ČESKÁ TECHNICKÁ NORMA

ICS 35.040, 35.240.15 **Leden 2015**

Informační technologie – Bezpečnostní techniky – Autentizační kontext pro biometriku

ČSN
ISO/IEC 24761
36 9886

Information technology – Security techniques – Authentication context for biometrics

Technologies de l,information – Techniques de sécurité – Contexte d,authentification biometriques

Tato norma je českou verzí mezinárodní normy ISO/IEC 24761:2009 včetně opravy ISO/IEC 24761:2009/Cor.1:2013-03. 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 24761:2009, including its Corrigendum ISO/IEC 24761:2009/Cor.1:2013-03. 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 8824 (všechny části) | ITU-T Recommendations X.680-683 zavedena v ČSN ISO/IEC 8824 (36 9632) Informační technologie – Abstraktní syntaxe zápisu jedna (ASN. 1)

ISO/IEC 8825-4:2008 | ITU-T Recommendation X.693 zavedena v ČSN ISO/IEC 8825-4:2012 (36 9635) Informační technologie – Pravidla kódování ASN. 1: Pravidla kódování XML (XER)

ISO/IEC 9594-2 | ITU-T Recommendation X.501 nezavedena

ISO/IEC 9594-8 | ITU-T Recommendation X.509 nezavedena

ISO/IEC 19785-1:2006 zavedena v ČSN ISO/IEC 19785-1:2009 (36 9864) Informační technologie – Společný rámec formátů biometrické výměny dat – Část 1: Specifikace datového prvku

ISO/IEC 19785-3:2007 zavedena v ČSN ISO/IEC 19785-3:2010 (36 9864) Informační technologie – Společný rámec formátů biometrické výměny dat – Část 3: Specifikace formátů patrona

RFC 3852 nezavedena

RFC 5911 nezavedena

Souvisící ČSN

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

ČSN ISO/IEC 7816-8:2010 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 8: Příkazy pro bezpečnostní operace

ČSN ISO/IEC 7816-11:2005 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 11: Ověřování osob biometrickými metodami

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

ČSN ISO/IEC 19795-1:2008 (36 9861) Informační technologie – Testování a hodnocení výkonnosti biometrik – Část 1: Principy a základní struktura

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 24761
Autentizační kontext pro biometriku První vydání
2009-05-15

Obsah

Strana

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 vývoji mezinárodních norem prostřednictvím technických komisí, ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oblastech 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 JTC 1.

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.

ISO/IEC 24761 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*.

Úvod

Proces biometrické verifikace prováděný na vzdáleném místě je vystaven mnoha rizikům: zfalšovaným referenčním šablonám, padělaným původním datům, nespolehlivým biometrickým zařízením, atd. Jak může validátor zkontrolovat, zda proces biometrické verifikace provedený na vzdáleném místě je důvěryhodný? Tato mezinárodní norma poskytuje mechanismus pro vypořádání se s tímto problémem.

Obecně je spolehlivost výsledku procesu biometrické verifikace závislá jak na úrovni bezpečnosti prováděného procesu, tak na úrovni funkční výkonnosti použitých biometrických zařízení. Jsou-li použita zařízení nabízející vyšší úroveň funkční výkonnosti, výsledek bude spolehlivější. Nejsou-li zařízení bezpečná, nebo jestliže byl proces prováděn v nezabezpečeném prostředí, pak výsledek nebude spolehlivý.

V internetovém prostředí obvykle validátor procesu biometrické verifikace přímo neví, jaká biometrická zařízení byla použita, ani jaký (jaké) proces (procesy) byly provedeny na vzdáleném místě. Získáním důvěryhodných informací, jako je úroveň funkční výkonnosti použitých biometrických zařízení, úroveň bezpečnosti vzdáleného systému a také znalostí toho, že procesy v systému byly provedeny bezpečně, může validátor učinit lepší rozhodnutí o tom, do jaké míry je možné důvěřovat výsledku biometrické verifikace.

Tato mezinárodní norma poskytuje řešení výše uvedeného problému tak, že informace o použitých zařízeních a procesech provedených na vzdáleném místě jsou poslány validátorovi.

Obecně se proces biometrické registrace skládá z následujících podprocesů: zachycení dat, zpracování mezilehlých signálů, zpracování konečných signálů (nebo extrakce rysů), a uložení. (To je obecné, ale existuje mnoho možných variant.)

Obecně se proces biometrické verifikace skládá ze zachycení dat, zpracování mezilehlých signálů, zpracování konečných signálů, znovuzískání uložených informací, porovnání a rozhodnutí. (To je obecné, ale existuje mnoho možných variant.)

