



**Systémy s identifikačními kartami -
Telekomunikační karty s integrovanými
obvody a koncová zařízení -
Část 2: Bezpečnostní aspekty**

**ČSN
EN 72 6-2**

36 9723

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 2: Security framework

Systèmes de cartes d'identification - Cartes à circuit intégré et terminaux pour les télécommunications - Partie 2: Cadre général pour la sécurité

Identifikationskartensysteme - Chipkarten und Endgeräte für Telekommunikationszwecke - Teil 2: Sicherheitsgrundgerüst

Tato norma je českou verzí evropské normy EN 726-2:1995. Evropská norma EN 726-2:1995 má status české technické normy.

This standard is the Czech version of the European Standard EN 726-2:1995. The European Standard EN 726-2:1995 has the status of a Czech Standard.

Nahrazení předchozích norem

Tato norma nahrazuje ČSN EN 726-2 (36 9723) z března 1997.

© Český normalizační institut, 1997

26030

Strana 2

Národní předmluva

Pro přehlednost překladu normy je u některých termínů uveden v závorce kurzívou i původní anglický termín. Jsou-li termíny pouze v anglickém jazyce, je český překlad uveden v závorce kurzívou.

Změny proti předchozí normě

Proti předchozí normě dochází ke změně způsobu převzetí EN 726-2:1995 do soustavy norem ČSN. Zatímco ČSN EN 726-2 z března 1997 převzala EN 726-2:1995 schválením k přímému používání jako ČSN, tato norma ji přejímá překladem.

Citované normy

EN 726-1 zavedena v ČSN EN 726-1 Systémy s identifikačními kartami - Telekomunikační karty s integrovanými obvody a koncová zařízení - Část 1: Přehled systémů (36 9723)

EN 726-3:1994 zavedena v ČSN EN 726-3 Systémy s identifikačními kartami - Telekomunikační karty s integrovanými obvody a koncová zařízení - Část 3: Aplikačně nezávislé požadavky na karty (36 9723)

prEN 726-7:1994 dosud nezavedena

EN 27498:1989 zavedena v ČSN EN 27498 Systémy na zpracování informací. Propojení otevřených systémů. Základní referenční model (36 9614)

ISO 7498-2:1989 zavedena v ČSN ISO 7498-2 Systémy na zpracování informací. Propojení otevřených systémů. Základní referenční model - Část 2: Bezpečnostní architektura (36 9615)

ISO/IEC 9798-2 dosud nezavedena

ISO 9798-3 dosud nezavedena

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

Vypracování normy

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

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Jaromír Čížek

Strana 3

**EVROPSKÁ NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM**

**EN 726-2
Listopad 1995**

ICS 33.120.00; 35.240.60

Deskriptory: telecommunications, telecommunication terminals, IC cards, specifications, utilization, safety

Systémy s identifikačními kartami - Telekomunikační karty s integrovanými obvody a koncová zařízení - Část 2: Bezpečnostní aspekty

Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 2: Security framework

Systèmes de cartes d'identification - Cartes à circuit intégré et terminaux pour les télécommunications - Partie 2: Cadre général pour la sécurité

Identifikationskartensysteme - Chipkarten und Endgeräte für Telekommunikationszwecke - Teil 2: Sicherheitsgrundgerüst

Tato evropská norma byla schválena CEN 1995-10-18. Členové CEN jsou povinni splnit požadavky Vnitřních předpisů CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoli modifikací uděluje status národní normy.

Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze vyžádat v Ústředním sekretariátu CEN nebo u kteréhokoliv člena CEN.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce, přeložená členem CEN do jeho vlastního jazyka, za kterou odpovídá a kterou notifikuje 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 Brussels

