

# ČESKÁ TECHNICKÁ NORMA

ICS 35.040, 35.240.15 **Červen 2014**

**ČSN**  
**ISO/IEC 19795-7**  
36 9861

## **Informační technologie - Testování a podávání zpráv o biometrické výkonnosti - Část 7: Testování algoritmů biometrického porovnávání na kartě**

Information technology – Biometric performance testing and reporting –  
Part 7: Testing of on-card biometric comparison algorithms

Technologies de l'information – Essais et rapports de performance biométriques –  
Partie 7: Essais des algorithmes de comparaison biométrique sur carte

Tato norma je českou verzí mezinárodní normy ISO/IEC 19795-7:2011. 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 19795-7:2011. 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 7816-4:2005 zavedena v ČSN ISO/IEC 7816-4:2006 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 4: Organizace, bezpečnost a příkazy pro výměnu

ISO/IEC 7816-6:2004 zavedena v ČSN ISO/IEC 7816-6:2005 (36 9734) Identifikační karty – Karty s integrovanými obvody – Část 6: Mezioborové datové prvky pro výměnu

ISO/IEC 7816-11:2004 zavedena v ČSN ISO/IEC 7816-11:2005 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 11: Ověřování osob biometrickými metodami

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

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

ISO/IEC 19795-2:2007 zavedena v ČSN ISO/IEC 19795-2:2009 (36 9861) Informační technologie – Biometrické testování a hodnocení výkonnosti – Část 2: Metodologie testování pro hodnocení technologie a scénáře

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42 Výměna dat

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

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 členské 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 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 fotokopíí 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](mailto:copyright@iso.org)

Web [www.iso.org](http://www.iso.org)

Published in Switzerland

**MEZINÁRODNÍ NORMA**

Informační technologie – Testování a podávání zpráv ISO/IEC 19795-7

o biometrické výkonnosti – První vydání

Část 7: Testování algoritmů biometrického porovnávání na kartě 2011-01-15

Obsah

Strana

Předmluva 8

Úvod 9

**1** Předmět normy 10

**2** Shoda 10

**3** Citované dokumenty 10

**4** Termíny a definice 11

**5** Zkratky 11

**6** Požadavky na plánování testů 11

**6.1** Základní koncept testu 11

**6.2** Specifikace hardwarového a softwarového rozhraní 12

**6.3** Specifikace formátů dat 12

**6.3.1** Formát dat pro porovnávání 12

**6.3.2** Formát pro obrazy a šablony mimo kartu 12

**6.4** Profilování BIT 12

**6.5** Kombinace subsystému kartového porovnávání 13

**6.6** Fázované (postupně prováděné) testování 13

**6.7** Volby účasti 13

**6.8** Metriky 13

**6.9** Výsledky porovnávání 14

**7** Požadavky na provedení testů 14

**7.1** Obecně 14

**7.2** Podmínky pro demonstrování ekvivalence algoritmů na kartě a mimo kartu 14

**7.3** Zpracování BIT 14

**7.4** Měření rychlosti provedení 14

**7.4.1** Veličiny určené k měření 14

**7.4.2** Metody pro měření doby trvání 15

**7.4.3** Metody pro měření neurčitosti 15

**8** Specifikace rozhraní biometrického porovnávání na kartě 15

**8.1** Přehled 15

- 8.2** Přístup k použití ISO/IEC 7816 15
- 8.3** Ustavení komunikací 15
- 8.4** Výběr testovací aplikace 15
- 8.5** Uložení registrační šablony na kartě 16
- 8.6** Čtení šablony BIT 17
- 8.7** Použití BIT 17

Strana

- 8.8** Ověření 19
  - 8.8.1** Specifikace APDU 19
  - 8.8.2** Zamknutí karty 19
  - 8.8.3** Zamknutí algoritmu založeného na PC 20
  - 8.8.4** Skóre porovnání 20
  - 8.8.5** Zákaz chování se zapamatováním stavu 20
- 8.9** Čtení identifikátoru karty 20
- 8.10** Čtení identifikátoru subsystému porovnávání 21