Obvykle jsou podprocesy vykonávány v jedné nebo více jednotkách biometrického zpracování (BPUs), z nichž každá má svoji vlastní neměnnou úroveň bezpečnosti. Několik podprocesů je zahrnuto v procesu biometrické verifikace, ale bezpečnost podprocesu znovuzískání uložených informací je také závislá na podprocesech obsažených v procesu biometrické registrace.

Tato mezinárodní norma je navržena pro použití v tomto modelu procesů biometrické verifikace, který je rozšířením modelu biometrického systému definovaného v ISO 19092, ale je také aplikovatelná na jiné modely procesů biometrické verifikace.

Tato mezinárodní norma definuje datový formát bezpečnostních dat generovaných BPUs, například senzoru, čipové karty nebo porovnávacího zařízení, k poskytnutí certifikovaných informací o BPU, a pomoci tak validátorovi určit spolehlivost výsledku procesu biometrické verifikace.

Tato mezinárodní norma je založena na technologii infrastruktury veřejných klíčů (PKI) a na PKIX (viz ISO/IEC 9594-8 | ITU-T Doporučení X.509 a RFC 3852). Tato mezinárodní norma používá digitální podpis jako základ pro důvěru a nepopiratelnost. Tato mezinárodní norma požaduje, aby vstupní a výstupní informace byly hašovány, a následně digitálně podepsány s dalšími daty, například s výzvou od validátora, a výsledkem hodnocení činností BPU.

Tato mezinárodní norma připouští, že požadavky soukromí týkající se uložení biometrických prvků musí být odezvou a musí být v souladu s místními zákony a legislativou souvisící se soukromím dat. ACBio zajistí, že validátor může validovat výsledek procesu biometrické verifikace, aniž by obdržel privátní data, například biometrický vzorek získaný od žadatele nebo biometrickou referenční šablonu použitou pro porovnání.

Instance ACBio je zpráva, která je zakódována s použitím XML Encoding Rules (XER) nebo Basic Encoding Rules (BER) ASN. 1 [viz ISO/IEC 8824 (všechny části) | ITU-T Doporučení X.680-683 a ISO/IEC 8825-4 | ITU-T Doporučení X.693], obvykle podporovaná dodavateli soustavy kryptografických nástrojů (tool kits). Syntaxe je nezávislý algoritmus a podporuje poskytnutí integrity dat a autentizace původu dat. Jsou doporučeny kryptografické algoritmy specifikované subkomisí ISO/IEC JTC 1/SC 27, i když je možné použít jakýkoliv algoritmus vhodný k použití danou komunitou.

Tato mezinárodní norma používá certifikáty BPU, vydané certifikační organizací BPU (důvěryhodnou třetí stranou, která vydává certifikáty týkající se bezpečnosti BPU) a certifikáty biometrické referenční šablony (BRT), vydané certifikační organizací BRT, která vydává certifikáty týkající se vytváření a uchovávání biometrické referenční šablony v databázi nebo na čipové kartě.

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňují, že shoda s tímto dokumentem může zahrnovat použití patentu týkajícího se instance ACBio uvedené v kapitolách 5, 6, 7 a 8.

ISO a IEC nezastávají žádné stanovisko ohledně důkazu, platnosti a rozsahu tohoto patentového práva.

Držitel tohoto patentového práva ujistil ISO a IEC, že je ochoten vyjednat licence za rozumných a ne-diskriminačních podmínek se žadateli po celém světě. V tomto směru je držitel tohoto patentového práva registrován u ISO a IEC. Informace je možné obdržet od:

Toshiba Corporation, Toshiba Solutions Corporation,

1-1, Shibaura 1-chome, Minato-ku,
Tokyo 105-8001, Japan

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.

1 Předmět normy

Tato mezinárodní norma definuje strukturu a datové prvky autentizačního kontextu pro biometriku (Authentication Context for Biometrics (ACBio)), který je použit pro kontrolu validity výsledku procesu biometrické verifikace prováděného na vzdáleném místě. Tato mezinárodní norma umožňuje jakékoliv instanci ACBio spojit se s jakoukoliv datovou položkou, která se účastní jakéhokoliv biometrického procesu souvisícího s verifikací a registrací. Specifikace ACBio je aplikovatelná nejen na jednu modální biometrickou verifikaci, ale také na multimodální kombinaci (fusion).

Tato mezinárodní norma specifikuje kryptografickou syntaxi instance ACBio. Kryptografická syntaxe instance ACBio je založena na abstraktním schématu syntaxe kryptografických zpráv (CMS), jehož konkrétní hodnoty mohou být reprezentovány pomocí buďto kompaktního binárního kódování nebo člověkem čitelného zápisu v XML.

Tato mezinárodní norma nedefinuje protokoly, které mají být používány mezi entitami, jako jsou BPUs, žadatel a validátor. Zabývá se výhradně obsahem a kódováním instancí ACBio pro různé činnosti zpracování.