ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Květen 2015**

Identifikační karty – Karty s integrovanými obvody – Část 4: Organizace, bezpečnost a příkazy pro výměnu

ČSN
ISO/IEC 7816-4
36 9205

Identification cards – Integrated circuit cards –
Part 4: Organization, security and commands for interchange

Cartes d,identification – Cartes a circuit intégré –
Partie 4: Organisation, sécurité et commandes pour les échanges

Tato norma je českou verzí mezinárodní normy ISO/IEC 7816-4:2013 včetně opravy ISO/IEC 7816-4:2013/Cor.1:2014-08. 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 7816-4:2013 including its Corrigendum ISO/IEC 7816-4:2013/Cor.1:2014-08. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 7816-4 (36 9205) z ledna 2006.

Národní předmluva

Změny proti předchozí normě

Toto vydání zrušuje a nahrazuje druhé vydání této normy, které bylo technicky revidováno. Implementace založené na druhém vydání budou vyhovovat také třetímu vydání této normy.

Informace o citovaných dokumentech

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

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

ISO/IEC 8825-1:2002 nezavedena

Souvisící ČSN

ČSN EN 14890-1:2010 (36 9710) Aplikační rozhraní pro čipové karty používané jako zařízení pro vytváření bezpečného podpisu – Část 1: Základní služby

ČSN EN 14890-2:2010 (36 9710) Aplikační rozhraní pro čipové karty používané jako zařízení pro vytváření bezpečného podpisu – Část 2: Další služby

ČSN ISO/IEC 7810:2004 (36 9725) Identifikační karty – Fyzikální charakteristiky

ČSN ISO/IEC 7816 (všechny části) (36 9205) Identifikační karty – Karty s integrovanými obvody

ČSN ISO/IEC 9796 (všechny části) (36 9780) Informační technologie – Bezpečnostní techniky – Schémata
digitálního podpisu umožňující obnovu zprávy

ČSN ISO/IEC 9797 (všechny části) (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro
autentizaci zprávy (MACs)

ČSN ISO/IEC 9798 (všechny části) (36 9743) Informační technologie – Bezpečnostní techniky – Autentizace entit

ČSN ISO/IEC 10118 (všechny části) (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce

ČSN ISO/IEC 10536 (všechny části) (36 9741) Identifikační karty – Bezkontaktní karty s integrovanými obvody – Karty s těsnou vazbou

ČSN ISO/IEC 14443 (všechny části) (36 9760) Identifikační karty – Bezkontaktní karty s integrovanými obvody – Karty s vazbou na blízko

ČSN ISO/IEC 15693-1 (36 9762) Identifikační karty – Bezkontaktní karty s integrovanými obvody – Karty s vazbou na dálku – Část 1: Fyzikální charakteristiky

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. Pokud jde o vazbu typu „the value of the DO“ překládá se jako „hodnota objektu DO“.

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

Anglický termín/vazba	**Obvyklé překlady**
• below • see text below	• níže • viz text níže
• byte set to	• bajt nastaven na • bajt s hodnotou
• a.k.a. • also known as	• neboli • také známý jako
• discretionary data	• volitelná data • data podle uvážení

• comparison data	• porovnávací data • data pro porovnání
• concatenation	• zřetězení (datových objektů) • spojení
• DataString • data string	• DataString (vyhrazený termín) • datový řetězec
• default	• standardní
• enabling/disabling (channel/interface))	• odblokováno/zablokováno
• ephemeral (public key)	• jednorázový (veřejný klíč)
• expanded format	• rozšířený formát • expandovaný formát
• extended header list	• seznam rozšířených záhlaví
• external world	• vnější svět • externí svět
• feature on the card • general feature management template	• charakteristika (zajímavost) na kartě • šablona správy obecných charakteristik
• flag	• návěští
• file management data, FMD	• data pro správu souboru • data pro management souboru
• child (of the file)	• podřazený (soubor) • dítě
• independent tag allocation schemes	• schémata přidělování nezávislých příznaků
• indicate	• indikuje • vyznačuje
• management	• správa (dat, klíčů, souborů) • (lineární/cyklické) uspořádání (DO) • management (životního cyklu)
• master key	• hlavní klíč • master klíč
• to match • skipped match	• odpovídat si/být ve shodě • přeskočená shoda
• mode	• režim • mód
• nonce	• nonce (nepřekládá se) • (číslo generované pro specifické použití, např. autentizace relace)
• offset	• ofset • posunutí
• parent (file)	• nadřazený (soubor) • rodičovský (soubor)
• payload	• přenášená data • (data za jejichž přenos se platí)
• parsing	• analýza • rozbor
• Primary Account Number, PAN	• základní číslo účtu