## **Příloha A** (informativní) Konverze záznamu podle ISO/IEC 19794-2 na šablony kompaktní velikosti 22

- A.1** Obecný úvod 22
  - A.1.1** Účel 22
  - A.1.2** Přehled 22
  - A.1.3** Formát záznamu 22
  - A.1.4** Formát kompaktní velikosti 23
- A.2** Jedinečnost markantu 25
- A.3** Přítomnost šablon BIT na kartě 25
- A.4** Použití BITs 25
- A.5** Počet markantů 25
  - A.5.1** Omezení počtu 25
  - A.5.2** Účinek BIT 26
  - A.5.3** Mechanismus osekání 26

**A.5.4** Střed pro osekání 27

**A.6** Třídící řazení markantů 27

**A.6.1** Podpora řazení 27

**A.6.2** Třídění modulo pro velké obrazy 27

**Příloha B** (informativní) Normalizované kódy polohy prstu 28

**Příloha C** (informativní) Vzorový materiál při plánování plánu testu 29

**C.1** Účel 29

**C.2** Specifikace API založená na PC 29

**C.2.1** Testovací rozhraní 29

**C.2.2** Profil a shoda formátu dat 29

**C.2.3** Předložení 29

**C.2.4** Testovací rozhraní 29

**C.2.5** Chování doby zpracování (výpočtu) 30

**Příloha D** (informativní) API pro vytváření a přiřazování šablony markantu otisku prstů 32

**D.1** Extrakce markantů 32

**D.2** Přiřazování markantů 33

**D.3** Identifikátory implementace 34

Bibliografie 35

Obrázky

Obrázek A.1 – Konverze INCITS 378 dat na data ISO/IEC 19794-2 25

Strana

Tabulky

Tabulka 1 – Třídy účasti 13

Tabulka 2 – Příkaz APDU pro výběr aplikace porovnávání na kartě 16

Tabulka 3 – Příklad ID aplikace 16

Tabulka 4 – Odezva APDU od výběru aplikace porovnání 16

Tabulka 5 – Příkaz APDU pro uložení referenční šablony 16

Tabulka 6 – Odezva APDU od uložení referenční šablony 16

Tabulka 7 – Příkaz APDU pro získání biometrické informační šablony	17
Tabulka 8 – Odezva APDU od získání biometrické informační šablony	17
Tabulka 9 – Biometrická informační šablona založená na ISO/IEC 19785-3 a ISO/IEC 19794-2 (PŘÍKLAD)	18
Tabulka 10 – Příkaz APDU pro porovnání biometrických šablon	19
Tabulka 11 – Odezva APDU z porovnání biometrických šablon	19
Tabulka 12 – Příkaz APDU pro získání skóre ověřovacího porovnání	20
Tabulka 13 – Odezva APDU pro získání skóre ověřovacího porovnání	20
Tabulka 14 – Příkaz APDU pro získání identifikátoru karty	21
Tabulka 15 – Odezva APDU pro získání identifikátoru karty	21
Tabulka 16 – Příkaz APDU pro získání identifikátoru subsystému porovnání	21
Tabulka 17 – Odezva APDU pro získání identifikátoru subsystému porovnávání	21
Tabulka 0AA.1 – Profil záznamu podle normy ISO/IEC 19794-2:2005	23
Tabulka 0AA.2 – Profil karty podle normy ISO/IEC 19794-2:2005	23
Tabulka 0AA.3 – DO šablon markantů podle ISO/IEC 19794-2	23
Tabulka 0AA.4 – DO zonální kvality podle ISO/IEC 19794-2	23
Tabulka 0AA.5 – Data zonální kvality podle ISO/IEC 19794-2	23
Tabulka 0BB.1 – Kódy polohy prstu podle ISO/IEC 19794-2 a ISO/IEC 19785-3	28
Tabulka 0DD.1 – API funkce create_template	32
Tabulka 0DD.2 – API funkce match_templates	33
Tabulka 0DD.3 – API funkce get_pids	34

## 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 JTC1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnici 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 19795-7 vypracovala společná technická komise ISO/IEC JTC1 *Informační technologie*, subkomise SC 37 *Biometrika*.

