 Osobně identifikovatelné informace a univerzální jedinečné identifikátory 16

4.6 Společenské úvahy 17

5 Bezpečnostní aspekty biometrického systému 17

5.1 Bezpečnostní požadavky pro biometrické systémy na ochranu biometrických informací 17

5.2 Bezpečnostní hrozby a protiopatření v biometrických systémech 18

5.3 Bezpečnost datových záznamů obsahujících biometrické informace 21

6 Řízení soukromí biometrických informací 24

6.1 Hrozby pro soukromí biometrických informací 24

6.2 Požadavky a směrnice pro soukromí biometrických informací 24

6.3	Regulační požadavky a požadavky politiky	25
6.4	Řízení soukromí životního cyklu biometrických informací	25
6.5	Povinnosti vlastníka biometrického systému	26
7	Modely aplikací biometrických systémů a bezpečnost	27
7.1	Modely aplikací biometrických systémů	27
7.2	Bezpečnost v každém modelu biometrické aplikace	28
Příloha A	(informativní) Bezpečné svázání a použití oddělených DB_{IR} a DB_{BR}	39
A.1	Obecně	39
A.2	Bezpečné svázání mezi oddělenou DB_{IR} a DB_{BR}	39
A.3	Tvrzení BR pro verifikaci	40
A.4	Tvrzení IR pro identifikaci	40
Příloha B	(informativní) Kryptografické algoritmy pro bezpečnost biometrických systémů	42
B.1	Kryptografické algoritmy poskytující důvěrnost	42
B.2	Kryptografické algoritmy poskytující integritu	42
B.3	Kryptografické algoritmy poskytující důvěrnost a integritu	42
Příloha C	(informativní) Rámec pro obnovitelné biometrické reference	43
C.1	Obnovitelné biometrické reference	43
C.2	Vytvoření	43
C.3	Porovnání	44
C.4	Uplynutí doby platnosti	44
C.5	Revokace	44
C.6	Přehled architektury	45
Příloha D	(informativní) Příklady technologií pro obnovitelné biometrické reference	46
D.1	Přehled	46
Příloha E	(informativní) Použití biometrického vodoznaku	48
E.1	Použití biometrického vodoznaku	48
E.2	Vkládání a extrakce biometrického vodoznaku	48

E.3 Příklady aplikací 48

Bibliografie 50



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2011

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace 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) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a 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. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC1.

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

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv.

ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 24745 vypracovala společná technická komise ISO/IEC JTC1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

Úvod

Jak se Internet stává čím dál více všudypřítomnou částí denního života, jsou jeho prostřednictvím

poskytovány různé služby, například internetové bankovníctví, zdravotní péče na dálku, atd. Aby byly tyto služby poskytovány bezpečným způsobem, stává se potřeba autentizačních mechanismů mezi subjekty a poskytovanou službou stále kritičtější. Některé z již vyvinutých autentizačních mechanismů zahrnují schémata založená na tokenech, osobní identifikační a transakční čísla (PIN/TAN), schémata digitálních podpisů založená na kryptosystémech s veřejnými klíči, a autentizační schémata s použitím biometrických technik.

Biometrika – automatické rozpoznávání osob založené na jejich behaviorálních a fyziologických charakteristikách – dospěla, a zahrnuje rozpoznávací technologie založené na obrazu otisku prstů, vzorech hlasu, obrazu duhovky, obrazu obličeje apod. Cena biometrických technik klesá, zatímco jejich spolehlivost se zvyšuje, a jsou nyní akceptovatelné a použitelné jako autentizační mechanismus.

Biometrická autentizace zavádí potenciální diskrepanci mezi soukromím a autentizační zárukou. Na jedné straně jsou biometrické charakteristiky ideálně neměnnou vlastností spojenou s jednotlivou osobou a pro tuto osobu nesporná. Toto svázání pověření (credential) s osobou poskytuje silnou záruku autentizace. Na druhé straně toto silné svázání také představuje základ pro zájmy soukromí spojené s použitím biometriky, například nezákonné zpracování biometrických dat, a představuje výzvy pro bezpečnost biometrických systémů, aby se zabránilo kompromitování biometrických referencí. Obvyklé řešení kompromitování autentizačních pověření – změna hesla nebo vydání nového tokenu – není pro biometrickou autentizaci obecně dostupné, protože biometrické charakteristiky, což jsou buďto skutečné fyziologické vlastnosti nebo behaviorální znaky (traits) jednotlivých osob, je obtížné nebo nemožné změnit. Nanejvýš by mohl být zaregistrován jiný prst nebo oko, ale výběr je obvykle omezený. Proto je podstatné přijetí vhodných protiopatření na ochranu bezpečnosti biometrického systému a soukromí subjektů dat.

Biometrické systémy obvykle svazují biometrickou referenci s jinými osobně identifikovatelnými informacemi (PII, Personally Identifiable Information) k autentizaci jednotlivých osob. V tomto případě je provázanost potřebná, aby se zaručila bezpečnost datového záznamu obsahujícího biometrické informace. V důsledku narůstající provázanosti biometrických referencí s jinými PII a sdílení biometrických informací napříč soudními jurisdikcemi je pro organizace extrémně obtížné zaručit ochranu biometrických informací a dosáhnout shody s různými předpisy týkajícími se soukromí.

1 Předmět normy

Tato mezinárodní norma poskytuje návod na ochranu biometrických informací při různých požadavcích na důvěrnost, integritu a obnovitelnost/revokovatelnost v průběhu uložení a přenosu. Navíc tato mezinárodní norma poskytuje požadavky a směrnice pro bezpečné a soukromí zajišťující řízení a zpracování biometrických informací.

Tato mezinárodní norma specifikuje:

- analýzu hrozeb a protiopatření vlastních biometrickým modelům a aplikačním modelům biometrických systémů;
- bezpečnostní požadavky pro bezpečné svázání biometrické reference a identitní reference;
- modely aplikací biometrických systémů s různými scénáři pro uložení a porovnání biometrických referencí; a
- návod na ochranu soukromí jednotlivých osob při zpracování biometrických informací.

Tato mezinárodní norma nezahrnuje otázky obecného managementu vztahující se k fyzické

bezpečnosti, environmentální bezpečnosti a správě klíčů pro kryptografické techniky.

Konec náhledu - text dále pokračuje v placené verzi ČSN.