

2019

Identifikační karty – Karty s integrovanými obvody –
Část 11: Ověřování osob biometrickými metodami

ČSN
ISO/IEC 7816-11

36 9205

Identification cards – Integrated circuit cards –
Part 11: Personal verification through biometric methods

Cartes d'identification – Cartes à circuit intégré –
Partie 11: Vérification personnelle par méthodes biométriques

Tato norma je českou verzí mezinárodní normy ISO/IEC 7816-11:2017. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 7816-11:2017. It was translated by the Czech Agency for Standardization. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 2382-37:2017 zavedena v ČSN ISO/IEC 2382-37:2018 (36 9001) Informační technologie – Slovník – Část 37: Biometrika

ISO/IEC 7816-4:2013 zavedena v ČSN ISO/IEC 7816-4:2015 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 4: Organizace, bezpečnost a příkazy pro výměnu

Související ČSN

ČSN ISO/IEC 10536 (soubor) (36 9741) Identifikační karty – Bezkontaktní karty s integrovanými obvody

ČSN ISO/IEC 14443-1 (36 9760) Karty a bezpečnostní zařízení pro osobní identifikaci – Bezkontaktní objekty s vazbou na blízko – Část 1: Fyzikální charakteristiky

ČSN ISO/IEC 14443-3 (36 9760) Karty a bezpečnostní zařízení pro osobní identifikaci – Bezkontaktní objekty s vazbou na blízko – Část 3: Inicializace a antikolize

ČSN ISO/IEC 14443-4 (36 9760) Karty a bezpečnostní zařízení pro osobní identifikaci – Bezkontaktní objekty s vazbou na blízko – Část 4: Protokol přenosu

ČSN ISO/IEC 15693-1 (36 9762) Karty a bezpečnostní zařízení pro osobní identifikaci – Bezkontaktní objekty s vazbou na dálku – Část 1: Fyzikální charakteristiky

ČSN ISO/IEC 24761 (36 9886) Informační technologie – Bezpečnostní techniky – Autentizační kontext pro biometriku

ČSN EN ISO 3166-1 (97 1002) Kódy pro názvy zemí a jejich částí – Část 1: Kódy zemí

ČSN ISO/IEC 7812-1 (36 9732) Identifikační karty – Identifikace vydavatelů karet – Část 1: Systém číslování

ČSN ISO/IEC 7816-1 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 1: Karty s kontakty – Fyzikální charakteristiky

ČSN ISO/IEC 7816-2 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 2: Karty s kontakty – Rozměry a umístění kontaktů

ČSN ISO/IEC 7816-3 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 3: Karty s kontakty – Elektrické rozhraní a protokoly přenosu

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

ČSN ISO/IEC 7816-5 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 5: Registrace poskytovatelů aplikací

ČSN ISO/IEC 7816-7 (36 9205) Identifikační karty – Karty s integrovanými obvody s kontakty – Část 7: Mezioborové příkazy pro strukturovaný kartový dotazovací jazyk (SCQL)

ČSN ISO/IEC 7816-10 (36 9205) Identifikační karty – Karty s integrovanými obvody s kontakty – Část 10: Elektronické signály a odpověď na reset pro synchronní karty

ČSN ISO/IEC 7816-12 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 12: Karty s kontakty – Elektrické rozhraní USB a provozní procedury

ČSN ISO/IEC 7816-13 (36 9205) Identifikační karty – Karty s integrovanými obvody – Část 13: Příkazy pro správu aplikací v multiaplikačním prostředí

Vysvětlivky k textu převzaté normy

V překladu se ponechávají zkratky např. „DO“. Pokud zkratka vyjadřuje plurál (DOs), překládá se jako „objekty DO“ resp. „datové objekty“ atp.

