

	Identifikationskartensysteme Chipkarten und Endgeräte für Telekommunikationszwecke Teil 6: Leistungsmerkmale Deutsche Fassung EN 726-6 : 1995	DIN EN 726-6
ICS 33.120.00; 35.240.60 Deskriptoren: Identifikationskarte, Chipkarte, Endgerät, Telekommunikation Identification card systems — Telecommunications integrated circuit(s) cards and terminals — Part 6: Telecommunication features; German version EN 726-6 : 1995 Systèmes de cartes d'identification — Cartes à circuit intégré et terminaux pour les télécommunications — Partie 6: Services de télécommunications; Version allemande EN 726-6 : 1995 Die Europäische Norm EN 726-6:1995 hat den Status einer Deutschen Norm. Nationales Vorwort Die vorliegende Norm ist Teil einer mehrteiligen Europäischen Norm mit dem Titel "Identifikationskartensysteme — Anforderungen an Chipkarten für Telekommunikationszwecke". Sie stammt aus dem Arbeitsprogramm von CEN/TC 224 und geht auf Arbeiten von ETSI STC-TE9 zurück. Für die im Abschnitt 2 zitierten Internationalen Normen wird im folgenden auf die entsprechenden Deutschen Normen hingewiesen: ISO 1073 siehe DIN 66008-1 ISO/IEC 7816-5 siehe DIN EN ISO/IEC 7816-5 Nationaler Anhang (informativ) Literaturhinweise DIN 66008-1 Schrift A für die maschinelle optische Zeichenerkennung — Teil 1: Zeichen und Nennmaße DIN EN ISO/IEC 7816-5 Identifikationskarten — Chipkarten mit Kontakten — Teil 5: Numerierungssystem und Registrierverfahren für Anwendungsbezeichner (ISO/IEC 7816-5 : 1994); Deutsche Fassung EN ISO/IEC 7816-5 : 1995 Fortsetzung 18 Seiten EN Normenausschuß Informationstechnik (NI) im DIN Deutsches Institut für Normung e.V.		

ICS 33.120.00; 35.240.60

Deskriptoren: Telekommunikation, Terminal, Chipkarte, Anforderung, Schnittstellen, Dienstleistung, Benummerung, Datei

Deutsche Fassung

Identifikationskartensysteme

Chipkarten und Endgeräte für Telekommunikationszwecke

Teil 6: Leistungsmerkmale

Identification card systems — Telecommunications integrated circuit(s) cards and terminals — Part 6: Telecommunication features

Systèmes de cartes d'identification — Cartes à circuit intégré et terminaux pour les télécommunications — Partie 6: Services de télécommunications

Diese Europäische Norm wurde von CEN am 1995-10-18 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien und dem Vereinigten Königreich.

