

ČESKÁ TECHNICKÁ NORMA

ICS 03.060; 35.240.40 **Duben 2009**

Finanční služby – Biometrika – Struktura bezpečnosti

ČSN
ISO 19092
97 9123

Financial services – Biometrics – Security framework

Services financiers – Biométrie – Cadre de sécurité

Tato norma je českou verzí mezinárodní normy ISO 19092:2008. 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 19092:2008. 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 10202-3 zavedena v ČSN EN ISO 10202-3 (36 9736) Karty pro finanční transakce – Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody – Část 3: Vztahy mezi kryptografickými klíči

ISO/IEC 19790 dosud nezavedena

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. Petr Wallenfels

MEZINÁRODNÍ NORMA

Finanční služby – Biometrika – Struktura bezpečnosti ISO 19092

První vydání

2008-01

ICS 03.060

Obsah

Předmluva 6

Úvod 7

1 Předmět normy 8

2 Shoda 8

3 Citované normativní dokumenty 8

4 Termíny a definice 9

5 Symboly a zkrácené termíny 14

6 Přehled biometrické technologie 14

6.1 Všeobecně 14

6.2 Biometrika otisku prstů 15

6.3 Biometrika hlasu 15

6.4 Biometrika duhovky 16

6.5 Biometrika sítnice 16

6.6 Biometrika obličeje 16

6.7 Biometrika geometrie ruky 16

6.8 Biometrika podpisu 17

6.9 Biometrika žil 17

7 Technologické úvahy 17

7.1 Vlastnosti biometrických systémů 17

7.2 Univerzálnost 17

7.3 Individuálnost 18

7.4 Přesnost 18

7.5 Hodnocení výkonnosti 20

7.6 Interoperabilita 21

8 Základní principy biometrických architektur 21

8.1 Model biometrického systému 21

8.2 Subsystem sběru dat 21

- 8.3** Subsystem přenosu 22
- 8.4** Subsystem zpracování signálu 22
- 8.5** Subsystem srovnání 23
- 8.6** Rozhodovací subsystem 23
- 8.7** Subsystem uložení 24
- 8.8** Přenosné tokeny 24

Strana

9 Požadavky na management a bezpečnost 24

- 9.1** Základní aplikace 24
- 9.2** Stěžejní bezpečnostní požadavky 25
- 9.3** Zaregistrování 25
- 9.4** Verifikace 26
- 9.5** Identifikace 27
- 9.6** Přenos a uložení 27
- 9.7** Ukončení a archivace 28
- 9.8** Shoda a deník událostí 29

10 Bezpečnostní infrastruktura 29

- 10.1** Komponenty 29
- 10.2** Fyzické techniky 30

11 Cíle kontroly biometrické validace 30

- 11.1** Kritéria periodických revizí a auditu 30
- 11.2** Kontroly prostředí 31
- 11.3** Kontroly životního cyklu správy klíčů 41
- 11.4** Životní cyklus biometrických informací 45

Příloha A (informativní) Deník událostí 52

Příloha B (normativní) Biometrická registrace 55

Příloha C (normativní) Bezpečnostní pokyny 56

Příloha D (normativní) Bezpečnostní požadavky na biometrická zařízení 65

Příloha E (informativní) Existující aplikace 67

Bibliografie 68

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, pomocí kterých byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat.

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



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO 2008

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) tvoří celosvětovou federaci národních normalizačních orgánů (členských orgánů ISO). Práce na přípravě mezinárodních norem provádějí obvykle technické komise ISO. Každý členský orgán, který se zajímá o předmět, pro který byla komise ustavena, má právo účastnit se práce v této komisi. Práce se zúčastňují i jiné mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech elektrotechnické normalizace.

Mezinárodní normy jsou připravovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem technických komisí je připravovat mezinárodní normy. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním členům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Pozornost je nutné věnovat možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO neodpovídá za identifikaci jakéhokoli nebo všech takových patentových práv.

Mezinárodní norma ISO 19092 byla připravena technickou komisí ISO/TC 68, *Finanční služby*, subkomisí SC 2, *Management bezpečnosti a všeobecné bankovní operace*.

První vydání ISO 19092 ruší a nahrazuje ISO 19092-1:2006, jejíž menší revizi představuje; zejména byly odstraněny odkazy na projekt 19092-2.

Úvod

Tato mezinárodní norma nahrazuje ISO 19092-1:2006. Když byla mezinárodní norma ISO 19092-1:2006 publikována, očekávalo se, že bude následovat publikace druhé části ISO 19092 (ISO 19092-2, *Finanční služby – Biometrika – Část 2: Syntaxe zpráv a kryptografické požadavky*). ISO 19092-2 však vlivem nedostatku konsenzu nebyla dokončena. ISO 19092-1:2006 byla aktualizována do této mezinárodní normy s odstraněním všech odkazů na ISO 19092-2 a s provedením určitých menších redakčních úprav.

Se zavedením počítačových technologií se změnila obchodní a podnikatelská praxe. Nahrazení papírových transakcí elektronickými transakcemi snížilo náklady a zvýšilo efektivnost. V systémově významných platebních systémech a dalších finančních systémech jsou denně přenášeny biliony dolarů v peněžních prostředcích a cenných papírech prostřednictvím telefonů, telefonních služeb a dalších mechanismů elektronické komunikace. Vysoká hodnota nebo čistý objem takových transakcí v otevřeném prostředí vystavuje finanční komunitu a její zákazníky potenciálně vážným rizikům náhodné nebo úmyslné změny, nahrazení nebo zničení dat. Vzájemně propojené sítě a rostoucí počet a sofistikovanost zlomyslných protivníků vytvářejí toto riziko.

