

ICS 33. 120. 00; 35. 240. 60

ČESKÁ NORMA

Duben 1997

Systémy s identifikačními kartami -

Telekomunikační karty s integrovanými obvody

a koncová zařízení - Část 3: Aplikačně nezávislé

požadavky na karty

ČSN EN 726-3

36 9723

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 3: Application independent card requirements

Systèmes de cartes d'identification - Cartes à circuit intégré et terminaux pour les télécommunications - Partie 3: Spécifications de la carte indépendantes des applications

Identifikationskartensysteme - Anforderungen an Chipkarten und Endgeräte für Telekommunikationszwecke - Teil 3: Applikationsunabhängige Anforderungen an die Karte

Tato norma je identická s EN 726-3: 1994 a je vydána se souhlasem CEN, rue de Stassart 36, B-1050 Bruxelles, Belgium.

This standard is identical with EN 726-3: 1994 and is published with the permission of CEN, rue de Stassart 36, B-1050 Bruxelles, Belgium.

Národní předmluva

Pro přehlednost překladu normy je u některých termínů uveden navíc v závorce kurzivou i původní anglický termín. U termínů používaných v anglickém jazyce je český překlad uveden v závorce kurzivou.

Citované normy

EN 726-1 dosud nezavedena

EN 726-21} dosud nezavedena

EN 726-4 dosud nezavedena

ENV 1375-11} dosud nezavedena

EN V 1375-21> dosud nezavedena

EN 27810: 1989 zavedena v ČSN EN 27810 Identifikační karty - Fyzikální vlastnosti (idt ISO 7810: 1985)(36 9725)

EN 27811-1: 1989 zavedena v ČSN EN 27811-1 Identifikační karty - Záznamová technika - Část 1: Reliéfní písmo (idt ISO 7811-1: 1985) (36 9731)

EN 27811-2: 1989 zavedena v ČSN EN 27811-2 Identifikační karty - Záznamová technika - Část 2: Magnetický proužek (idt ISO 7811-2: 1985) (36 9731)

EN 27812: 1989 zavedena v ČSN EN 27812 Identifikační karty - Číselný systém a záznamový postup pro identifikaci vydavatele (idt ISO 7812: 1987) (36 9732)

EN 27816-1: 1989 zavedena v ČSN EN 27816-1 Identifikační karty - Karty s integrovanými obvody a s kontakty Část 1: Fyzikální vlastnosti (idt ISO 7816-1: 1987) (36 9205)

J) v době vydání EN ve stádiu návrhu

© Český normalizační institut, 1996

20621

ČSN EN 726-3

EN 27816-2: 1989 zavedena v ČSN EN 27816-2 Identifikační karty - Karty s integrovanými obvody a s kontakty Část 2: Rozměry a umístění kontaktů (idt ISO 7816-2: 1988) (36 9205)

EN 27816-3: 1992 zavedena v ČSN EN 27816-3 Identifikační karty - Karty s integrovanými obvody a s kontakty Část 3: Elektronické signály a protokoly přenosu (idt ISO/IEC 7816-3: 1989) (36 9205)

EN 27816-3: 1992/A1: 1993 dosud nezavedena

I-ETS 300045-1: 1992 nahrazena I-ETS 300045-1: 1994 zavedenou v ČSN P 87 2526: 1995 Evropský digitální buňkový telekomunikační systém (Fáze 1). Specifikace rozhraní modulu identity účastníka - Mobilní stanice (SIM-ME) Část 1: Všeobecně (GSM 11. 11)

ISO 639: 1988 dosud nezavedena

ISO/IEC 646: 1991 zavedena v ČSN/ISO 646 Informační technika. 7-bitový kódovaný soubor znaků ISO pro výměnu informací (36 9104)

ISO 3166: 1988 zavedena v ČSN ISO 3166 Kódy pro názvy zemí (97 1002)

ISO/IEC 7816-41) dosud nezavedena

ISO/IEC 7816-5 zavedena v ČSN EN ISO/IEC 7816-5 Identifikační karty - Karty s integrovanými obvody s kontakty - Část 5: Systém číslování a registrační postup identifikátorů aplikací (36 9734)

ISO 8859-1: 1987 zavedena v ČSN ISO 8859-1 Zpracování dat. Jedním 8-bitovým bytem kódované soubory grafických znaků. Část 1: Latinská abeceda č. 1 (36 9111)

ISO 9564-1: 1991 zavedena v ČSN ISO 9564-1 Bankovníctví - Řízení a bezpečnost osobních identifikačních karet. Část 1: Principy a techniky ochrany PIN (idt EN 29654-1: 1993) (97 9007)