CEN

EUROPÄISCHES KOMITEE FÜR NORMUNG

European Committee for Standardization

Comité Européen de Normalisation

Zentralsekretariat: rue de Stassart 36, B-1050 Brüssel

Inhalt

	Seite		Seite
Vorwort	3	6 Beschränkende Telekommunikations- Leistungsmerkmale	11
1 Anwendungsbereich	3	6.1 Allgemeines Konzept	11
2 Normative Verweisungen	3	7 Wahl festgelegter Rufnummern	11
3 Begriffe und Abkürzungen	4	7.1 Allgemeines Konzept	11
3.1 Begriffe	4	7.2 Erforderliche Daten	11
3.2 Abkürzungen	4	7.2.1 Spezielle Dateien für die Wahl festgelegter Nummern	11
3.3 Bezeichnungen	4	7.2.2 EF _{FIX}	11
4 Allgemeines Konzept	4	7.2.3 Datei für Leistungsfähigkeits-/ Konfigurations-Parameter für Wahl festgelegter Rufnummern: EF _{CCPF}	12
4.1 Auswahl eines Telekommunikations- Leistungsmerkmals	4	7.2.4 Datei für Erweiterungen der Wahl festgelegter Rufnummern: EF _{EXTF}	13
4.2 Konzept eines Telekommunikations- Leistungsmerkmals innerhalb einer Kartenarchitektur	5	7.3 Abläufe für die Wahl festgelegter Rufnummern	13
4.3 Übereinstimmung von Schlüsseln und Algorithmen	5	7.3.1 Teilnehmer auswählen mittels Wahl festgelegter Rufnummern	13
5 Kurzwahl	5	7.3.2 Einspeichern der festgelegten Rufnummern (Verwaltungs-Tätigkeit)	14
5.1 Allgemeines Konzept	5	Anhang A (informativ) Wahl fester Rufnummern mit der Fähigkeit, die Beschränkungen unwirksam zu machen	15
5.2 Sicherheitsvorkehrungen	5	A.1 Architektur der Karte	15
5.3 Arten von Kurzwahlmöglichkeiten	5	A.2 Struktur der Karte	15
5.3.1 Kurzwahl	5	A.3 Betriebsarten	15
5.3.2 Wahlwiederholung	6	A.3.1 Karte, bei der Beschränkungen der Wahl fester Rufnummern nicht wirksam sind	15
5.4 Erforderliche Daten	6	A.3.2 Karte, bei der die Applikation Wahl fester Rufnummern aktiv ist (beschränkter Zugriff auf LIMITED-Anwendung)	15
5.4.1 Spezielle Dateien für Kurzwahl	6	A.4 Vermittlungsfunktionalität	15
5.4.2 Beschreibung der Applikation DF _{DIAL}	6	A.4.1 Wahl fester Rufnummern aktiv	15
5.4.3 Datei für die Kurzwahl: EF _{DIAL}	6	A.4.2 Wahl fester Rufnummern unwirksam	15
5.4.4 Datei für Leistungsfähigkeits-/ Konfigurations-Parameter: EF _{CCP}	8	Anhang B (informativ) Beschränkte Tele- kommunikations-Leistungsmerkmale ..	16
5.4.5 Datei für Erweiterungen: EF _{EXT}	8	B.1 Allgemeines Konzept	16
5.4.6 Datei für Wahlwiederholung: EF _{LND}	9	B.2 Erforderliche Daten für ein beschränkendes Telekommunikations- Leistungsmerkmal	16
5.4.7 EF _{CHV}	9	B.2.1 Struktur der Datei	16
5.4.8 EF _{KEY_MAN} und EF _{KEY_OP}	10	B.2.2 DF _{ING}	17
5.5 Abläufe speziell für Kurzwahl-Arten	10	B.2.3 EF _{PASSWORD}	17
5.5.1 Anwahl eines Kurzwahl-Leistungsmerkmals ..	10	B.2.4 EF _{CHV}	17
5.5.2 Teilnehmer auswählen mit alphanumerischer ID	10	B.2.5 EF _{KEY_MAN} und EF _{KEY_OP}	18
5.5.3 Hinzufügen einer neuen Teilnehmernummer durch Erzeugen eines neuen Datensatzes	10		
5.5.4 Aktualisieren eines bestehenden Datensatzes	11		
5.6 Abläufe speziell für die Wahlwiederholung	11		
5.6.1 Anwahl des Leistungsmerkmals Wahlwiederholung	11		
5.6.2 Teilnehmer auswählen mit Wahlwiederholung	11		
5.6.3 Speichern der letzten gewählten Nummer	11		

Vorwort

Diese Europäische Norm wurde vom Technischen Komitee CEN/TC 224 "Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren", dessen Sekretariat von AFNOR betreut wird, erarbeitet.

Diese Europäische Norm muß den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Mai 1996, und etwaige entgegenstehende nationale Normen müssen bis Mai 1996 zurückgezogen werden.

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die folgenden Länder gehalten, diese Europäische Norm zu übernehmen:

Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Italien, Luxemburg, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien und das Vereinigte Königreich.

Diese Europäische Norm unter dem Haupttitel "Identifikationskarten — Anforderungen an Chipkarten und Endgeräte für Telekommunikationszwecke" besteht aus folgenden Teilen:

- Teil 1: Systemüberblick
- Teil 2: Sicherheitsgrundgerüst
- Teil 3: Applikationsunabhängige Anforderungen an die Karte
- Teil 4: Applikationsunabhängige, kartenbezogene Anforderungen an Endgeräte
- Teil 5: Bezahlungsmethoden
- Teil 6: Leistungsmerkmale
- Teil 7: Sicherheitsmodul

1 Anwendungsbereich

Dieser Teil der EN 726 legt die Telekommunikations-Leistungsmerkmale für den Gebrauch von Chipkarten fest. Diese Telekommunikationsmerkmale können für mehr als nur eine Anwendung genutzt werden.

