

ICS 33.120.00: 35.240.60

Deskriptoren: Telekommunikation, Chipkarte, Endgerät, Sicherheit, IC-Karte

Identification card systems – Telecommunications integrated circuit(s) cards and terminals –

## Part 2: Security framework:

German version EN 726-2:1995

## Systèmes de cartes d'identification – Cartes à circuit intégré et terminaux pour les télécommunications –

Partie 2: Cadre général pour la sécurité;

Version allemande EN 726-2:1995

**Die Europäische Norm EN 726-2 : 1995 hat den Status einer Deutschen Norm.**

## Nationales Vorwort

Die vorliegende Norm ist Teil einer mehrteiligen Europäischen Norm mit dem Titel "Identifikationskartensysteme – Chipkarten und Endgeräte für Telekommunikationszwecke".

Sie stammt aus dem Arbeitsprogramm von CEN/TC 224 und geht auf Arbeiten von ETSI STG-TE9 zurück.

Fortsetzung 32 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, Ausnutzung, Sicherheit

**Deutsche Fassung**

Identifikationskartensysteme

**Chipkarten und Endgeräte für Telekommunikationszwecke  
Teil 2 : Sicherheitsgrundgerüst**

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

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 |
|-------------------------------------------------------|-------|-----------------------------------------------------------------------------------------------------------------|-------|
| <b>Vorwort</b> .....                                  | 2     | 6.3.1 Information zur Zugangskontrolle .....                                                                    | 14    |
| <b>1 Anwendungsbereich</b> .....                      | 3     | 6.3.2 PIN-Mechanismus .....                                                                                     | 14    |
| <b>2 Normative Verweisungen</b> .....                 | 3     | 6.3.3 Interne Echtheitsüberprüfung .....                                                                        | 15    |
| <b>3 Definitionen und Abkürzungen</b> .....           | 3     | 6.3.4 Externe Echtheitsüberprüfung .....                                                                        | 15    |
| 3.1 Definitionen .....                                | 3     | 6.3.5 Geschützter Modus .....                                                                                   | 16    |
| 3.2 Abkürzungen .....                                 | 4     | 6.3.6 Verschlüsselter Modus (stamped mode) .....                                                                | 16    |
| <b>4 Bezugsmodell</b> .....                           | 4     | 6.3.7 Datei zum Laden des Schlüssels .....                                                                      | 17    |
| <b>5 Allgemeiner Sicherheitsansatz</b> .....          | 4     | <b>7 Applikationsabhängige Sicherheit</b> .....                                                                 | 17    |
| 5.1 Methodik .....                                    | 4     | 7.1 Methodik .....                                                                                              | 17    |
| 5.2 Festlegung der Sicherheitsanforderungen .....     | 4     | 7.2 Flußdiagramm .....                                                                                          | 18    |
| 5.2.1 Herstellung von Chip und Chipkarte (Phase 1) .. | 5     | <b>Anhang A (normativ) Verwendung des TESA-7-Algorithmus in Telekommunikationsanwendungen nach EN 726</b> ..... | 19    |
| 5.2.2 Vorbereitung der Karte (Phase 2) .....          | 5     | A.1 Einführung .....                                                                                            | 19    |
| 5.2.3 Vorbereitung der Applikation (Phase 3) .....    | 5     | A.2 Allgemeine Spezifikation externer Schnittstellen für TESA-7-Modi .....                                      | 19    |
| 5.2.4 Benutzung (Phase 4) .....                       | 5     | A.2.1 Funktion Schlüsselerstellung .....                                                                        | 19    |
| 5.2.5 Beendigung der Benutzung (Phase 5) .....        | 5     | A.2.2 Funktion Echtheitsüberprüfung .....                                                                       | 20    |
| 5.3 Allgemeine Sicherheitsdienste .....               | 5     | A.2.3 MAC-Modus .....                                                                                           | 21    |
| 5.3.1 Zugangskontrolle .....                          | 5     | A.2.4 Funktion umgekehrte Schlüsselerstellung .....                                                             | 22    |
| 5.3.2 Überprüfung der Echtheit .....                  | 5     | A.2.5 Schlüsseldiversifizierungs-Modus .....                                                                    | 22    |
| 5.3.3 Vertraulichkeit .....                           | 5     | A.3 Verwendung des TESA-7-Algorithmus .....                                                                     | 23    |
| 5.3.4 Fälschungsschutz .....                          | 5     | A.3.1 Interne Echtheitsüberprüfung/Kryptogrammprüfung .....                                                     | 23    |
| 5.3.5 Nicht-Zurückweisung .....                       | 6     | A.3.2 Externe Echtheitsüberprüfung/Kryptogrammberechnung .....                                                  | 24    |
| 5.3.6 Prüffunktion .....                              | 6     | A.3.3 Geschützter Modus/BERECHNE MAC (SM) oder VERMINDERE (SM) .....                                            | 26    |
| 5.4 Allgemeine Sicherheitsmechanismen .....           | 6     | A.3.4 Verschlüsselter Modus/PRÜFE MAC oder ERHÖHE (SM) oder AKTUALISIERE (SM) ..                                | 27    |
| <b>6 Applikationsunabhängige Sicherheit</b> .....     | 6     | A.3.5 Berechne Lade-Schlüssel .....                                                                             | 29    |
| 6.1 Applikationsunabhängige Sicherheitsanforderungen  | 6     | A.3.6 LADE-SCHLÜSSEL-DATEI .....                                                                                | 30    |
| 6.1.1 Herstellung von Chip und Chipkarte (Phase 1) .. | 7     | A.3.7 Diversifiziere Schlüsselsatz .....                                                                        | 31    |
| 6.1.2 Vorbereitung der Karte (Phase 2) .....          | 8     |                                                                                                                 |       |
| 6.1.3 Vorbereitung der Applikation (Phase 3) .....    | 9     |                                                                                                                 |       |
| 6.1.4 Benutzung (Phase 4) .....                       | 10    |                                                                                                                 |       |
| 6.1.5 Beendigung der Benutzung (Phase 5) .....        | 11    |                                                                                                                 |       |
| 6.2 Applikationsunabhängige Sicherheitsdienste .....  | 12    |                                                                                                                 |       |
| 6.3 Applikationsunabhängige Sicherheitsmechanismen    | 13    |                                                                                                                 |       |