ISO 9564-2: 1991 zavedena v ČSN ISO 9564-2 Bankovníctví - Řízení a bezpečnost osobních identifikačních karet. Část 2: Schválené algoritmy pro šifrování PIN (idt EN 29654-2: 1993) (97 9007)

ISO 9807: 1991 zavedena v ČSN ISO 9807 Bankovníctví - Požadavky na autentizaci zpráv (bankovní služby pro drobnou klientelu) (97 9005)

ISO 9992-1: 1991 zavedena v ČSN ISO 9992-1 Identifikační karty. Karty pro finanční transakce. Zprávy mezi kartou s integrovanými obvody a zařízením akceptujícím kartu. Část 1: Pojmy a struktury (36 9735)

ISO 9992-21) dosud nezavedena

ISO 10202-01) dosud nezavedena

ISO 10202-1: 1991 zavedena v ČSN ISO 10202-1 Identifikační karty - Karty pro finanční transakce - Bezpečnostní architektura systémů finančních transakcí, využívající karty s integrovanými obvody - Část 1: Životní cyklus karty. (36 9736)

ISO 10202-21) dosud nezavedena

ISO 10202-31) dosud nezavedena

ISO 10202-41) dosud nezavedena

ISO 10202-51) dosud nezavedena

ISO 10202-61) dosud nezavedena

l) v době vydání EN ve stádiu návrhu

2

ČSN EN 726-3

CCITT E. 118: 1988 Doporučení CCITT jsou dostupná v TESCO Praha, Hvoždanská 3, 148 00 Praha 4

CCITT T. 50: 1988 Doporučení CCITT jsou dostupná v TESCO Praha, Hvoždanská 3, 148 00 Praha 4

Další související normy

ČSN EN 24909: 1994 Identifikační karty - Bankovní karty - Obsah dat magnetického proužku pro stopu 3 (idt ISO 4909, 2. vydání, 1987) (36 9727)

ČSN EN 27811-3: 1993 Identifikační karty - Záznamová technika - Část 3: Umístění reliéfních znaků na kartách ID-1 (idt ISO 7811-3: 1985) (36 9731)

ČSN EN 27811-4: 1994 Identifikační karty - Záznamová technika - Část 4: Umístění magnetických stop určených pouze pro snímání - Stopy 1 a 2 (idt ISO 7811-4: 1985) (36 9731)

ČSN EN 27813: 1994 Identifikační karty - Karty pro finanční transakce (idt ISO 7813: 1990) (36 9733)

ČSN ISO 7580: 1994 Identifikační karty - Zprávy vytvořené kartou - Obsah pro finanční transakce (36 9215)

Vypracování normy

Zpracovatel: Dr. Karel Jurák, Praha, IČO 40812839

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Jaromír Čížek

3

ČSN EN 726-3

EVROPSKÁ NORMA EUROPEAN STANDARD NORME EUROPÉENNE EUROPÄISCHE NORM

EN 726-3

Prosinec 1994

ICS 33. 120. 00; 35. 240. 60

Deskriptory: telecommunications, IC cards, telecommunication terminals, specifications, characteristics

Systémy s identifikačními kartami - Telekomunikační karty s integrovanými obvody a koncová zařízení- Část 3: Aplikačně nezávislé požadavky na karty

Identification card systems -

Telecommunications integrated circuit(s) cards

and terminals - Part 3: Application independent

card requirements

Systèmes de cartes d'identification - Cartes à circuit intégré et terminaux pour les télécommunications - Partie 3: Spécifications de la carte indépendantes des applications

Identifikationskartensysteme - Anforderungen an Chipkarten und Endgeräte für Telekommunikationszwecke - Teil 3: Applikationsunabhängige Anforderungen an die Karte

Tato evropská norma byla schválena CEN 5. prosince 1994. Členové CEN jsou povinni splnit Vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých je třeba této evropské normě bez jakýchkoliv změn dát status národní normy.

Aktualizované seznamy těchto národních norem s jejich bibliografickými odkazy lze obdržet na vyžádání u Ústředního sekretariátu nebo u kteréhokoliv člena CEN.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v jakémkoliv jiném jazyku přeložená členem CEN do jeho vlastního jazyka, za kterou tento člen zodpovídá a notifikuje ji Ústřednímu sekretariátu, má stejný status jako oficiální verze.

Členy CEN jsou národní normalizační orgány Belgie, Dánska, Finska, Francie, Irska, Islandu, Itálie, Lucemburska, Německa, Nizozemska, Norska, Portugalska, Rakouska, Řecka, Spojeného království, Španělska, Švédska a Švýcarska.