Slova psaná velkými písmeny/kapitálkami, případně více slov psaných dohromady, patří do příslušného softwaru a nepřekládají se.

anglický termín

algorithm reference

biometric based

biometric data

obvyklé překlady

- odkaz na algoritmus
- reference algoritmu
- biometrický
- založený na biometrice
- biometrická data
- biometrické údaje

biometric feature	· biometrický rys · biometrická charakteristika
biometric information template	· skupinová šablona pro šablony biometrických informací
group template	
biometric payload	· biometrická přenášená data · biometrická přenášená data, za která se platí
biometric probe	· biometrický dotaz · biometrická sonda
biometric reference	· biometrická reference · biometrický odkaz
CBEFF patron formats	· formáty CBEFF dle patrona
challenge template	· šablona výzvy
enable/disable	· povolit/zakázat
Enrollment	· registrace (biometrického typu) · zařazení (biometrického typu)
off-card verification	· verifikace mimo kartu
operation	· operace · činnost
patron	· patron · schválená registrační organizace
pattern	· vzor · obrazec
proprietary	· proprietární · podle uvážení majitele
timeout	· ukončení při překročení časového limitu · ukončení (neúplného úkolu) po časovém limitu
var.	· var. · variable/proměnná
verification	· ověřovací: určený k ověřování, např. biometrický ověřovací systém · ověřovaný: subjekt porovnávání s biometrickými referencemi · ověření: potvrzení biometrického tvrzení · ověřování: proces (opakovaného) porovnávání s biometrickými referencemi

Upozornění na národní poznámky

Do normy byly k Předmluvě, ke kapitole 4, k tabulce 8 a k tabulce C.1 doplněny vysvětlující národní poznámky.

Vypracování normy

Zpracovatel: Anna Juráková, Praha, IČO 61278386, Dr. Karel Jurák

Technická normalizační komise: TNK 42 Výměna dat

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

ICS 35.240.15

Obsah

Strana

Předmluva.....	7
Úvod.....	8
1..... Předmět normy.....	9
2..... Citované dokumenty.....	9
3..... Termíny a definice.....	9
4..... Značky a zkrácené termíny.....	11
5..... Příkazy pro biometrické ověření a příslušné procesy.....	12
5.1..... Obecně.....	12
5.2..... Příkazy pro proces statického biometrického ověření.....	12
5.3..... Příkazy pro proces dynamického biometrického ověření.....	13
5.4..... Příkaz proved' biometrickou operaci.....	13
5.4.1... Obecná definice příkazu PBO.....	13

5.4.2... Operace příkazu

PBO.....
..... 14

5.4.3... Registrace biometrické

reference.....
16

5.4.4... Vybavení biometrické

reference.....
16

5.4.5... Porovnání biometrického

dotazu..... 16

5.4.6... Zpětnovazební mechanismus v průběhu procesu biometrické

akvizice..... 17

6..... Příkazy pro specifické případy biometrického ověření a příslušné

procesy..... 17

6.1.....

Obecně.....
..... 17

6.2..... Případ použití pro

ISO/IEC 24761.....
.... 17

6.2.1... Operace příkazu

PBO.....
..... 17

6.2.2... Registrace biometrické

reference.....
17

6.2.3... Vybavení biometrické

reference.....
18

6.2.4... Porovnání biometrického

dotazu..... 18

7..... Datové

prvky.....
..... 19

7.1..... Biometrické

informace.....
..... 19

7.2..... Biometrická

data.....	21
7.3..... Ověřovací informace.....	22
7.3.1... Účel.....	22
7.3.2... Datový objekt ověřovací informace (VIDO).....	23
7.3.3... Šablona ověřovacích informací (VIT).....	24
Příloha A (informativní) Proces biometrického ověření.....	25
Příloha B (informativní) Příklady datových objektů biometrických informací.....	28
Příloha C (informativní) Seznam tagů objektů biometrických dat v šabloně biometrických informací.....	30
Bibliografie.....	31



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2017, Publikováno ve Švýcarsku

Veškerá práva vyhrazena. Žádná část této publikace nesmí být, není-li specifikováno jinak nebo nepožaduje-li se to v souvislosti s její implementací, reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopíí nebo zveřejňování na internetu nebo intranetu, bez předchozího písemného souhlasu. O souhlas lze požádat buď ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

ISO copyright office

Ch. de Blandonnet 8 · CP 401

CH-1214 Vernier, Geneva, Switzerland

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

copyright@iso.org

www.iso.org

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 svých 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 JTC 1.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnících ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnících ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamena schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL: www.iso.org/iso/foreword.html.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 17 *Karty a osobní identifikace*. [NP1](#)

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 7816-11:2004), které bylo technicky zrevidováno. Hlavní změnou je doplnění specifikace příkazu PERFORM BIOMETRIC OPERATION, který umožňuje ICC pružně používat různé biometrické operace.