## Vorwort

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

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 "Identifikationskartensysteme – 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 Anforderung an das Endgerät
- Teil 5: Bezahlungsmethoden
- Teil 6: Leistungsmerkmale
- Teil 7: Sicherheitsmodul

## 1 Anwendungsbereich

Dieser Teil der EN 726 legt einen Sicherheitsrahmen für den Einsatz von Chipkarten im Telekommunikationsbereich fest. Diese Festlegung beschreibt jedoch keine Einzelheiten der Durchführung.

Sie beschreibt:

- einen allgemeinen, zu einer Methodik führenden Sicherheitsansatz, unterschiedliche Kartenstadien zur Identifizierung von Sicherheitsanforderungen und eine Beschreibung von Sicherheitsdiensten, die von der Chipkarte angeboten werden können;
- die Umsetzung des allgemeinen Sicherheitsansatzes in eine anwendungsunabhängige Chipkarte. Dies führt zu einer Liste von anwendungsunabhängigen Sicherheitsanforderungen, einer Auswahl von notwendigen Sicherheitsdiensten und einer Beschreibung von gemeinsamen anwendungsunabhängigen Sicherheitsmechanismen;
- die Umsetzung des allgemeinen Sicherheitsansatzes in Anwendungen, bei denen Chipkarten zum Einsatz kommen. Dies führt zu einer Methodik, die zur Gestaltung der für spezielle Anwendungen benötigten Sicherheitsmechanismen benutzt wird.

## 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 und Überarbeitungen dieser Publikation 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

Anforderungen an Chipkarten und Endgeräte für Telekommunikationszwecke – Teil 1: Systemüberblick

EN 726-3 : 1994

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

prEN 726-7 : 1994

Chipkarten und Endgeräte für Telekommunikationszwecke – Teil 7: Sicherheitsmodul

EN 27498 : 1989

Informationsverarbeitungssysteme – Kommunikation offener Systeme – Basis-Referenzmodell

ISO 7498-2 : 1989

Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

ISO/IEC 9798-2

Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms

ISO 9798-3

Information technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm

ISO 10202-1 : 1991

Financial transaction cards – Security architectures of financial transaction systems using integrated circuit cards – Part 1: Card life cycle

## 3 Definitionen und Abkürzungen

### 3.1 Definitionen

Im Sinne dieses Teiles der EN 726 gelten folgende Definitionen:

**3.1.1 Information zur Zugangskontrolle:** Information, die die Bedingungen für jede Aktion beschreibt, welche die Karte in einer bestimmten Datei ausüben kann.

**3.1.2 Aktion:** Eine Aktion, die von einer externen Applikation auf einer Karte vollzogen werden kann, ist ein Befehl, gefolgt von einer Reaktion. Es gibt zwei Arten von Aktionen: normale Aktionen in Dateien auf der Karte (wie z. B. Lesen, Schreiben, Auswählen, Ausführen, Ungültigmachen, Wiederherstellen usw.) und Management-Aktionen in Dateien auf der Karte (z. B. Erzeugen, Löschen, Erweitern usw.).

**3.1.3 Applikation:** Eine Applikation besteht aus einer Reihe von Sicherheitsmechanismen, Dateien, Daten und Protokollen (außer Übertragungsprotokollen), welche in sowie außerhalb der Chipkarte (externe Applikation) angesiedelt sind und benutzt werden.