ISO/IEC 19795 se skládá z následujících částí se společným názvem *Informační technologie – Testování a podávání zpráv o biometrické výkonnosti*.

- Část 1: *Principy a rámec*
- Část 2: *Metodologie testování pro hodnocení technologie a scénáře*
- Část 3: *Testování specifické podle modalit [Technická zpráva]*
- Část 4: *Testování výkonnosti interoperability*
- Část 5: *Scénář řízení přístupu a klasifikační schéma*
- Část 7: *Testování algoritmů biometrického porovnávání na kartě*

Následující část se připravuje:

- Část 6: *Metodologie testování hodnocení provozuschopnosti*

## Úvod

Biometrické rozpoznávací algoritmy byly portovány do karet s integrovanými obvody podle ISO/IEC 7816, aby se realizovaly přínosy zvýšení soukromí, uplatňované u paradigmatu biometrického porovnávání na kartě.

Zatímco nejběžnější komerční realizací této schopnosti je porovnávání šablon markantů otisku prstů na kartě, bylo také implementováno porovnávání dat z jiných modalit. Příslušné normy pro karty byly ve skutečnosti

explicitně navrženy pro podporu libovolných biometrických modalit. Další informace o aspektech specifických pro modalitu jsou uvedeny v ISO/IEC 19795-3. V každém případě, zatímco výpočetní schopnost takových karet se v posledních letech zvýšila, zůstává otázkou, zda je nutné vzdát se přesnosti ověřování ve prospěch rychlosti nebo velikosti dat nebo obou. Pro šablony otisku prstů vedl cíl zvýšit efektivnost k vývoji ISO/IEC 19794-2:2005 formátů karet kompaktní velikosti specificky pro biometrické porovnávání na kartě.

Tato část ISO/IEC 19795 specifikuje mechanismus pro měření přesnosti i rychlosti ISO/IEC 7816 ICC zpracovávající data z libovolných modalit. Zahrnuje příklady pro datové struktury a příkazy potřebné pro shodu konformních šablon markantů ISO/IEC 19794-2:2005 na kartách.

## 1 Předmět normy

Tato část ISO/IEC 19795 stanoví mechanismus pro měření základních algoritmických schopností algoritmů biometrického porovnávání provozovaných na kartách s integrovanými obvody podle ISO/IEC 7816. Konkrétně tato část ISO/IEC 19795

- konkretizuje mechanismus pro testování biometrického porovnávání na kartách;
- normalizuje postupy pro měření přesnosti implementací biometrického porovnávání na kartách provozovaných na objektech založených vzorcích karet, specifických pro test;
- normalizuje postupy pro měření trvání různých operací; a

- podává příklady pro shodu se šablonami markantů kompaktních karet ISO/IEC 19794-2:2005.

Následující oblasti nejsou předmětem této části ISO/IEC 19795:

- postupy pro zabezpečení komunikačních kanálů, včetně kryptografické ochrany biometrických šablon;
  - postupy pro ochranu integrity vzorků nebo šablon pomocí digitálních podpisů;
  - autentizace karty a čtecího zařízení;
  - výběr nebo použití přenosových protokolů (například bezkontaktních);
- 
- profily specifických norem pro výměnu dat;
  - postupy pro hodnocení čtecích zařízení, včetně výkonu, shody a interoperability;
  - postupy pro hodnocení odolnosti nebo trvanlivosti karty;
  - generování šablony na kartě (například extrakce markantů z obrazů),
  - aktualizace nebo úprava šablony;
  - formální testy shody podle ISO/IEC 7816-4 a ISO/IEC 7816-11;
  - testování zařízení neodpovídajících ISO/IEC 7816, včetně všech zařízení pro systémy na kartě.

Konec náhledu - text dále pokračuje v placené verzi ČSN.