

2003

	Identifikační karty - Karty s integrovanými obvody s kontakty - Část 9: Doplnkové mezioborové příkazy a atributy zabezpečení	ČSN ISO/IEC 7816-9 36 9205
--	--	----------------------------------

Identification cards - Integrated circuit(s) cards with contacts -
Part 9: Additional interindustry commands and security attributes

Cartes d'identification - Cartes à circuit(s) intégré(s) à contacts -
Partie 9: Commandes intersectorielles additionnelles et attributs de sécurité

Identifikationskarten - Chipkarten mit Kontakten -
Teil 9: Zusätzliche interindustrielle Kommandos und Sicherheitsattribute

Tato norma je českou verzí mezinárodní normy ISO/IEC 7816-9:2000. Mezinárodní norma ISO/IEC 7816-9:2000 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 7816-9:2000. The International Standard ISO/IEC 7816-9:2000 has the status of a Czech Standard.

© Český normalizační institut,
2003

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.

66329

Citované normy

ISO/IEC 7816-4:1995 zavedena v ČSN ISO/IEC 7816-4:1997 (36 9205) Informační technologie - Identifikační karty - Karty s integrovanými obvody s kontakty - Část 4: Mezioborové příkazy pro výměnu (idt EN ISO/IEC 7816-4:1996, idt ISO/IEC 7816-4:1995)

ISO/IEC 7816-7:1999 dosud nezavedena

ISO/IEC 7816-8:1999 dosud nezavedena

ISO/IEC TR 9577:1996 dosud nezavedena

Vysvětlivky k textu převzaté normy

Anglický termín	obvyklé termíny	použitý termín
applets	<ul style="list-style-type: none">· applety· programy v jazyku Java	applety
CRT usage qualifier DO	<ul style="list-style-type: none">· datový objekt kvalifikátoru používání šablony řídicích odkazů· DO kvalifikátoru používání CRT	DO kvalifikátoru používání CRT
secure messaging, SM	<ul style="list-style-type: none">· zabezpečené zpracování zpráv· zabezpečená výměna zpráv· zabezpečené sdělování dat	zabezpečené zpracování zpráv
SE template DO	<ul style="list-style-type: none">· datový objekt šablony zabezpečeného prostředí· DO šablony SE	DO šablony SE
security	<ul style="list-style-type: none">· zabezpečení· bezpečnost	zabezpečení
SM response	<ul style="list-style-type: none">· odezva zabezpečená prostředky zabezpečeného zpracování zpráv· SM odezva	SM odezva

Vypracování normy

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

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Natálie Mišeková

1	Předmět normy 7	
2	Normativní odkazy 7	
3	Termíny a definice 7	
4	Značky (a zkratky) 8	
5	Řídicí parametry souboru 9	
6	Status životního cyklu 10	
6.1	Vymezení a účel 10	
6.2	Zásady používání 10	
6.3	Pravidla životního cyklu 10	
6.4	Zakódování celočíselného LCS..... 11	
7	Atributy zabezpečení - obecné zásady.....	11
7.1	Vymezení a účel 11	

7.2	Zásady používání	11
7.3	Zabezpečená prostředí používaná pro řízení přístupu	12
7.4	Autorizace přístupu kódovaná v certifikátech	12
8	Atributy zabezpečení - mechanismy a kódování	12
8.1	Kódování	12
8.2	Odkazy	12
8.2.1	Odkazy v FCI	12
8.2.2	Odkazy v SCQL	13
8.2.3	Odkazy na datové objekty	13
8.3	Atributy zabezpečení různých režimů rozhraní	13
8.4	Kompaktní formát	13
8.4.1	Úvod	13
8.4.2	Podmínky používání	13
8.4.3	Byte režimu přístupu	

.....	13
8.4.4 Byte podmínek zabezpečení
	15
8.5 Rozšířený formát
 16
8.5.1 Úvod
 16
8.5.2 Datový objekt režimu přístupu (AM_DO).....	16
8.5.3 Datové objekty podmínek zabezpečení (SC_DO).....	17
8.5.4 Odkazy na pravidla přístupu
	17

9 Příkazy
 18
9.1 Vymezení a rozsah platnosti
	18
9.2 Příkaz CREATE FILE
 19
9.2.1 Vymezení a rozsah platnosti
	19
9.2.2 Podmíněné používání a zabezpečení	

.....	19
9.2.3 Zpráva příkazu 19	
9.2.4 Zpráva odezvy 19	
9.2.5 Stavové podmínky 19	
9.3 Příkaz DELETE FILE 20	
9.3.1 Vymezení a rozsah platnosti 20	
9.3.2 Podmíněné používání a zabezpečení 20	
9.3.3 Zpráva příkazu 20	
9.3.4 Zpráva odezvy 20	
9.3.5 Stavové podmínky 20	
9.4 Příkaz DEACTIVATE FILE 21	
9.4.1 Vymezení a rozsah platnosti	