**3.1.4 Vorzugsinformation der Applikation:** Fähigkeiten der externen Applikation, die benutzt werden, um die Rechte der externen Applikation auszuüben.

**3.1.5 Applikationsausstatter:** Die Instanz, die nach der Einrichtung der Applikation dafür verantwortlich ist. Ein Ausstatter kann durchaus mehrere Applikationen auf einer Karte haben. Die einer Anwendung entsprechenden Dateien in der Karte werden Kartenapplikation genannt. In einer Karte können mehrere Anwendungen ein und desselben Applikationsausstatters vorhanden sein.

**3.1.6 Karte:** Eine multi-applikative Karte kann als eine Vielzahl von Dateien aufgefaßt werden, wobei einige der Dateien von mehreren Ausstattern und/oder Karten-Herausgebern gemeinsam, andere dagegen ausschließlich von einem Ausstatter und/oder Karten-Herausgeber benutzt werden. Die Dateien können beispielsweise gelesen, beschrieben oder ausgeführt werden. Die Dateien auf der Karte, die einem Ausstatter zugeordnet sind, werden Kartenapplikation genannt.

**3.1.7 Kartenapplikation:** Der sich auf die Karte beziehende Teil einer Applikation.

**3.1.8 Kartenausgeber:** Der Herausgeber der Karte ist verantwortlich für die allgemeinen Daten auf der Karte und für die Zuweisung des Speichers an die einzelnen Applikationen, und er versorgt die Ausstatter der Karte mit den Instrumenten, die zum Laden der jeweiligen Applikation benötigt werden.

**3.1.9 Kartenhersteller:** Der Hersteller der Karte ist derjenige, der die Karte produziert und den Chip darin einbettet.

**3.1.10 Externe Applikation:** Derjenige, der in der Außenwelt angesiedelt ist und mit der betreffenden Kartenapplikation kommuniziert.

**3.1.11 Außenwelt:** Alle mit Bezug zur Karte außerhalb der Karte.

**3.1.12 Kern:** Teil der Karte oder der Außenwelt, welcher applikationsunabhängige Daten / Codes beinhaltet, einschließlich MF (im Falle eines Kartenkerns) und Betriebssystem.

**3.1.13 Betriebssystem:** Das System, welches benötigt wird, um die logischen Ressourcen des Systems einschließlich der Prozeßsteuerung und des Dateien-Managements zu bewältigen.

