ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Leden 2012**

Informační technologie – Společný rámec formátů biometrické výměny – Část 4: Specifikace formátu bezpečnostního bloku

ČSN ISO/IEC 19785- 4
36 9864

Information technology – Common Biometric Exchange Formats Framework – Part 4: Security block format specifications

Technologies de l,information – Cadre de formats d,échange biométriques communs – Partie 4: Spécifications de format de bloc de sécurité

Tato norma je českou verzí mezinárodní normy ISO/IEC 19785-4:2010. 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 19785-4:2010. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných normativních dokumentech

ISO/IEC 8824 (soubor) | ITU Rec. X. 680-683 zavedena v ČSN ISO/IEC 8824 (36 9632) Informační technologie – Abstraktní syntaxe způsobu zápisu jedna (ASN)

ISO/IEC 8825 (soubor) | ITU Rec. X.690-693 zavedena v ČSN ISO/IEC 8825 (36 9635) Informační technologie – Pravidla kódování pro ASN.1

ISO/IEC 9798-6 dosud nezavedena

ISO/IEC 19784-1 dosud nezavedena

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

ISO/IEC 24761 dosud nezavedena

RFC 3852 nezavedeno

RFC 5911 nezavedeno

Souvisící ČSN

ČSN ISO/IEC 19785-2:2009 (36 9864) Informační technologie – Společný rámec formátů biometrické výměny – Část 2: Postupy pro činnost Biometrické registrační autority

Vysvětlivky k textu převzaté normy

Anglický termín symbol se překládá českým slovem symbol, protože se zde používá ve významu nadřazeného termínu vůči podřazeným termínům značky, znaky, označení atd., aby se všechny tyto termíny nemusely vypisovat.

Message-Digest algorithm je rozšířená rodina hašovacích funkcí, která vytváří ze vstupních dat výstup (otisk) fixní délky. Otisk je též označován jako miniatura, kontrolní součet (v zásadě nesprávné označení), fingerprint, hash (česky někdy psán i jako haš). Jeho hlavní vlastností je, že malá změna na vstupu vede k velké změně na výstupu, tj. k vytvoření zásadně odlišného otisku.

Vypracování normy

Zpracovatel: INFO 7, IČ 44266154, Ing. Jaroslav Ošlejšek

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie – ISO/IEC 19785-4
Společný rámec formátů biometrické výměny – První vydání
Část 4: Specifikace formátu bezpečnostního bloku 2010-08-15

ICS 35.040

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 copyri ght@iso.org

Web www.iso.org

Published in Switzerland

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 zřízených příslušnou organizací, aby se zabývaly určitou oblastí technické činnosti. V oblastech společného zájmu technické komise ISO a IEC spolupracují. Práce se zúčastňují i jiné mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Mezinárodní normy jsou připravovány v souladu s pravidly určenými ve Směrnicích ISO/IEC části 2.

Hlavním úkolem společné technické komise je připravovat mezinárodní normy. Návrhy mezinárodních norem přijaté společnou technickou komisí se rozesílají národním členům 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 a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv.

Mezinárodní norma ISO/IEC 19785-4 byla připravena společnou technickou komisí ISO/IEC JTC 1 *Informační technologie*, subkomisí SC 37, *Biometrika.*

ISO/IEC 19785 sestává z následujících částí, pod společným názvem *Informační technologie – Společný rámec formátů biometrické výměny –*

Část 1: Specifikace datových prvků

Část 2: Postupy pro činnost Biometrické registrační autority

Část 3: Specifikace formátu patrona

Část 4: Specifikace formátu bezpečnostního bloku

Úvod

Biometrické ověření a identifikace jsou důležité techniky pro autentizaci a/nebo identifikaci

jednotlivce. Biometrická data použitá v biometrickém ověření a identifikaci musí být z důvěryhodného zdroje bez rušení v přenosu (integrita). To může, ale nemusí být nezbytné pro to, aby byla utajena (šifrována) v závislosti na bezpečnostní politice. Tato část ISO/IEC 19785 poskytuje jak integritu, tak šifrování biometrických dat.

K zajištění interoperability spojil Společný rámec formátů biometrické výměny (CBEFF) specifikovaný v ISO/IEC 19785-1 metadata s jedním nebo více bloky biometrických dat (BDBs). V ISO/IEC 19785-1 jsou definovány možnosti integrity, šifrování a pojetí bezpečnostního bloku z toho důvodu, aby byly zahrnuty bezpečnostní informace, týkající se těchto možností, ale není specifikován formát a podrobný obsah bezpečnostních bloků (formáty SB).