.....	21
9.4.2 Podmíněné používání a zabezpečení 21
9.4.3 Zpráva příkazu 21
9.4.4 Zpráva odezvy 21
9.4.5 Stavové podmínky 21
9.5 Příkaz ACTIVATE FILE 22
9.5.1 Vymezení a rozsah platnosti 22
9.5.2 Podmíněné používání a zabezpečení 22
9.5.3 Zpráva příkazu 22
9.5.4 Zpráva odezvy 22
9.5.5 Stavové podmínky 22
9.6 Příkaz TERMINATE DF	

.....	23
9.6.1 Vymezení a rozsah platnosti
.....	23
9.6.2 Podmíněné používání a zabezpečení 23
9.6.3 Zpráva příkazu
.....	23
9.6.4 Zpráva odezvy
.....	23
9.6.5 Stavové podmínky
.....	23
9.7 Příkaz TERMINATE EF
.....	23
9.7.1 Vymezení a rozsah platnosti
.....	23
9.7.2 Podmíněné používání a zabezpečení 24
9.7.3 Zpráva příkazu
.....	24
9.7.4 Zpráva odezvy
.....	24
9.7.5 Stavové podmínky

.....	24
9.8 Příkaz TERMINATE CARD USAGE.....	24
9.8.1 Vymezení a rozsah platnosti	24
9.8.2 Podmíněné používání a zabezpečení	24
9.8.3 Zpráva příkazu	25

9.8.4 Zpráva odezvy	25
9.8.5 Stavové podmínky	25
9.9 Příkaz SEARCH BINARY	25
9.9.1 Vymezení a rozsah platnosti	25
9.9.2 Podmíněné používání a zabezpečení	25
9.9.3 Zpráva příkazu	

.....	25
9.9.4 Zpráva odezvy 26
9.9.5 Stavové podmínky 26
9.10 Příkaz SEARCH RECORD 26
9.10.1 Vymezení a rozsah platnosti 26
9.10.2 Podmíněné používání a zabezpečení 26
9.10.3 Zpráva příkazu 27
9.10.4 Zpráva odezvy 28
9.10.5 Stavové podmínky 28
10 Příkazy mající původ v kartě 28
10.1 Vymezení 28
10.2 Spouštění	

kartou	
.....	
.....	29
10.3 Vybavení zprávy a	
odpověď	
.....	
29	
10.4 Formáty zprávy a	
odpovědi	
.....	
. 29	
10.5 Podmínky	
používání	
.....	
.....	29
Příloha A (normativní) Stavby životního cyklu	
souboru.....	30
A.1	
Příkazy	
.....	
.....	30
Příloha B (informativní) Příklady používání atributů zabezpečení pro zavádění	
dat.....	31
B.1	
Úvod	
.....	
.....	31
B.2	
Předpoklady	
.....	
.....	31
B.3 Zabezpečené	
zavádění	
.....	
.....	31
B.4 Kompaktní formát kódování atributů zabezpečení souboru EF	
1.....	32
B.5 Rozšířený formát kódování atributů zabezpečení souboru EF	
1.....	33
B.6 Kódování příslušných zabezpečených prostředí	
(SE).....	33

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.

Mezinárodní normy jsou připravovány v souladu s pravidly určenými Směrnicemi ISO/IEC, část 3.

V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1. 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 této části ISO/IEC 7816 mohou být předmětem patentových oprávnění. ISO a IEC neodpovídají za identifikování libovolných nebo všech takových patentových oprávnění.

Mezinárodní norma ISO/IEC 7816-9 byla připravena společnou technickou komisí ISO/IEC JTC 1 *Informační technologie*, subkomisí SC 17, *Identifikační karty a příslušná zařízení*.

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

- *Část 1: Fyzikální charakteristiky*
- *Část 2: Rozměry a umístění kontaktů*
- *Část 3: Elektronické signály a protokoly přenosu*
- *Část 4: Mezioborové příkazy pro výměnu*
- *Část 5: Systém číslování a registrační postup identifikátorů aplikací*
- *Část 6: Mezioborové datové prvky*
- *Část 7: Mezioborové příkazy strukturovaného kartového dotazovacího jazyka (SCQL)*
- *Část 8: Mezioborové příkazy pro zabezpečení*
- *Část 9: Doplnkové mezioborové příkazy a atributy zabezpečení*
- *Část 10: Elektronické signály a odpověď na reset pro synchronní karty*

Příloha A této části ISO/IEC 7816 je normativní. Příloha B je pouze informativní.

1 Předmět normy

Tato část ISO/IEC 7816 specifikuje:

- popis a kódování životního cyklu karet a příslušných objektů;
- popis a kódování atributů zabezpečení příslušných objektů karty;
- funkce a syntax doplňkových mezioborových příkazů;
- datové prvky asociované s těmito příkazy;
- mechanismus inicializace zpráv, které mají původ v kartě.

Tato část ISO/IEC 7816 se nezabývá interní implementací v kartě a/nebo ve vnějším světě.

-- Vynechaný text --