ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Leden 2006**

Identifikační karty - Karty s integrovanými obvody - Část 4: Organizace, bezpečnost a příkazy pro výměnu	ČSN ISO/IEC 78164 36 9205

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

Cartes d'identification - Cartes à circuit intégré -
Partie 4: Organisation, sécurité et commandes pour les échanges

Identifikationskarten - Chipkarten -
Teil 4: Regeln, Sicherheitsfunktionen und Befehle für den Datenaustausch

Tato norma je českou verzí mezinárodní normy ISO/IEC 7816-4:2005. Mezinárodní norma ISO/IEC 7816-4:2005 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 7816-4:2005. The International Standard ISO/IEC 7816-4:2005 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN ISO/IEC 7816-4 (36 9205) z prosince 1997.

Národní předmluva

Změny proti předchozí normě

Text druhého vydání doplňuje první vydání ISO/IEC 7816-4:1995 a zapracovává některé články z ISO/IEC 7816-5:1994, ISO/IEC 7816-6:1996, ISO/IEC 7816-8:1999 a ISO/IEC 7816-9:2000. Rovněž zapracovává změnu ISO/IEC 7816-4:1995/Amd.1:1997.

Dále byla přesunuta část textu z prvního vydání ISO/IEC 7816-4 do třetího vydání ISO/IEC 7816-3 tak, že protokoly přenosu T=0 a T=1 jsou nyní uvedeny pouze v ISO/IEC 7816-3 a již nikoli v ISO/IEC 7816-4.

Informace o citovaných normativních dokumentech

ISO/IEC 7816-3 zavedena v ČSN ISO/IEC 7816-3 (36 9205) Informační technologie - Identifikační karty - Karty s integrovanými obvody s kontakty - Část 3: Elektronické signály 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 dosud nezavedena

Vysvětlivky k textu převzaté normy

Anglický termín	**Obvyklé termíny**	**Použitý termín**
discretionary data	· volitelná data · data podle uvážení	volitelná data
master key	· hlavní klíč · master klíč	hlavní klíč
mode	· režim · mód	režim
offset	· ofset · posunutí	ofset
public modulus	· veřejný modul · veřejný modul operace modulo	veřejný modul
qualification	· bližší určení · kvalifikace	bližší určení
qualifier	· kvalifikátor · bližší určovatel	kvalifikátor
quartet	· čtyřbitový byte · čtveřice	čtyřbitový byte
response	· odezva · odpověď	odezva
verification data	· ověřovací data · data vytvořená pro porovnání s referenčními daty	ověřovací data
witness	· svědectví · svědek	svědectví
wrapper	· obálka · obal	obálka
time stamp	· časové razítko · vyznačení času	časové razítko

Upozornění na národní poznámky

Do normy byly k Předmluvě a k článku 8.1.1.2.3 doplněny informativní národní poznámky.

Vypracování normy

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

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Martin Kratoška

MEZINÁRODNÍ NORMA

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

ISO/IEC 7816-4

Druhé vydání

2005-01-15

ICS 35.240.15

ã

Obsah

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 v části 2 Směrnic ISO/IEC.

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.

ISO/IEC 7816-4 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Identifikační karty*, subkomisí SC 17, *Karty a identifikace osob*.

Toto druhé vydání ruší a nahrazuje první vydání (ISO/IEC 7816-4:1995) a zapracovává materiál extrahovaný z ISO/IEC 7816-5:1994, ISO/IEC 7816-6:1996, ISO/IEC 7816-8:1999 a ISO/IEC 7816-9:2000. Rovněž zapracovává změnu ISO/IEC 7816-4:1995/Amd.1:1997.

Dále byl vybrán materiál z prvního vydání ISO/IEC 7816-4 a přesunut do třetího vydání ISO/IEC 7816-3 tak, že protokoly přenosu T=0 a T=1 jsou nyní uvedeny pouze v ISO/IEC 7816-3 a již nikoli v ISO/IEC 7816-4.

