

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

Související 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

- below
- see text below
- byte set to
- a.k.a.
- also known as
- discretionary data

Obvyklé překlady

- níže
- viz text níže
- bajt nastaven na
- bajt s hodnotou
- neboli
- také známý jako
- volitelná data
- data podle uvážení

- comparison data
- concatenation
- DataString
- data string
- default
- enabling/disabling (channel/interface)
- ephemeral (public key)
- expanded format
- extended header list
- external world
- feature on the card
- general feature management template
- flag
- file management data, FMD
- child (of the file)
- independent tag allocation schemes
- indicate
- management
- master key
- to match
- skipped match
- mode
- nonce
- offset
- parent (file)
- payload
- parsing
- Primary Account Number, PAN

- porovnávací data
- data pro porovnání
- zřetězení (datových objektů)
- spojení
- DataString (vyhrazený termín)
- datový řetězec
- standardní
- odblokováno/zablokováno
- jednorázový (veřejný klíč)
- rozšířený formát
- expandovaný formát
- seznam rozšířených záhlaví
- vnější svět
- externí svět
- charakteristika (zajímavost) na kartě
- šablona správy obecných charakteristik
- návštěví
- data pro správu souboru
- data pro management souboru
- podřazený (soubor)
- dítě
- schémata přidělování nezávislých příznaků
- indikuje
- vyznačuje
- správa (dat, klíčů, souborů)
- (lineární/cyklické) uspořádání (DO)
- management (životního cyklu)
- hlavní klíč
- master klíč
- odpovídat si/být ve shodě
- přeskočená shoda
- režim
- mód
- nonce (nepřekládá se)
- (číslo generované pro specifické použití, např. autentizace relace)
- ofset
- posunutí
- nadřazený (soubor)
- rodičovský (soubor)
- přenášená data
- (data za jejichž přenos se platí)
- analýza
- rozbor
- základní číslo účtu

(dokončení)

Anglický termín/vazba

- procedure
- proprietary
- proprietary rights
- public modulus
- quartet

Obvyklé překlady

- procedura
- postup
- proprietární
- vlastnická práva
- veřejný modul
- veřejný modul operace modulo
- čtyřbitový bajt
- čtveřice

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

Předmluva	12
Úvod	13
1 Předmět normy	15
2 Citované dokumenty	15
3 Termíny a definice	15
4 Značky a zkratky termínů	20
5 Dvojice příkaz-odezva	22
5.1 Podmínky činnosti	22
5.2 Syntaxe	22
5.3 Procedury řetězení	23
5.3.1 Obecně	23
5.3.2 Fragmentace přenášených dat	23
5.3.3 Řetězení příkazů	23
5.3.4 Řetězení odezev	24
5.4 Bajt třídy	25
5.4.1 Kódování	25
5.4.2 Logické kanály	26
5.5 Bajt instrukce	26
5.6 Bajty statusu	27
6 Datové objekty	31
6.1 Datové objekty SIMPLE-TLV	31
6.2 Datové objekty BER-TLV	31
6.3 Konstruované a primitivní datové objekty	31
7 Struktury aplikací a dat	32
7.1 Dostupné struktury	32
7.2 Oblast validity	33

7.2.1	Definice a atributy	33
7.2.2	Základní pravidla pro správu VA a její používání	33
7.3	Výběr struktury	34
7.3.1	Metody výběru struktury	34
7.3.2	Datový prvek a DO odkazu na soubor	35
7.3.3	Datový prvek a DO obecného odkazu	35
7.3.4	Metody odkazování se na data v elementárních souborech	35
7.4	Řídící informace souboru a dat	36
7.4.1	Načtení řídicí informace souboru	36
7.4.2	Načtení řídicí informace dat	37
7.4.3	Řídící parametry	37
7.4.4	Krátký identifikátor souboru EF	38
7.4.5	Bajt deskriptoru souboru	38
7.4.6	Indikátor profilu	39
7.4.7	Bajt deskriptoru dat	39
7.4.8	Datové prvky seznamu DF a EF	40
7.4.9	Datový prvek čísla instance	40
7.4.10	Status životního cyklu	40
7.4.11	Nepřímé odkazování pomocí krátkého identifikátoru EF použitím DO'A2'	41
7.4.12	Šablona bezpečnostních atributů závislá na rozhraní a statusu životního cyklu	41
8	Specifické použití objektů DO a související pojmy	42
8.1	Přenášená data ber-tlv a doplňování	42
8.1.1	Podmínky doplňování	42
8.1.2	Procedura doplňování	43
8.2	Generace aktuální šablony a datového objektu	43
8.2.1	Aktuální šablona a aktuální DO	43
8.2.2	Rozšíření šablony	43