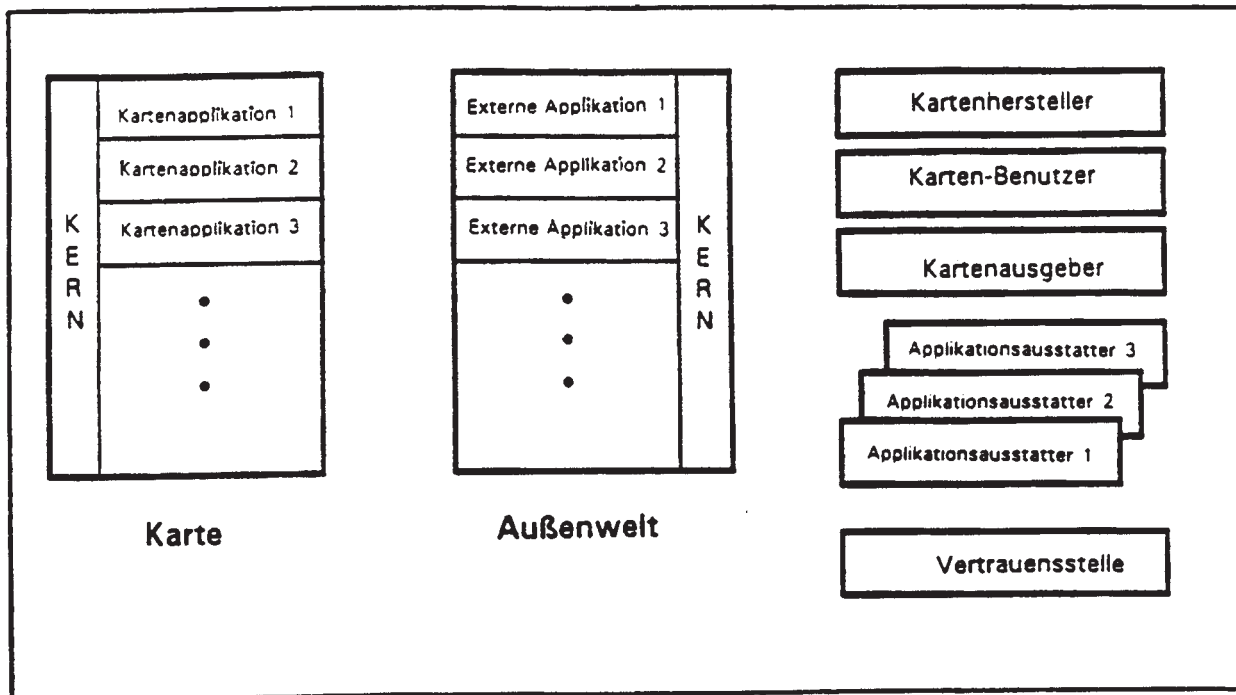


Bild 1: Bezugsmodell

**3.1.14 Protokoll-Kontrollinformation (PCI = Protocol Control Information):** Ein Informationsaustausch zwischen Applikations-Einheiten, die Übertragungsprotokolle zur Koordination der gemeinsamen Unternehmung benutzen.

**3.1.15 Eingriffe:** Die Vornahme nicht autorisierter Änderungen, welche die richtige Funktionsweise der Karte in der Weise verändert, daß die Sicherheit herabgesetzt wird.

**3.1.16 Vertrauensstelle:** Eine unabhängige Stelle, die vom Standpunkt der Sicherheit Richtlinien festlegt und das System überwacht.

## 3.2 Abkürzungen

Für diesen Teil der EN 726 gelten folgende Abkürzungen:

- AC** Zugangsbedingungen (= Access Conditions)
- ACI** Information zur Zugangskontrolle (= Access Control Information)
- API** Vorzugsinformation der Applikation (= Application Privilege Information)
- CHV** Kartenbesitzer-Überprüfung (= Card Holder Verification)
- EF** Elementardatei (= Elementary File)
- EW** Außenwelt (= External World)
- IC** Integrierte Schaltung (= Integrated Circuit)
- MF** Stammdatei (= Master File)
- PIN** Persönliche Geheimzahl (= Personal Identification Number)

## 4 Bezugsmodell

Das Bezugsmodell wird an dieser Stelle eingebracht, da es in den folgenden Abschnitten gebraucht wird.

Die folgenden Einheiten werden im Bild 1 zur Beschreibung des Bezugsmodells benutzt:

- die Karte, die aus dem Kern und einer oder mehreren Kartenapplikationen besteht (Kartenapplikation 1, Kartenapplikation 2, Kartenapplikation 3 ...);

- die Außenwelt, welche entweder ein On-line- oder auch ein Off-line-System sein kann (siehe EN 726-1). Die Außenwelt besteht auch aus einem Kern und einem oder mehreren externen Applikationen (externe Applikation 1, externe Applikation 2, externe Applikation 3 ...). In diesem Zusammenhang hat der Kern der Außenwelt beispielsweise die Funktion der Übertragung von und zur Karte sowie die Unterstützung der applikationsunabhängigen Aktionen. Sicherheitsdienste der Außenwelt können in den Sicherheitsmodulen enthalten sein;

- der Kartenhersteller (in diesem Modell sind sowohl der Chip- als auch der Kartenhersteller gemeint);
- der Benutzer der Karte;
- der Ausgeber der Karte, der gleich dem Applikations-Ausstatter sein kann;
- ein oder mehrere Applikations-Ausstatter;
- als Option eine Vertrauensstelle.

## 5 Allgemeiner Sicherheitsansatz

Dieser Abschnitt beschreibt den allgemeinen Ansatz zur Einrichtung von Sicherheit in einer Umgebung, in der Karten und Kartenterminals benutzt werden.

### 5.1 Methodik

Die Methodik besteht aus drei Schritten (siehe ISO 7498-2). Im ersten Schritt werden bestimmte Anforderungen formuliert, die vom System zu erfüllen sind, damit es sicher betrieben werden kann. Im nächsten Schritt werden Sicherheitsdienste zur Erfüllung jeder Anforderung festgelegt. Schließlich müssen die Sicherheitsmechanismen spezifiziert werden, die die zuvor festgelegten Sicherheitsdienste umsetzen.

### 5.2 Festlegung der Sicherheitsanforderungen

Um alle vom System zu erfüllenden Sicherheitsanforderungen in bezug auf Karte und Kartenterminal festlegen zu können, damit es sicher funktioniert, unterscheidet man fünf verschiedene Lebenszyklusphasen (siehe ISO 10202-1).

Jede dieser Phasen wird durch die darin stattfindenden Aktivitäten beschrieben.

ANMERKUNG: Im Laufe des Lebenszyklus der Karte können einzelne Phasen für jede Karte mehrmals auftreten.

### 5.2.1 Herstellung von Chip und Chipkarte (Phase 1)

Die erste Phase ist gekennzeichnet durch

- das Halbleiter-Design des IC (integrierte Schaltung) und die Softwareentwicklung des Betriebssystems;
- den Transport des Betriebssystems zum Hersteller des IC;
- die Halbleiterherstellung des IC;
- die Assemblierung des IC sowie den Transport des IC zum Kartenhersteller;
- die Einbettung des IC in die Karte und den Transport der Chipkarte zum Kartenausgeber.