Seznam všech částí souboru ISO/IEC 7816 lze nalézt na webových stránkách ISO.

Úvod

ISO/IEC 7816 je souborem mezinárodních norem, který specifikuje karty s integrovanými obvody a použití těchto karet pro výměnu. Tyto karty jsou identifikačními kartami určenými pro výměnu informací vyjednávaných mezi vnějším světem a integrovaným obvodem na kartě. Jako výsledek výměny informací dodá karta informaci (výsledek výpočtu, uložená data) a/nebo karta modifikuje svůj obsah (uchování dat, zaznamenání událostí).

Pět částí souboru ISO/IEC 7816 je specifických pro karty s galvanickými kontakty a tři z nich specifikují elektrické rozhraní.

- ISO/IEC 7816-1 specifikuje fyzikální charakteristiky karet s kontakty.
- ISO/IEC 7816-2 specifikuje rozměry a umístění kontaktů.
- ISO/IEC 7816-3 specifikuje elektrické rozhraní a protokoly přenosu pro asynchronní karty.
- ISO/IEC 7816-10 specifikuje elektrické rozhraní a odpověď na reset pro synchronní karty.
- ISO/IEC 7816-12 specifikuje elektrické rozhraní a pracovní procedury pro karty USB.

Všechny další části souboru ISO/IEC 7816 jsou nezávislé na fyzikální technologii rozhraní. Platí pro karty s přístupem pomocí kontaktů a/nebo radiofrekvenčně.

- ISO/IEC 7816-4 specifikuje organizaci, bezpečnost a příkazy pro výměnu.
- ISO/IEC 7816-5 specifikuje registraci poskytovatelů aplikací.
- ISO/IEC 7816-6 specifikuje mezioborové datové prvky pro výměnu.
- ISO/IEC 7816-7 specifikuje příkazy strukturovaného kartového dotazovacího jazyka.
- ISO/IEC 7816-8 specifikuje příkazy pro bezpečnostní operace.
- ISO/IEC 7816-9 specifikuje příkazy pro správu karet.
- ISO/IEC 7816-11 specifikuje biometrické metody ověřování osob.
- ISO/IEC 7816-13 specifikuje příkazy pro správu životního cyklu aplikací.
- ISO/IEC 7816-15 specifikuje aplikaci kryptografických informací.

Soubor ISO/IEC 10536 specifikuje přístup pomocí těsné vazby. Soubor ISO/IEC 14443 a soubor ISO/IEC 15693 specifikují radiofrekvenční přístup. Takové karty se nazývají bezkontaktní karty.

Mezinárodní organizace pro standardizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) zdůrazňují fakt, že shoda s tímto dokumentem může zahrnovat použití patentů, které se vztahují na instanci Autentizačního kontextu biometriky (ACBio) specifikované v ISO/IEC 24761, podrobnosti v 6.2.

ISO a IEC nezaujímá stanovisko k prokázání, platnosti ani předmětu těchto patentových práv.

Držitelé těchto patentových práv ujistili ISO a IEC, že si přejí za přiměřených a nediskriminačních

podmínek vyjednat licence se žadateli v celém světě. Příslušná prohlášení držitelů těchto patentových práv jsou registrována u ISO a IEC. Podrobnosti lze získat od:

Toshiba Corporation, Toshiba Solutions Corporation, 1-1, Shibaura 1-chome, Minato-ku, Tokyo 105-8001, Japan.

1 Předmět normy

Tento dokument specifikuje mezioborové příkazy vztahující se na bezpečnost při ověřování osob biometrickými metodami na kartách s integrovanými obvody. Dokument rovněž definuje datové struktury a metody přístupu k datům při používání karet jako nosičů biometrické reference a/nebo jako zařízení pro ověření biometrického dotazu držitele karty (biometrické porovnání na kartě). Identifikace osob používající biometrické metody je mimo předmět tohoto dokumentu.

Konec náhledu - text dále pokračuje v placené verzi ČSN.

[NP1\)](#) NÁRODNÍ POZNÁMKA V přejímané normě není uveden úplný název subkomise SC 17. Subkomise SC 17 má název *Karty a bezpečnostní zařízení pro osobní identifikaci*.