8.2.3	Podstrom datového objektu	43
8.2.4	Životní cyklus datového objektu	44
8.3	Identifikace datových prvků a datových objektů	44
8.3.1	Zásady	44
8.3.2	Interpretace příznaku v datových polích příkazu a odezvy nebo v přenášených datech	44
8.3.3	Přidělování příznaků	44
8.3.4	Schéma přidělování standardních příznaků	45
8.3.5	Schéma přidělování kompatibilních příznaků	45
8.3.6	Schéma přidělování koexistenčních příznaků	45
8.3.7	Zabránění nezávislým schématům přidělování příznaků	45
8.4	Citování a načtení objektů DO a datových prvků	46
8.4.1	Obecně	46
8.4.2	Seznam prvků	46
8.4.3	Seznam příznaků	46
8.4.4	Seznam záhlaví	46
8.4.5	Rozšířené záhlaví a seznam rozšířených záhlaví	47
8.4.6	Rozlišení rozšířeného záhlaví	47
8.4.7	Rozlišení v seznamu rozšířených záhlaví	48
8.4.8	Obálka	48
8.4.9	Obálka s příznakem	49
9	Bezpečnostní architektura	49
9.1	Obecně	49
9.2	Šablona identifikátorů kryptografických mechanismů	50
9.3	Bezpečnostní atributy	51
9.3.1	Cíle bezpečnostních atributů	51
9.3.2	Kompaktní formát	51
9.3.3	Rozšířený formát	55

- 9.3.4** Odkazy na pravidla přístupu 58
- 9.3.5** Bezpečnostní atributy pro datové objekty 59
- 9.3.6** Šablona bezpečnostních parametrů 59
- 9.3.7** Bezpečnostní atributy pro logické kanály 64
- 9.4** Datové prvky podpory bezpečnosti 64
- 10** Bezpečné předávání zpráv 66
 - 10.1** Pole SM a datové objekty SM 66
 - 10.1.1** Ochrana SM přenášených dat příkazu 66
 - 10.1.2** Ochrana SM zřetěžených příkazů a odezev 66
 - 10.1.3** Datové objekty SM (SM DO) 66
 - 10.2** Základní datové objekty SM 67
 - 10.2.1** Datové objekty SM pro zapouzdření nezašifrovaných hodnot 67
 - 10.2.2** Datové objekty SM pro důvěrnost 68
 - 10.2.3** Datové objekty SM pro autentizaci 68
 - 10.3** Pomocné datové objekty SM 69
 - 10.3.1** Šablony řídicích odkazů 70
 - 10.3.2** Datové objekty řídicích odkazů v šablonách řídicích odkazů 70
 - 10.3.3** Bezpečnostní prostředí 72
 - 10.3.4** Šablona deskriptoru odezvy 73
 - 10.4** Dopad SM na dvojici příkaz-odezva 74
- 11** Příkazy pro výměnu 75
 - 11.1** Výběr 75
 - 11.1.1** Příkaz select 75
 - 11.1.2** Příkaz manage channel 77
 - 11.2** Používání datových jednotek 78
 - 11.2.1** Datové jednotky 78
 - 11.2.2** Obecně 78
 - 11.2.3** Příkaz read binary 79

- 11.2.4** Příkaz write binary 79
- 11.2.5** Příkaz update binary 80
- 11.2.6** Příkaz search binary 80
- 11.2.7** Příkaz erase binary 80
- 11.2.8** Funkce compare binary 81
- 11.3** Používání záznamů 81
 - 11.3.1** Záznamy 81
 - 11.3.2** Obecně 82
 - 11.3.3** Příkaz read record (s) 82
 - 11.3.4** Příkaz write record 84
 - 11.3.5** Příkaz update record 85

Strana

- 11.3.6** Příkaz append record 85
- 11.3.7** Příkaz search record 86
- 11.3.8** Příkaz erase record (s) 87
- 11.3.9** Příkaz activate record (s) 88
- 11.3.10** Příkaz deactivate record (s) 88
- 11.3.11** Funkce compare record 89
- 11.4** Používání datových objektů 89
 - 11.4.1** Obecně 89
 - 11.4.2** Příkaz select data 90
 - 11.4.3** Příkazy get data/get next data – sudý kód INS 93
 - 11.4.4** Příkaz get data/get next data – lichý kód INS 94
 - 11.4.5** Obecné vlastnosti příkazů put/put next/update data 96
 - 11.4.6** Příkaz put data 96
 - 11.4.7** Příkaz put next data 97
 - 11.4.8** Příkaz update data 98
 - 11.4.9** Funkce compare data 98