Dieser Teil der EN 726 beschreibt die Kartenschnittstelle des Endgerätes. Wo es erforderlich ist, wird jedoch auch die Umgebung betrachtet.

Dieser Teil der EN 726 beschreibt die folgenden Telekom-munikations-Leistungsmerkmale:

- Kurzwahl
- Wahlwiederholung (Speicherung in der Karte)
- Feste Wahlziele

2 Normative Verweisungen

Diese Europäische Norm enthält durch datierte oder undatierte Verweisungen Festlegungen aus anderen Publikationen. Diese normativen Verweisungen sind an den jeweiligen Stellen im Text zitiert, und die Publikationen sind nachstehend aufgeführt. Bei datierten Verweisungen gehören spätere Änderungen oder Überarbeitungen dieser Publikationen nur zu dieser Europäischen Norm, falls sie durch Änderung oder Überarbeitung eingearbeitet sind. Bei undatierten Verweisungen gilt die letzte Ausgabe der in Bezug genommenen Publikation.

EN 726-1

Identification card systems — Telecommunications integrated circuit(s) cards and terminals — Part 1: System overview

EN 726-2

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

EN 726-3 : 1994

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

EN 726-4

Identification card systems — Telecommunications integrated circuit(s) cards and terminals — Part 4: Application independent card related terminal requirements

prEN 726-5

Identification card systems — Telecommunications integrated circuit(s) cards and terminals — Part 5: Payment methods.

ISO/IEC 646 : 1991

Information technology — ISO 7-bit coded character set for information interchange

ISO 1073-1 : 1976

Alphanumeric character sets for optical recognition — Part 1: Character set OCR-A — Shapes and dimensions of the printed image

ISO 1073-2 : 1976

Alphanumeric character sets for optical recognition — Part 2: Character set OCR-B — Shapes and dimensions of the printed image

ISO/IEC 7816-5

Identification cards — integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers

ISO 10202-3

Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 3: Cryptographic key relationships

CCITT Recommendation E.164 : 1991

Numbering plan for ISDN ERA

CCITT Recommendation I.330 : 1988

ISDN numbering and addressing principles

CCITT Recommendation T.50 : 1988

International alphabet No. 5

GSM 03.40 — Version 3.5.0

European digital cellular telecommunication system (Phase 2). Technical realization of the Short Message Service (SMS) Point-to-Point (PP)



Documents

Document Sharing Hub

3 Begriffe und Abkürzungen

3.1 Begriffe

Für diese Norm gelten folgende Definitionen:

3.1.1 Zugriffsbedingungen (AC): Eine Reihe von Sicherheitsattributen für eine Datei.

3.1.2 Anwendung: Eine Anwendung (Applikation) besteht aus einer Reihe von Sicherheitsmechanismen, Dateien, Daten, Protokollen (nicht Übertragungsprotokollen), die innerhalb der Chipkarte (Karten-Anwendung) und außerhalb (externe Anwendung) angesiedelt sind und angewandt werden.

3.1.3 Anwendungs-Anbieter (AP): Die Instanz, die nach der Einrichtung der Anwendung dafür verantwortlich ist. Ein AP kann mehrere Anwendungen in einer Karte haben. Die einer Anwendung entsprechenden Dateien in der Karte werden Karten-Anwendung genannt. In einer Karte können mehrere Anwendungen ein und desselben Anwendungs-Anbieters vorhanden sein.

3.1.4 Karte: Eine Multi-Applikationskarte kann als Sammlung von Dateien betrachtet werden, von denen einige von den verschiedenen Anwendungs-Anbietern und/oder Kartenherausgebern gemeinsam benutzt werden, während andere Dateien ausschließlich den verschiedenen Anwendungs-Anbietern oder dem Kartenherausgeber gehören. Dateien können z. B. gelesen, beschrieben oder ausgeführt werden.

3.1.5 Karten-Anwendung: Der kartenbezogene Teil einer Anwendung.

3.1.6 Kartenausgeber: Der Kartenausgeber ist verantwortlich für die gemeinsamen Daten der Karte, die Zuteilung des Speicherplatzes für die Anwendungen und versorgt die Anwendungs-Anbieter mit den notwendigen Hilfsmitteln, um die gewünschte Anwendung laden zu können.

3.1.7 Zugeordnete Datei (DF): Eine Datei mit Zugriffsbedingungen und zugeteiltem Speicher. Sie kann Stammdatei für Elementar-Dateien und/oder Zugeordnete Dateien sein.