### 5.2.2 Vorbereitung der Karte (Phase 2)

Die zweite Phase ist gekennzeichnet durch

- die Personalisierung der Karte: Zuteilung und Personalisierung des MF, das Laden der applikationsunabhängigen Daten, Funktionen und Schlüssel;
- die Aktivierung des MF;
- die Verteilung der Karten an die Applikations-Ausstatter.

Der Ausgeber der Karten ist für die Phase der Vorbereitung der Karte verantwortlich.

### 5.2.3 Vorbereitung der Applikation (Phase 3)

Die dritte Phase ist durch fünf Unterphasen gekennzeichnet:

- die Zuteilung der Applikationen unter der Verantwortung des Kartenausgebers. Dies beinhaltet die Zuteilung von Speicherplätzen im Speicher des IC;
- Zuteilung einiger Schlüssel für ausschließliche Benutzung in bestimmten Funktionen (applikationsabhängig);
- die Personalisierung der Applikationen. Dieser Prozeß beinhaltet das Laden der applikationsbezogenen Schlüssel und Daten in die zugeteilten Speicherplätze (einschließlich Fernladen);
- die Aktivierung einer Applikation;
- den Transport der Chipkarte zum Benutzer.

Die Personalisierung und Aktivierung von Applikationen werden auf Verantwortung des Applikations-Ausstatters, der auch Ausgeber der Karte sein kann, durchgeführt.

### 5.2.4 Benutzung (Phase 4)

Die vierte Phase ist gekennzeichnet durch

- den Gebrauch der allgemeinen Kartenfunktionen für den Zugang zu einzelnen Applikationen. Während der Benutzung ist die Karte in der Kontrolle des Kartenbenutzers;
- die Deaktivierung und Aktivierung einer Applikation, unter der Kontrolle des Applikations-Ausstatters;
- die Deaktivierung und Aktivierung von Dateien auf der Ebene des MF, unter der Kontrolle des Kartenausgebers;
- den Wechsel der Schlüssel-Version für eine Applikation, in der Verantwortung des Applikations-Ausstatters;
- den Wechsel der Schlüssel-Version auf der Ebene des MF, unter der Kontrolle des Kartenausgebers.

### 5.2.5 Beendigung der Benutzung (Phase 5)

Die fünfte Phase ist gekennzeichnet durch

- die Beendigung einer Kartenapplikation, in der Verantwortung des Applikations-Ausstatters. Eine einmal beendetete Applikation kann nicht wieder aktiviert werden;

- die Beendigung der Benutzung der ganzen Karte, in der Verantwortung des Kartenausgebers.

## 5.3 Allgemeine Sicherheitsdienste

Dieser Unterabschnitt beschreibt alle möglichen Sicherheitsdienste, die die Chipkarte bieten kann.

Hier werden ausschließlich technische Sicherheitsdienste in Bezug zu Chipkarte und Außenwelt beschrieben. Organisatorische Sicherheitsmaßnahmen und andere Methoden, die zur Erfüllung der Sicherheitsprinzipien notwendig sind, sind nicht Bestandteil dieser Norm.

### 5.3.1 Zugangskontrolle

Die Funktion der Zugangskontrolle bietet einen Schutz gegen unberechtigte Zugriffe auf Informationen oder Prozesse auf der Karte.

Der Schutz wird für Operationen, wie beispielsweise Lesen, Schreiben, Löschen, Erzeugen und Ausführen, gewährt.

### 5.3.2 Überprüfung der Echtheit

Es werden die folgenden Überprüfungen unterschieden:

a) Überprüfung der Echtheit des Datenursprungs unter der Angabe, daß die Identität der Quelle der empfangenen Daten den Angaben entspricht:

- 1) Die Karte liefert den Beweis dafür, daß sie die Quelle der gesendeten Daten ist;
- 2) die Karte bestätigt den Ursprung der empfangenen Daten.

b) Überprüfung der Echtheit der Teilnehmer zueinander unter der Angabe, daß die Identität in einer Verbindung den Angaben entspricht:

- 1) Überprüfung von Kartenapplikation zu Kartenbenutzer (z. B. Name oder Logo);
- 2) Überprüfung von Kartenbenutzer zu Karte;
- 3) Überprüfung von Kartenbenutzer zu Außenwelt über die Karte
- 4) Überprüfung von Kartenapplikation zu Außenwelt sowie von Kern zu Außenwelt;
- 5) Überprüfung von Außenwelt zu Karte;
- 6) Überprüfung von Kartenapplikation zu Kartenapplikation (zwischen zwei Applikationen auf derselben Karte durch die Außenwelt).