CEN

Evropská komise pro normalizaci

European Committee for Standardization

Comité Européen de Normalisation

Europäisches Komitee für Normung

Ústřední sekretariát: rue de Stassart 36, B-1050 Bruxelles

5

ČSN EN 726-3

Obsah

Předmluva.....	6
1 Předmět normy a rozsah platnosti.....	6
2 Normativní odkazy.....	7
3 Definice, zkratky a značky.....	9
4 Fyzikální charakteristiky karty.....	11
5 Elektronické signály a protokoly přenosu.....	11
6 Logický model IC karet.....	12
7 Bezpečnostní prostředky pro karty.....	17
8 Popis funkcí.....	23
9 Popis příkazů.....	37

10 Obsah speciálních souborů	
EF.....	82
11 Možnost spolupráce IC karet.....	92
12 Bezpečnostní aspekty pro výrobce karet, provozovatele aplikací a vydavatele karet.....	92
Příloha A (informativní) Příklad vytvoření aplikace na kartě.....	94
Příloha B (informativní) Příklady mechanismů certifikace.....	95
Příloha C (informativní) Administrativní opatření.....	97

Předmluva

Tato evropská norma byla připravena ETSI STC TE9 a převzata CEN/TC 224 "Strojově čitelné karty, rozhraní a činnost souvisejících zařízení", jejíž sekretariát je držen AFNOR.

Tento dokument byl předložen k formálnímu hlasování a výsledky formálního hlasování byly pozitivní.

Této evropské normě bude nejpozději do června 1995 udělen status národní normy, a to buď vydáním identického textu, nebo schválením k přímému používání, a národní normy, které jsou s ní v rozporu, budou zrušeny nejpozději do června 1995.

V souladu s Vnitřními předpisy CEN/CENELEC jsou následující země povinny převzít tuto evropskou normu: Belgie, Dánsko, Finsko, Francie, Irsko, Island, Itálie, Lucembursko, Německo, Nizozemsko, Norsko, Portugalsko, Rakousko, Řecko, Spojené království, Španělsko, Švédsko a Švýcarsko.

Tato evropská norma sestává z následujících částí, pod společným názvem Systémy s identifikačními kartami Telekomunikační karty s integrovanými obvody a koncová zařízení:

Část 1: Přehled systémů

Část 2: Bezpečnostní aspekty

Část 3: Aplikačně nezávislé požadavky na karty

Část 4: Aplikačně nezávislé požadavky na koncová zařízení, vztahující se na karty

Část 5: Metody plateb

Část 6: Telekomunikační služby

Část 7: Bezpečnostní modul

1 Předmět normy a rozsah platnosti

Tato část EN 726 specifikuje aplikačně nezávislé charakteristiky víceaplikačních IC karet a zásuvných modulů pro telekomunikační aplikace, aby se zajistila vzájemná možnost spolupráce

telekomunikačních karet s různými systémy a koncovými zařízeními. Jednoaplikační karty se považují za podmnožinu víceaplikačních karet. Jsou definovány všechny společné charakteristiky, nezbytné pro interakce mezi kartou a vnějším světem.

Tato část EN 726 nebrání kartám z jiných sektorů, aby obsahovaly telekomunikační aplikaci (aplikace), založené na této části EN 726.

Aplikačně specifické charakteristiky nejsou definovány v této části EN 726. Tyto jsou definovány a popsány v příslušných aplikačních požadavcích.

6

ČSN EN 726-3

Tato část EN 726 nespecifikuje žádnou interní technickou implementaci. Tato část popisuje:

- požadavky na fyzikální charakteristiky karty, elektronické signály a protokoly přenosu;
- aplikačně nezávislý logický model, který má být použit jako základ pro návrh logické struktury, případně několika aplikací na kartě;
- bezpečnostní prostředky, které se vztahují na přístup k různým částem karty a možné interakce mezi těmito částmi. Rovněž jsou popisovány bezpečnostní funkce, které mohou být potřebné obecně pro různé aplikace. Tyto by měly být k dispozici jako společná sada;
- popis aplikačně nezávislých funkcí mezi kartou a vnějším světem by měl být použit jako normalizovaná společná sada pro všechny základní funkce používané, v mezinárodních aplikacích;
- mapování zpráv těchto aplikací (příkazy a odpovědi) pod normalizovanými protokoly;
- obsah hlavního souboru;
- vzájemná spolupráce IC karet;
- celkové bezpečnostní aspekty pro výrobce karet, provozovatele aplikací a vydavatele karet.

7