

2005

Identifikační karty - Karty s integrovanými obvody - Část 9: Příkazy pro správu karet	ČSN ISO/IEC 7816-9 36 9205
--	--------------------------------------

Identification cards - Integrated circuit(s) cards -
Part 9: Commands for card management

Cartes d'identification - Cartes à circuit intégré -
Partie 9: Commandes pour la gestion des cartes

Identifikationskarten - Chipkarten -
Teil 9: Kommandos für das Kartenmanagement

Tato norma je českou verzí mezinárodní normy ISO/IEC 7816-9:2004. Mezinárodní norma ISO/IEC 7816-9:2004 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 7816-9:2004. The International Standard ISO/IEC 7816-9:2004 has the status of a Czech Standard.

	© Český normalizační institut, 2005 72230 Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.
---	--

Předmět části 9 (vydání 2004) se zúžil na životní cyklus karty a na příkazy pro správu karet. Další příkazy z prvního vydání části 9 byly přesunuty do druhého vydání části 4. Podrobnosti jsou uvedeny v předmluvě na straně 4.

Od roku 2004 se změnila koncepce řady ISO/IEC 7816 takto: předměty částí 4, 5, 6, 8 a 9 byly navzájem posunuty tak, že po dokončení reorganizace (vydáním částí 4 a 5 v roce 2005) budou platit pouze nová vydání (2004 resp. 2005).

Citované normy

ISO/IEC 7816-4:- vydání připravované 2003-2004 dosud nezavedeno

ISO/IEC 7816 (všechny části) zavedeny v ČSN ISO/IEC 7816 (36 9205) Identifikační karty - Karty s integrovanými obvody s kontrakty

ISO/IEC 10536 (všechny části) zavedeny v ČSN ISO/IEC 10536 (36 9760) Identifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s těsnou vazbou

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

ISO/IEC 15693 (všechny části) zavedeny v ČSN ISO/IEC 15693 (36 9741) Identifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s vazbou na dálku

POZNÁMKA Soubor ISO/IEC 7816 platil do roku 2003 pouze pro karty s integrovanými obvody s kontakty. Předmět se postupně rozšiřuje rovněž na bezkontaktní karty, což se projevuje ve změně názvů jednotlivých částí.

Vysvětlivky k textu převzaté normy

Anglický termín, zkratka	Český termín (vazba)
Acces mode, AM	režim přístupu; přístupový mód
AM byte 1	byte 1 režimu AM
Application identifier, AID	identifikátor aplikace
Control reference data object, CRDO	datový objekt řídicích odkazů
Control reference template, CRT	šablona řídicích odkazů
Control reference template for - authentication, AT - digital signature, DST - cryptographic checksum, CCT	šablona řídicích odkazů pro - autentizaci - digitální podpis - kryptografický kontrolní součet
CRT usage qualifier DO	- DO šablony CRT kvalifikátoru použití - DO šablony řídicích odkazů kvalifikátoru použití
- L_c field - Length field for coding number N_c	- pole L _c - pole délky pro kódování počtu N _c
- L_e field - Length field for coding number N_e	- pole L _e - pole délky pro kódování počtu N _e
MANAGE SECURITY ENVIRONMENT command; MSE command	příkaz PŘEVEDETE SPRÁVU BEZPEČNOSTNÍHO PROSTŘEDÍ
Number of bytes in the command data field, N_c	počet bytů v datovém poli příkazu, N _c
Radio frequency	- radiofrekvenčně - vysokofrekvenčně
Security condition, SC	bezpečnostní podmínky
SC byte 1	byte 1 podmínek SC

Security environment identifier, SEID	identifikátor bezpečnostního prostředí
Usage qualifier data object (indicates the security action)	datový objekt kvalifikátoru použití (indikuje bezpečnostní akci)

Vypracování normy

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

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Radek Dvořák

Strana 3

MEZINÁRODNÍ NORMA

Identifikační karty -

Karty s integrovanými obvody s kontakty -

Část 9: Příkazy pro správu karet

ISO/IEC 7816-9

Druhé vydání

2004-06-01

ICS 35.240.15

Obsah

Strana

Předmluva

.....
..... 4

Úvod

.....
..... 5

1 Předmět
normy

.....
.. 5

2 Normativní
odkazy

..... 5

3 Termíny a
definice

..... 6

4 Zkratky a
notace

.....

. 6	
5	®ivotní
cyklus	
..... 6	
5.1	®ivotní cyklus
souboru	
..... 6	
6	Příkazy pro správu
karet..... 7	
6.1	Příkaz CREATE
FILE..... 7	
6.2	Příkaz DELETE
FILE..... 8	
6.3	Příkaz DEACTIVATE
FILE..... 8	
6.4	Příkaz ACTIVATE
FILE..... 9	
6.5	Příkaz TERMINATE
DF..... 9	
6.6	Příkaz TERMINATE
EF..... 10	
6.7	Příkaz TERMINATE CARD
USAGE..... 10	
Příloha A (informativní) Příklady bezpečnostních atributů použitých pro	
nahrávání..... 11	
Bibliografie	
..... 14	

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 Směrnicemi ISO/IEC, část 2.

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.

Je nutné upozornit na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových oprávnění. ISO a IEC neodpovídají za identifikování libovolných nebo všech takových patentových oprávnění.

ISO/IEC 7816-9 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, subkomisí SC 17, *Karty a identifikace osob*.

Toto druhé vydání společně s druhým vydáním ISO/IEC 7816-4, ISO/IEC 7816-5, ISO/IEC 7816-6 a ISO/IEC 7816-8, po důkladné reorganizaci těchto pěti částí, ruší a nahrazuje ISO/IEC 7816-4:1995, ISO/IEC 7816-5:1994, ISO/IEC 7816-6:1996, ISO/IEC 7816-8:1999 a ISO/IEC 7816-9:2000. Druhá vydání rovněž zahrnují změny ISO/IEC 7816-4:1995/Amd.1:1997, ISO/IEC 7816-5:1994/Amd.1:1996 a ISO/IEC 7816-6:1996/Amd.1:2000 a technickou opravu ISO/IEC 7816-6:1996/Cor.1:1998.

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: *Karty s kontakty - Elektronické signály a odpověď na reset pro synchronní karty*
- Část 11: *Ověřování osob biometrickými metodami*
- Část 15: *Aplikace kryptografické informace*

Úvod

ISO/IEC 7816 je řadou mezinárodních norem, která specifikuje karty s integrovanými obvody a použití těchto karet pro mezinárodní výměnu. Tyto karty jsou identifikačními kartami určenými pro výměnu informací vyjednávaných mezi vnějším 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. poznamenání dat do paměti).

- Pět částí 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 USB karty.
- 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 7816-15 specifikuje aplikaci kryptografické informace.

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

1 Předmět normy

Tento dokument specifikuje mezioborové příkazy pro správu karet a souborů. Tyto příkazy pokrývají celý životní cyklus karty a tedy některé příkazy mohou být použity dříve, než karta byla vydána držiteli karty nebo potom, když byla ukončena platnost karty.

Dokument nepokrývá vnitřní implementaci v rámci karty a/nebo ve vnějším světě.

-- Vynechaný text --