### 5.3.3 Vertraulichkeit

Diese Funktion bietet Schutz gegen die unberechtigte Verfügbarkeit oder Offenlegung von Informationen.

Die folgenden Funktionen werden diesbezüglich unterschieden:

- a) Daten in der Übertragung, d. h. Daten, die an und von der Karte gesendet werden;
- b) gespeicherte Daten, d. h. Daten, die auf der Karte gespeichert sind. Diese Daten können sein:
  - Daten des Benutzers;
  - Protokoll-Kontrollinformationen (PCI), z. B. Befehle, Adressen.

### 5.3.4 Fälschungsschutz

Diese Funktion bietet Schutz gegen unberechtigtes Verändern oder Löschen von Informationen.

Es können die folgenden Funktionen unterschieden werden:

- a) Daten in der Übertragung, d. h. Daten, die an die und von der Karte gesendet werden;
- b) gespeicherte Daten, d. h. Daten, die auf der Karte gespeichert sind (z. B. Schutz des Programmcodes). Diese Daten können sein:

- Daten des Benutzers;
- Protokoll-Kontrollinformationen (PCI), d. h. Befehle, Adressen.

### 5.3.5 Nicht-Zurückweisung

Diese Funktion bietet Schutz gegen das Abstreiten einer der am Kommunikationsprozeß beteiligten Parteien, an einem Teil oder auch am ganzen Kommunikationsprozeß teilgenommen zu haben.

Hier werden folgende Funktionen unterschieden:

- a) Nicht-Zurückweisung mit Beweis des Ursprungs: Der Empfänger von Daten (Karte oder Außenwelt) wird mit dem Beweis der Echtheit des Datenursprungs ausgestattet. Dies soll gegen jeden späteren Behauptungsversuch des Senders schützen, die Daten oder ihren Inhalt niemals abgeschickt zu haben.
- b) Nicht-Zurückweisung mit Beweis des Empfangs: Der Sender der Daten (Karte oder Außenwelt) wird mit dem Beweis des Datenempfangs ausgestattet. Dies soll gegen jeden späteren Behauptungsversuch des Systems schützen, die Daten oder ihren Inhalt niemals erhalten zu haben.

### 5.3.6 Prüffunktion

Die Prüffunktion bietet die Möglichkeit, Verletzungen der Sicherheit durch eine nachfolgende Sicherheitsüberprüfung aufzuspüren und zu untersuchen. Eine solche Sicherheitsüberprüfung besteht aus einer unabhängigen Nachprüfung und Untersuchung der Aufzeichnungen und Aktivitäten des Systems, um die Angemessenheit der Systemkontrollen zu testen. Dies wird durchgeführt, um die Befolgung der bestehenden Vorgehensweise und der Betriebsvorschriften zu gewährleisten.

Diese Überprüfung kann auch zu Verantwortlichkeitszwecken benutzt werden, d. h. zur Ermittlung des richtigen Benutzers für die korrekte Rechnungsstellung in Anspruch genommener Dienste.

## 5.4 Allgemeine Sicherheitsmechanismen

In dieser Norm werden nicht alle möglichen Sicherheitsmechanismen, die die Karte zu bieten hat, beschrieben. Eine Beschreibung der häufigsten Sicherheitsmechanismen ist in ISO 7498-2 zu finden.

## 6 Applikationsunabhängige Sicherheit

In diesem Abschnitt wird beschrieben, wie der Allgemeine Sicherheitsansatz auf die applikationsunabhängige Telekommunikations-Chipkarte anzuwenden ist.

### 6.1 Applikationsunabhängige Sicherheitsanforderungen

Dieser Unterabschnitt beschreibt die für alle Telekommunikations-Chipkarten relevanten applikationsunabhängigen Sicherheitsanforderungen. In den applikationsspezifischen Teilen dieser Norm werden die applikationsspezifischen Sicherheitsanforderungen beschrieben. In den folgenden Unterabschnitten werden für jede Phase des Karten-Lebenszyklus neben den Anforderungen auch die Verbindungen und Beziehungen zwischen den Beteiligten aufgezeigt.

Der Ausgeber der Karte ist für den Lebenszyklus der Karte, das Laden des Kerns (applikationsunabhängige Daten) auf die Karte sowie die Zuteilung der verschiedenen Applikationen auf der Karte verantwortlich. Sobald die Applikationen ihren Platz auf der Karte zugewiesen bekommen haben, werden sie vom Applikations-Ausstatter oder einer Vertrauensstelle kontrolliert (siehe detailliertes Beispiel im Anhang B der EN 726-3 : 1994).

Die im folgenden aufgelisteten Anforderungen werden für jede der fünf Phasen des Karten-Lebenszyklus beschrieben, so wie in EN 726-1 definiert.