- 11.5** Používání základní bezpečnosti 98
 - 11.5.1** Obecně 98
 - 11.5.2** Příkaz internal authenticate 99
 - 11.5.3** Příkaz get challenge 99
 - 11.5.4** Příkaz external authenticate 100
 - 11.5.5** Příkaz general authenticate 100
 - 11.5.6** Příkaz verify 102
 - 11.5.7** Příkaz change reference data 102
 - 11.5.8** Příkaz enable verification requirement 103
 - 11.5.9** Příkaz disable verification requirement 103
 - 11.5.10** Příkaz reset retry counter 104
 - 11.5.11** Příkaz manage security environment 104
- 11.6** Různé 106
 - 11.6.1** Příkaz compare 106
 - 11.6.2** Příkaz get attribute 107
- 11.7** Používání přenosu 108
 - 11.7.1** Příkaz get response 108
 - 11.7.2** Příkaz envelope 108
- 12** Aplikačně nezávislé služby karet 108
 - 12.1** Identifikace karty 109
 - 12.1.1** Historické bajty 109
 - 12.1.2** Obnovení řetězce počátečních dat 112
 - 12.2** Identifikace a výběr aplikace 113
 - 12.2.1** EF.DIR 113
 - 12.2.2** EF.ATR/INFO 113
 - 12.2.3** Identifikátor aplikace 114
 - 12.2.4** Šablona aplikace a příslušné datové prvky 115

12.2.5	Výběr aplikace	115
12.3	Výběr pomoci cesty	116
12.4	Načtení dat	117
12.5	Řetězce bajtů, které mají původ na kartě	117
12.5.1	Spouštění kartou	117
12.5.2	Dotazy a odpovědi	117
12.5.3	Formáty	117
12.6	Správa obecných charakteristik	118
12.6.1	Služby na kartě	118
12.6.2	Služby rozhraní	118
12.6.3	Služby profilu	118
12.6.4	Poskytování dalších informací	119
12.7	Správa jednotek APDU	119
12.7.1	Rozsáhlejší informace	119
12.7.2	Seznam podporovaných kódů INS	119
Příloha A	(informativní) Příklady identifikátorů objektů a schémat přidělování příznaků	120
A.1	Identifikátory objektů	120
A.2	Schémata přidělování příznaků	120
Příloha B	(informativní) Příklady bezpečného předávání zpráv	122
B.1	Kryptografický kontrolní součet	122
B.2	Kryptogramy	125
B.3	Řídící odkazy	126
B.4	Deskriptor odezvy	126
B.5	Příkaz envelope	126
B.6	Součinnost mezi bezpečným předáváním zpráv a bezpečnostními operacemi	126
Příloha C	(informativní) Příklady funkcí authenticate pomocí příkazů general authenticate	130
C.1	GENERAL AUTHENTICATE pomocí trojic svědectví-výzva-odezva	130
C.2	GENERAL AUTHENTICATE pro vícestupňový protokol autentizace	134

Příloha D (informativní) Identifikátory aplikací používající identifikační číslo vydavatele 137

D.1 Základní informace 137

D.2 Formát 137

Příloha E (informativní) Pravidla kódování BER 138

E.1 Pole příznaků ber-tlv 138

E.2 Pole délky ber-tlv 138

E.3 Pole hodnot ber-tlv 139

Příloha F (informativní) Používání datových objektů ber-tlv 140

F.1 Generace a šablony v konstruovaném DO 140

F.2 Odkazování pomocí rozšířeného záhlaví 141

F.3 Použití příkazu update data 143

F.4 Bezpečnostní atribut pro jeden DO 144

F.5 Příklad klíče, na který se odkazuje v DO se samokontrolou 145

Příloha G (informativní) Rozšíření šablony pomocí obálky s příznakem 146

G.1 Obecně 146

Strana

G.2 Odkazování v rámci aktuálního EF 146

G.3 Odkazování v rámci aktuálního DF aplikace, první příklad 147

G.4 Odkazování v aktuálním DF aplikace, druhý příklad 148

G.5 Odkazování mimo aktuální DF aplikace 148

G.6 Upozornění 148

Příloha H (informativní) Analýza rozšířeného záhlaví podle jeho cílového DO 149

Bibliografie 150



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2013

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakémkoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopíí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO v zemi žadatele.

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 mechanismy 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.

Konec náhledu - text dále pokračuje v placené verzi ČSN.