Nevyhnutelný nástup elektronických komunikací napříč nekontrolovanými veřejnými sítěmi, například Internetem, představuje také pro finanční odvětví rostoucí riziko. Nezbytnost expandování obchodních činností do těchto prostředí zvýšila požadavek na silnou autentizaci a vytvořila potřebu jiných druhů autentizace. Finanční komunita na tyto potřeby reaguje.

Biometrika, prvek identity „něco co jste nebo co jste schopný dělat“, se stala uznávaným prostředkem, a zahrnuje takové technologie, jako obraz prstu, identifikace hlasu, snímání očí a obraz obličeje. Cena biometrické technologie klesá zatímco spolehlivost roste, což obojí je nyní pro finanční odvětví akceptovatelné a realizovatelné.

Mezinárodní norma popisuje adekvátní kontroly a vhodné postupy při použití biometriky jako mechanismu autentizace pro bezpečný vzdálený elektronický přístup nebo lokální řízení fyzického přístupu ve finančním odvětví.

Biometrika může být použita pro autentizaci lidského faktoru pro fyzický a logický přístup. Logický přístup může zahrnovat přístup k aplikacím, službám nebo oprávněním. Tato mezinárodní norma podporuje integraci biometriky do finančního odvětví a management biometrických informací jako části celkového programu pro management informační bezpečnosti organizace. Stanovuje biometrickou technologii jako nástroj k posílení infrastruktury veřejných klíčů (PKI) pro vyšší autentizaci poskytnutím silnějších metod jakož i multifaktorové autentizace. Tato mezinárodní norma navíc umožňuje neustálé opětovné ujištění, že entita chystající se generovat digitální podpis, je ve skutečnosti osoba s autorizovaným přístupem k privátnímu klíči.

Úspěch biometrického systému u veřejnosti je založen na několika faktorech, a tyto faktory se liší v rámci dostupných biometrických technologií:

- vyhovující podmínky a snadnost použití;
- úroveň zřejmé bezpečnosti;
- výkonnost;
- neinvazivnost.

Systémy autentizace diskutované v této mezinárodní normě jsou určeny pro uzavřenou skupinu uživatelů, ve které členové skupiny odsouhlasili používání biometrické identifikace nebo sami identifikaci provádějí. Takovéto dohody mohou být explicitní (například servisní dohoda) nebo implicitní (například nasazení zařízení ukazující jasný záměr provést transakci). Systémy využitelné k monitorování neurčitěho počtu lidí nejsou předmětem této mezinárodní normy.

Techniky specifikované v této mezinárodní normě jsou vytvořeny k udržování integrity a důvěrnosti biometrických informací a k poskytnutí autentizace. Tato mezinárodní norma však nezaručuje, že konkrétní implementace bude bezpečná. Je odpovědností finanční instituce zavést do praxe celkový způsob zpracování s nezbytnými kontrolami, aby se zajistilo, že celý proces je bezpečně implementován. Kontroly by dále měly obsahovat aplikaci náležitých auditních testů s cílem ověřit shodu s touto mezinárodní normou.

1 Předmět normy

Tato mezinárodní norma popisuje strukturu bezpečnosti při používání biometrie pro autentizaci jednotlivců ve finančních službách. Zavádí typy biometrických technologií a řeší problémy týkající se jejich aplikací. Tato mezinárodní norma také popisuje architektury pro implementaci, specifikuje minimální bezpečnostní požadavky pro efektivní management a poskytuje kontrolní cíle a doporučení vhodné pro použití odbornými pracovníky.

Předmětem této mezinárodní normy je:

- využívání biometrie pro autentizaci zaměstnanců a osob požadujících finanční služby;
- ověření uplatňované identity;
- identifikaci jednotlivce;
- validace věrohodných údajů, například jména uživatele a hesla (credentials), předložených při registraci s cílem podpořit autentizaci požadovanou při řízení rizika;
- management biometrických informací v průběhu celého jejich životního cyklu, obsahujícího procesy registrace, přenosu a uchování, ověření, identifikace a ukončení;
- bezpečnost biometrických informací v průběhu celého jejich životního cyklu, zahrnujícího integritu dat, autentizaci původu a důvěrnost;
- aplikace biometrie na řízení logického a fyzického přístupu;
- dohled zajišťující ochranu finanční instituce a jejích zákazníků;
- bezpečnost fyzického hardwaru používaného během životního cyklu biometrických informací.

Předmětem této mezinárodní normy nejsou:

- práva na soukromí jednotlivých osob a vlastnictví biometrických informací;
- specifické techniky pro sběr dat, zpracování signálů a shoda biometrických dat a proces rozhodování o biometrické shodě;
- použití biometrické technologie při použití neautentizačních aplikací jako je například rozpoznávání řeči, uživatelská interakce a řízení anonymního přístupu.

Tato mezinárodní norma poskytuje závazné prostředky, pomocí kterých mohou být biometrické informace zašifrovány k zajištění důvěrnosti dat nebo pro jiné účely.

Ačkoliv se tato mezinárodní norma nezabývá specifickými požadavky a omezeními obchodních aplikací využívajících biometrickou technologii, mohou být tato témata řešena v jiných normách.

Konec náhledu - text dále pokračuje v placené verzi ČSN.