ANMERKUNG 1: Die Reihenfolge der nachfolgend beschriebenen Phasen kann durchaus von der im Lebenszyklus der Karte abweichen.

ANMERKUNG 2: Die Durchnummerierung der verschiedenen Bindeglieder in den Darstellungen soll keine chronologische Reihenfolge abbilden.

### 6.1.1 Herstellung von Chip und Chipkarte (Phase 1)

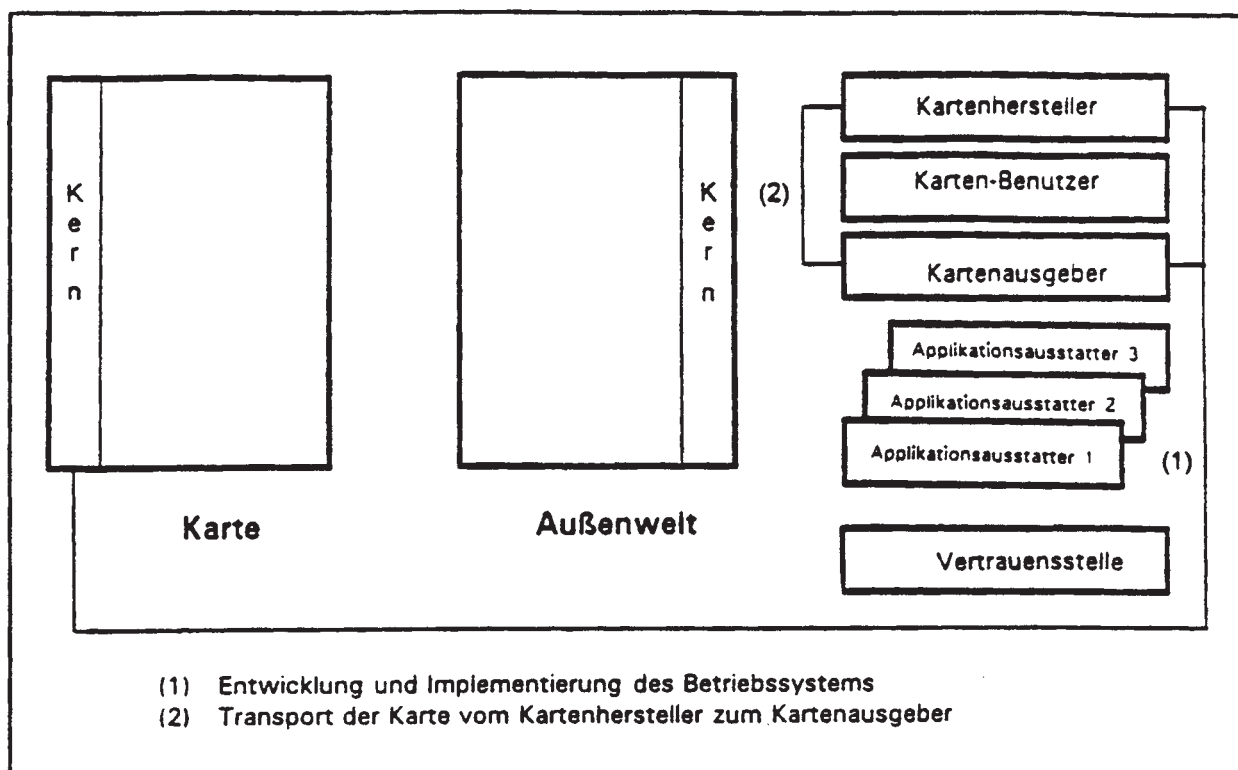


**Bild 2: Bezugsmodell für die Phasen der Herstellung von Chip und Chipkarte**

In bezug auf die Phase der Herstellung der Karte (z. B. unter Zuhilfenahme der Vertrauensstelle) müssen folgende Anforderungen berücksichtigt werden:

- a) Die Herstellung von Chip und Chipkarte muß in der Weise geschehen, daß die Beeinträchtigung der Implementierung einer Chipkarte nicht die einer anderen beeinträchtigt.
- b) Alle Prozesse sollen in einer sicheren Umgebung stattfinden unter Benutzung sicherer Maschinen, wo die vertrauliche Behandlung von Privatdaten auch gewährleistet ist.
- c) Die Chipkarte muß physikalisch und logisch sicher sein, um unbefugte Eingriffe zu vermeiden und die physikalische und logische Integrität der Daten und der Kodierung im Speicher des Chips aufrechtzuhalten.
- d) Das Kopieren von Original-Chipkarten soll nicht möglich sein.
- e) Das Betriebssystem im Chip soll keine unerlaubten Funktionen beinhalten (z. B. Trojanisches Pferd <sup>1)</sup>).
- f) Das Betriebssystem im Chip soll so implementiert sein, daß es eine ausführliche Suche nach dem CHV-Wert nicht ermöglicht.
- g) Das Betriebssystem im Chip gewährleistet, daß gelöschte Daten nicht wiederhergestellt werden können.
- h) Die reelle bzw. Pseudo-Zufallserzeugung wird so gesichert sein, daß Wiedergabeversuche unmöglich sind. Ein möglicher Eingriff soll den Zufallsgenerator nicht in einem vorhersagemöglichen Zustand lassen.
- i) Die Lagerung und der Transport der Chips und Chipkarten sollen physikalisch bzw. verschlüsselt gesichert sein.
- j) Herstellungsdaten werden im Chip sicher gespeichert.