(dokončení)

Anglický termín/vazba	**Obvyklé překlady**
• procedure	• procedura • postup
• proprietary • proprietary rights	• proprietární • vlastnická práva
• public modulus	• veřejný modul • veřejný modul operace modulo
• quartet	• čtyřbitový bajt • čtveřice

• record life cycle	• životní cyklus záznamu • životní cyklus (přidělený) záznamu
• reference data	• referenční data (pro porovnání s něčím) • data odkazu (na soubor atp.)
• referenced by	• citovaný (pomocí) • na který se odkazuje (čím)
• resolution (of wrappers)	• rozlišení (obálek)
• resolve	• rozlišit (položku v seznamu)
• response	• odezva • odpověď
• response trailer	• konec odezvy
• retrieval	• vyhledání • načtení • vybavení
• root	• kořen • kořenový uzel
• self-controlled DO	• DO se samokontrolou
• sole tag	• vlastní příznak
• sub-template	• dílčí šablona • sub-šablona
• sub-tree	• podstrom • substrom
• synergy	• součinnost • synergie
• tag allocation authority	• autorita pro přidělování příznaků • orgán pro přídělování příznaků
• time stamp	• vyznačení času • časové razítko
• verification data	• verifikační data • (data určenáná pro porovnání s referenčními daty)
• witness-challenge-response (triples)	• (trojice) svědectví-výzva-odezva
• wrapper	• obálka • obal

Upozornění na národní poznámky

Do normy byly v kapitole 3 a v 9.3.3.3 doplněny národní poznámky.

Do normy byly doplněny národní poznámky, upozorňující na zapracované opravy podle ISO/IEC 7816-4:2013/
Cor.1:2014-08.

Vypracování změny normy

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

Technická normalizační komise: TNK 42 Výměna dat

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

MEZINÁRODNÍ NORMA

Identifikační karty – Karty s integrovanými obvody – ISO/IEC 7816-4
Část 4: Organizace, bezpečnost a příkazy pro výměnu Třetí vydání
2013-04
ICS 35.240.15

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 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. V oblastech společného zájmu technické komise ISO a IEC spolupracují. Práce se zúčastňují také další vládní a 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 vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté společnou technickou komisí se rozesílají národním členům 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 7816-4 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 17 *Karty a identifikace osob*.

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 7816-4:2005) a zapracovává změnu ISO/IEC 7816-4:2005/Amd.1:2008.

ISO/IEC 7816 sestává z následujících částí, pod společným názvem *Identifikační karty – Karty s integrovanými obvody:*

- *Část 1: Karty s kontakty – Fyzikální charakteristiky*
- *Část 2: Karty s kontakty – Rozměry a umístění kontaktů*
- *Část 3: Karty s kontakty – Elektrické rozhraní a protokoly přenosu*
- *Část 4: Organizace, bezpečnost a příkazy pro výměnu*
- *Část 5: Registrace poskytovatelů aplikací*
- *Část 6: Mezioborové datové prvky pro výměnu*
- *Část 7: Mezioborové příkazy pro strukturovaný kartový dotazovací jazyk (SCQL)*
- *Část 8: Příkazy pro bezpečnostní operace*
- *Část 9: Příkazy pro správu karet*
- *Část 10: Elektronické signály a odpověď na reset pro synchronní karty*
- *Část 11: Ověřování osob biometrickými metodami*
- *Část 12: Karty s kontakty – Elektrické rozhraní USB a provozní procedury*
- *Část 13: Příkazy pro správu aplikací v multiaplikačním prostředí*
- *Část 15: Aplikace kryptografické informace*

Úvod

ISO/IEC 7816[6] je řadou norem, která specifikuje karty s integrovanými obvody a použití těchto karet pro výměnu. Tyto karty jsou identifikačními kartami určenými pro dohodnutou výměnu informací mezi vnějším světem a integrovaným obvodem karty. Jako výsledek výměny informací dodá karta informaci (výsledek výpočtu, uložená data) a/nebo karta modifikuje obsah (uchovávaných dat, zaznamenaných událostí).