Obsah	strana
Předmluva	6
1 Předmět normy a rozsah platnosti	6
2 Normativní odkazy	6
3 Definice a zkratky	7
3.1 Definice	7
3.2 Zkratky	8
4 Referenční model	9
5 Obecný bezpečnostní přístup	9
5.1 Metodika	9
5.2 Určení bezpečnostních požadavků	10
5.2.1 Výroba integrovaných obvodů a IC karet (fáze 1)	10
5.2.2 Fáze přípravy karty (fáze 2)	10
5.2.3 Příprava aplikace (fáze 3)	10
5.2.4 Fáze užití (fáze 4)	10
5.2.5 Ukončení používání (fáze 5)	10
5.3 Obecné bezpečnostní služby	11
5.3.1 Služba řízení přístupu	11
5.3.2 Služba ověření pravosti (autentizace)	11
5.3.3 Služba zajištění důvěrnosti	11
5.3.4 Služba zajištění integrity	11
5.3.5 Služba neodmítnutelnosti	12
5.3.6 Služba auditu	12
5.4 Obecné bezpečnostní mechanismy	12
6 Aplikačně nezávislá bezpečnost	12
6.1 Požadavky aplikačně nezávislé bezpečnosti	12
6.1.1 Výroba integrovaných obvodů a IC karet (fáze 1)	13
6.1.2 Fáze přípravy karty (fáze 2)	14
6.1.3 Příprava aplikace (fáze 3)	15
6.1.4 Fáze užití (fáze 4)	16
6.1.5 Ukončení používání (fáze 5)	17
6.2 Služby aplikačně nezávislé bezpečnosti	18
6.3 Mechanismy aplikačně nezávislé bezpečnosti	19
6.3.1 Informace řízení přístupu	20
6.3.2 Mechanismus PIN	21
6.3.3 Vnitřní autentizace	21
6.3.4 Vnější autentizace	22
6.3.5 Chráněný režim	22
6.3.6 Známkový režim	23
6.3.7 Zavedení klíčového souboru	23

7 Aplikačně závislá bezpečnost	23
7.1 Metodika	23
7.2 Blokované schéma	25

Příloha A (normativní)

Použití algoritmu TESA-7 v telekomunikačních aplikacích podle EN	726
A.1 Úvod	26
A.2 Obecná specifikace režimů vnějšího rozhraní pro TESA-7	26
A.2.1 Funkce vytvoření klíče	27
A.2.2 Funkce autentizace	27
A.2.3 Režim MAC	28
A.2.4 Inverzní funkce k vytvoření klíče	29
A.2.5 Režim diverzifikace klíče	29
A.3 Použití algoritmu TESA-7	29
A.3.1 INTERNAL AUTHENTICATION/VERIFY CRYPTOGRAM	30
A.3.2 EXTERNAL AUTHENTICATION/COMPUTE CRYPTOGRAM	31
A.3.3 Chráněný režim/COMPUTE MAC (SM) nebo DECREASE (SM)	32
A.3.4 Známkový režim/VERIFY MAC nebo INCREASE (SM) nebo UPDATE (SM)	34
A.3.5 COMPUTE LOAD KEY	35
A.3.6 LOAD KEY FILE	36
A.3.7 Diverzifikace sady klíčů	37

Předmluva

Tato evropská norma byla vypracována Technickou komisí CEN/TC 224 „Strojově čitelné karty, rozhraní a činnost souvisejících zařízení“ , jejíž sekretariát je při AFNOR.

Této evropské normě bude nejpozději do května 1996 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 května 1996.

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 možnosti

Část 7: Bezpečnostní modul

1 Předmět normy a rozsah platnosti

Tato část EN 726 specifikuje bezpečnostní aspekty pro používání IC karet v telekomunikacích. Tato specifikace nepopisuje žádné podrobnosti zavedení. Tato část popisuje:

- obecný bezpečnostní přístup, jehož výsledkem je metodika, jednotlivé fáze života karty pro stanovení bezpečnostních požadavků a popis bezpečnostních služeb, které mohou být nabízeny IC kartou;
- zavedení obecného bezpečnostního přístupu do aplikačně nezávislých IC karet, jehož výsledkem je seznam požadavků aplikačně nezávislé bezpečnosti, výběr potřebných bezpečnostních služeb a popis společné sady aplikačně nezávislých mechanismů;
- zavedení obecného bezpečnostního přístupu do aplikací používajících IC karty, jehož výsledkem je metodika použitá při návrhu sady bezpečnostních mechanismů pro specifické aplikace.

-- Vynechaný text --