3.1.8 Elementar-Datei (EF): Eine optionale Datei, die Zugriffsbedingungen, Daten oder ein Programm, aber keine weiteren Dateien enthält.

EF_{CHV} ist eine Elementar-Datei, die die Information für den Echtheitsnachweis des Kartenbesitzers enthält (CHV).

EF_{DIR} ist eine Elementar-Datei auf der Ebene der Haupt-Datei (MF), welche eine Liste aller (oder einen Teil der) verfügbaren Anwendungen der Karte enthält.

EF_{KEY_MAN} ist eine Elementar-Datei, die Schlüssel für die Verwaltung enthält.

EF_{KEY_OP} ist eine Elementar-Datei, die Schlüssel für Abläufe enthält.

3.1.9 Externe Anwendung: Teil, der außerhalb der Karte angesiedelt ist und welcher während der Nutzung mit der entsprechenden Karten-Anwendung in Verbindung steht.

3.1.10 Externe Welt: Alle anwendungsbezogenen Teile außerhalb der Karte (im Falle eines Off-Line-Systems: Kartenzugangsgerät, im Falle eines On-Line-Systems: Kartenzugangsgerät, Netzwerk, Host, ...).

3.1.11 Identifikator (ID): Die Identifikationsnummer einer Datei (MF, DF, EF). Sie besteht aus zwei Bytes.

3.1.12 Version der Schlüssel-Datei: Gibt die absolute Versionsnummer der Schlüssel-Datei (codiert in BCD) an.

3.1.13 Haupt-Datei (MF): Die einzige obligatorische Datei, die die Wurzel der Dateistruktur darstellt und Zugriffsbedingungen und zuordenbaren Speicher enthält. Sie kann Stammdatei von Elementar-Dateien und/oder Zugeordneten Dateien sein.

3.1.14 Betrieb: Eine Folge von Funktionsabläufen zwischen der Karten-Anwendung und der externen Welt.

3.1.15 Pfad: Verkettung von Identifikatoren ohne Begrenzung.

3.1.16 Datensatz: Eine Anzahl Bytes, die von der Chipkarte als Einheit behandelt wird und auf die mit einer Datensatz-Nummer oder einem Datensatz-Zeiger verwiesen wird.

3.1.17 Datensatz-Nummer: Sequentiell und einmalig innerhalb einer EF; wird von der Karte verwaltet.

3.1.18 Telekommunikations-Leistungsmerkmal: Eine Anwendung, die für verschiedene Telekommunikationsdienste geeignet ist unter Bedingungen, die in den entsprechenden Elementar-Dateien spezifiziert sind.

3.2 Abkürzungen

Im Sinne dieser Norm gelten folgende Abkürzungen:

AC	Zugriffsbedingungen
AID	Anwendungsbezeichner
CHV	Kartenbesitzer-Überprüfung (card holder verification)
DF	Zugeordnete Datei
EF	Elementar-Datei
ffs	noch festzulegen (for further study)
IC	Integrierter Schaltkreis
ICC	Karte mit integriertem Schaltkreis (IC-Karte, Chipkarte)
EW	Externe Welt
MF	Haupt-Datei
PIN	Persönliche Geheimzahl

3.3 Bezeichnungen

'0' bis '9' und 'A' bis 'F': die sechzehn Hexadezimal-Zeichen.

4 Allgemeines Konzept

4.1 Auswahl eines Telekommunikations-Leistungsmerkmals

Um festzustellen, welche Telekommunikations-Leistungsmerkmale durch die Chipkarte unterstützt werden, muß die externe Anwendung aus der Hauptdatei-Ebene die Datei EF_{DIR} auslesen (siehe 726-3 und ISO/IEC 7816-5). Diese EF_{DIR} kann alle standardisierten Anwendungsbezeichner der verschiedenen von der Karte unterstützten Anwendung und die für die Auswahl nötigen Pfade enthalten.

Wenn die Anwendung, die zu einem bestimmten Telekommunikationsmerkmal gehört, in der Karte vorhanden, aber nicht in der EF_{DIR} aufgeführt ist (versteckte Anwendung), dann sollte zumindest die externe Welt den Pfad und den entsprechenden Anwendungsbezeichner kennen.

Die externe Anwendung soll die Liste der in der Chipkarte verfügbaren Telekommunikations-Leistungsmerkmale mit