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

– *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: Karty s kontakty: Elektronické signály a odpověď na reset pro synchronní karty*

– *Část 11: Ověřování osob biometrickými metodami*

– *Část 12: Karty s kontakty: Elektrické rozhraní USB a pracovní postupy*

– *Část 15: Aplikace kryptografické informace*

A) NÁRODNÍ POZNÁMKA Starší název celého soubor norem ISO/IEC 7816 byl: „*Identifikační karty – Karty s integrovanými obvody a s kontakty*“ a platil pouze pro karty s kontakty.

Úvod

ISO/IEC 7816 je souborem norem, který specifikuje karty s integrovanými obvody a použití těchto karet pro mezinárodní výměnu. Tyto karty jsou identifikačními kartami určenými pro dohodnutou výměnu informací mezi externím světem a integrovaným obvodem karty. Jako výsledek výměny informací dodá karta informaci (výsledek výpočtu, uložená data) a/nebo karta modifikuje svůj obsah (uchovávání dat v paměti resp. zaznamenání události v paměti).

– Pět částí je specifických pro karty s galvanickými kontakty, tři z nich specifikují elektrická 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 postupy pro USB karty.

– Všechny další části jsou nezávislé na fyzikální technologii rozhraní. Platí pro karty s přístupem pomocí kontaktů a/nebo s radiofrekvenčním přístupem.

- 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 7816-15 specifikuje aplikaci kryptografické informace.

ISO/IEC 10536[13] specifikuje přístup pomocí těsné vazby. ISO/IEC 14443[15] a ISO/IEC 15693[17] specifikuje radiofrekvenční přístup. Takové karty se nazývají bezkontaktní karty.

ISO a IEC upozorňují na skutečnost, že shoda s tímto dokumentem může zahrnovat využívání následujících patentů a práv 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 vyjednávat 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 (datum priority: 1986-02-18; datum zveřejnění: 1996-03-19), FRA 8614996, KOR 44664 JPN 2557838 (datum priority: 1986-02-18; datum zveřejnění: 1996-09-05), FRA 8700343, GER 3700504, KOR 42243, USA 4841131 JPN 2537199 (datum priority: 1986-06-20; datum zveřejnění: 1996-07-08), FRA 8708646, FRA 8717770, USA 4833595, USA 4901276 JPN 2856393 (datum priority: 1987-02-17; datum zveřejnění: 1998-11-27), FRA 8801887, KOR 43929, USA 4847803 JPN 2137026 (datum priority: 1987-02-20; datum zveřejnění: 1998-06-26), JPN 3054119, FRA 8802046, KOR 44393, USA 4891506 JPN 2831660 (datum priority: 1988-08-26; datum zveřejnění: 1998-09-25), FRA 8911249, KOR 106290, USA 4988855

Orga Kartensysteme GmbH Am Hoppenhof 33 D-33104 Paderborn Germany	DE 198 55 596 (datum priority: 1998-12-02; datum zveřejnění: 2000-06-29) O použití dosud nebylo rozhodnuto v Evropě, Rusku, Japonsku, Číně, USA, Brazilii, Australii

---

1 Předmět normy

Tato část ISO/IEC 7816 specifikuje

– obsahy dvojic příkaz-odezva vyměňovaných na rozhraní;

– prostředky pro přečtení datových prvků a datových objektů z karty;

– struktury a obsahy historických bytů 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 bezpečnou výměnu zpráv;

– metody přístupu k algoritmům zpracovávaným kartou. Tyto algoritmy zde nejsou popisovány.

Tato část nepokrývá interní implementaci na kartě nebo v externím světě.

Tato část ISO/IEC 7816 nezávisí na fyzikální technologii rozhraní. Platí pro karty s přístupem pomocí jedné nebo více z následujících metod: pomocí kontaktů, těsné vazby a radiofrekvence.

-- Vynechaný text --