- Pět částí je specifických pro karty s galvanickými kontakty a tři z nich specifikují elektrická rozhraní.
- ISO/IEC 7816-1 specifikuje fyzikální charakteristiky pro karty 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 provozní procedury pro karty USB.
- Všechny další části 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 používání životního cyklu aplikací.
- ISO/IEC 7816-15 specifikuje aplikaci kryptografických informací.

ISO/IEC 10536[15] specifikuje přístup pomocí těsné vazby. ISO/IEC 14443[18] a ISO/IEC 15693[20] specifikuje radiofrekvenční přístup. Takové karty se nazývají bezkontaktní karty.

ISO a IEC upozorňují na skutečnost, že bylo nárokováno, že shoda s tímto dokumentem může zahrnovat použití následujících patentů a patentů dalších smluvních stran.

- JPN 2033906, Přenosné elektronické zařízení
- JPN 2557838, Karta s integrovanými obvody
- JPN 2537199, Karta s integrovanými obvody
- JPN 2856393, Přenosné elektronické zařízení
- JPN 2137026, Přenosné elektronické zařízení
- JPN 2831660, Přenosné elektronické zařízení
- DE 198 55 596, Přenosný nosič dat s mikroprocesorem, který může být použit s kontakty nebo bez nich

ISO a IEC neodpovídají za průkaznost, platnost a předmět těchto patentových oprávnění.

Držitelé těchto patentových práv ujistili ISO a IEC, že si přejí vyjednat licence za rozumných a nediskriminačních termínů a podmínek pro aplikace v celém světě. V tomto smyslu jsou prohlášení držitelů těchto patentových oprávnění registrována u ISO a IEC. Informace lze získat následovně:

Kontakt	**Podrobnosti patentů**

Toshiba Corporation Intellectual Property Division 1-1, Shibaura 1-Chome Minato-ku, Tokyo 105-8001, Japan	JPN 2033906 (priority date: 1986-02-18; publication date: 1996-03-19), FRA 8614996, KOR 44664 JPN 2557838 (priority date: 1986-02-18; publication date: 1996-09-05), FRA 8700343, GER 3700504, KOR 42243, USA 4841131 JPN 2537199 (priority date: 1986-06-20; publication date: 1996-07-08), FRA 8708646, FRA 8717770, USA 4833595, USA 4901276 JPN 2856393 (priority date: 1987-02-17; publication date: 1998-11-27), FRA 8801887, KOR 43929, USA 4847803 JPN 2137026 (priority date: 1987-02-20; publication date: 1998-06-26), JPN 3054119, FRA 8802046, KOR 44393, USA 4891506 JPN 2831660 (priority date: 1988-08-26; publication date: 1998-09-25), FRA 8911249, KOR 106290, USA 4988855
Orga Kartensysteme Gmbh Am Hoppenhof 33 D-33104 Paderborn Germany	DE 198 55 596 (priority date: 1998-12-02; publication date: 2000-06-29) Applications pending in Europe, Russia, Japan, China, USA, Brazil, Australia

1 Předmět normy

O této části ISO/IEC 7816 se předpokládá, že se bude používat v libovolných oblastech činnosti. Tato část specifikuje:

- obsahy dvojic příkaz-odezva vyměňovaných na rozhraní;
- prostředky pro načtení datových prvků a datových objektů z karty;
- struktury a obsah historických bajtů pro popis provozních charakteristik karty;
- struktury pro aplikace a data na kartě, z pohledu na rozhraní, při provádění příkazů;
- metody přístupu k souborům a datům na kartě;
- bezpečnostní architekturu, která definuje přístupová práva k souborům a datům na kartě;
- prostředky a mechanizmy pro identifikování a adresování aplikací na kartě;
- metody pro bezpečné předávání zpráv;
- metody přístupu k algoritmům zpracovávaným kartou. Tyto algoritmy zde nejsou popisovány.

Tato část nepokrývá interní implementaci na kartě nebo ve vnějším světě.

Tato část ISO/IEC 7816 nezávisí na fyzikální technologii rozhraní. Platí pro karty s přístupem pomocí jedné nebo více z následujících metod: kontakty, těsná vazba a radiofrekvence. Pokud karta podporuje simultánní použití více než jednoho fyzického rozhraní, pak vztahy mezi tím, co se stane na různých fyzických rozhraních, je mimo předmět tohoto vydání ISO/IEC 7816-4.