Dále je uvedeno několik kroků v řetězci počínaje formátem patrona CBEFF.

Zaprvé, formát patrona může určit, že abstraktní hodnota datového prvku CBEFF CBEFF_BDB_šifrování_volby je stanovena jako ŽÁDNÉ ŠIFROVÁNÍ a že datový prvek CBEFF CBEFF_BIR_integrita_volby je stanoven jako ŽÁDNÁ INTEGRITA. V tomto případě pak není potřeba, aby byl v tomto formátu patrona požadován bezpečnostní blok.

Jestliže formát patrona požaduje, aby byl v některých případech zahrnut bezpečnostní blok, může určit, že to bude jeden z bezpečnostních bloků definovaných v této části ISO/IEC 19785 (nebo jako některé jiné bezpečnostní bloky), nebo může zahrnout datové prvky CBEFF CBEFF_SB-formát_vlastníka a CBEFF_SB_formát_typ pro identifikaci jednoho z těchto nebo některý jiný formát bezpečnostního bloku.

Kromě formátů bezpečnostního bloku definovaných v této části ISO/IEC 19785, bude existovat mnoho dalších možných formátů bezpečnostního bloku CBEFF, které pokryjí různé potřeby. Například ISO/IEC 24713-3 se specifikuje formát bezpečnostního bloku pro ILO profil námořníků. Formát bezpečnostního bloku, který je specifikován v kapitole 5, je navržen tak, aby byl co možná nejobecnější. Formát bezpečnostního bloku, specifikovaný v kapitole 6, je navržen tak, aby poskytoval základní bezpečnostní ochranu a podporoval pouze integritu.

Tato část ISO/IEC 19785 specifikuje dva formáty bezpečnostních bloku.

První bezpečnostní blok specifikuje formát pro všeobecný účel bezpečnostního bloku s volitelnými prvky pro šifrování a integritu a využívá RFC 3852 Kryptografická syntaxe zprávy (CMS) s některými úpravami entit **ObalenáData, ŠifrovanáData, PodepsanáData,** a **AutentizovanáData,** aby uspokojil potřeby a požadavky pro vyjádření bezpečnosti biometrických informací ve shodě s CBEFF. Druhý blok se nazývá „formát pouze pro podpis bezpečnostního bloku“, který je definován s pomocí RFC 3852.

Formát pro všeobecný účel bezpečnostního bloku specifikovaný v této části ISO/IEC 19785 také obsahuje Autentizační kontext pro biometrické výskyty (ACBio) specifikované v ISO/IEC 24761. ACBio také využívá RFC 3852 schéma Kryptografické syntaxe zprávy. Zahrnutí výskytů ACBio umožňuje určit bezpečnostní úrovně systémů, které vytvářejí autentizovanou biometriku. Volitelné použití výskytů ACBio je důležitou částí zajištění infrastruktury telebiometrické autentizace (TAI) [3].

1 Předmět normy

Tato část ISO/IEC 19785 specifikuje formáty bezpečnostního bloku (viz ISO/IEC 19785-1) registrované ve shodě s ISO/IEC 19785-2, jako formáty definované biometrickou organizací CBEFF ISO/IEC JTC 1/SC 37 a specifikuje jejich registrované identifikátory formátu bezpečnostního bloku.

POZNÁMKA Identifikátor formátu bezpečnostního bloku je zaznamenán v normalizovaném

biometrickém záhlaví (SBH) formátu patrona (nebo je definovaný tímto formátem patrona jako jediný dostupný formát bezpečnostního bloku).

Účelem formátu pro všeobecný účel bezpečnostního bloku je specifikovat, zda biometrický datový blok (BDB) je šifrován, nebo SBH a BDB aplikují integritu (nebo obojí) a zda může obsahovat výskyt ACBio (viz ISO/IEC 24761). Tento bezpečnostní blok poskytuje všechny nezbytné bezpečnostní parametry včetně těch, které jsou použity pro šifrování nebo integritu.

Tím se neomezují algoritmy a parametry použité pro šifrování nebo integritu, ale poskytuje se záznam takových algoritmů a hodnot parametrů.

Je to důvod pro vytváření profilů ke stanovení pro určité oblasti aplikace, jaké algoritmy a rozsahy parametrů lze použít generátorem bezpečnostního bloku a tedy to, jaké algoritmy a rozsahy parametrů musí uživatel bezpečnostního bloku podpořit. To je ale mimo rozsah této části ISO/IEC 19785.

Druhý bezpečnostní blok je více omezen, ale je jednodušší (a zejména nesmí obsahovat výskyty ACBio a nepodporuje šifrování BDB).