<sup>1)</sup> Trojanisches Pferd: Ein Trojanisches Pferd hat bei der Einführung in das System neben seiner berechtigten auch eine unberechtigte Funktion. Zum Beispiel ist eine erneute Abspielung, welche Nachrichten auch zu einem unberechtigten Kanal überträgt, ein Trojanisches Pferd (siehe ISO 7498-2).

### 6.1.2 Vorbereitung der Karte (Phase 2)

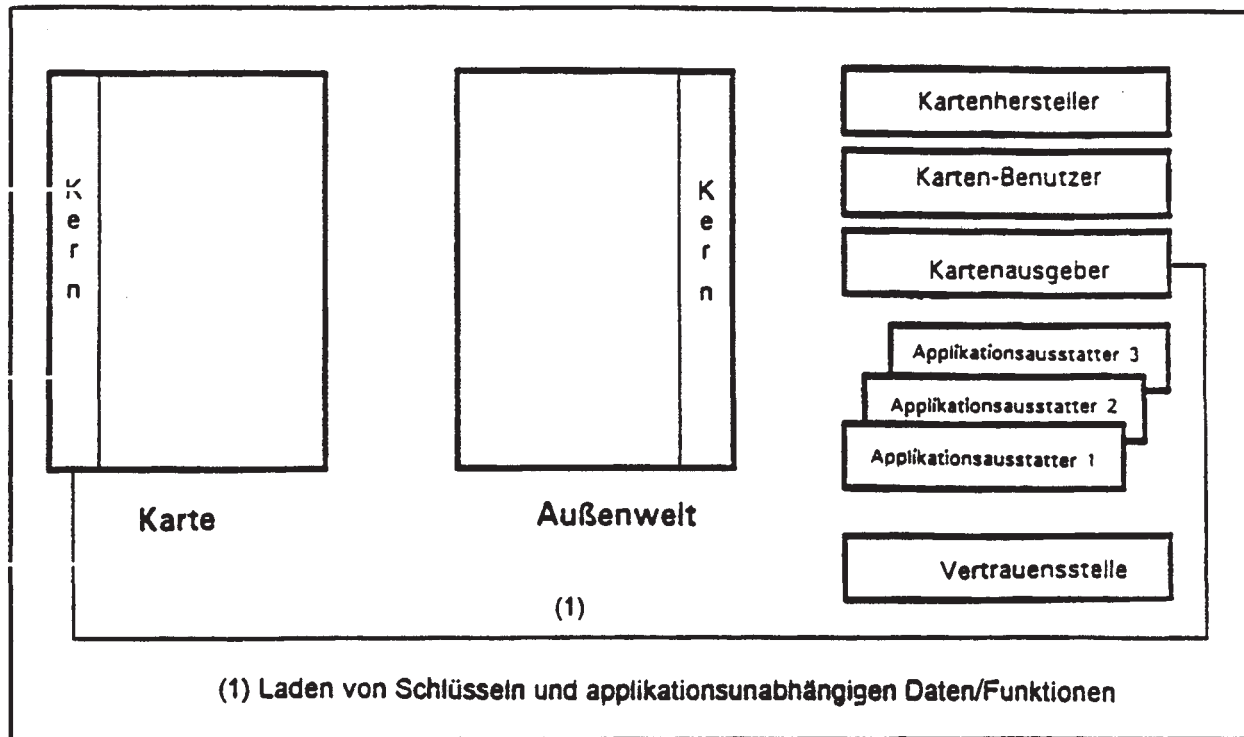


Bild 3: Bezugsmodell für die Phase der Kartenvorbereitung

In bezug auf die Phase der Vorbereitung der Karte müssen die folgenden Anforderungen berücksichtigt werden:

- Die Personalisierung der Karte soll in der Weise geschehen, daß die Beeinträchtigung der Implementierung einer Chipkarte nicht die irgendeiner anderen beeinträchtigt.
- Das Laden von applikationsunabhängigen Daten und Funktionen soll auf sichere Weise geschehen.
- Das Kopieren von Originalkarten soll nicht möglich sein.

### 6.1.3 Vorbereitung der Applikation (Phase 3)

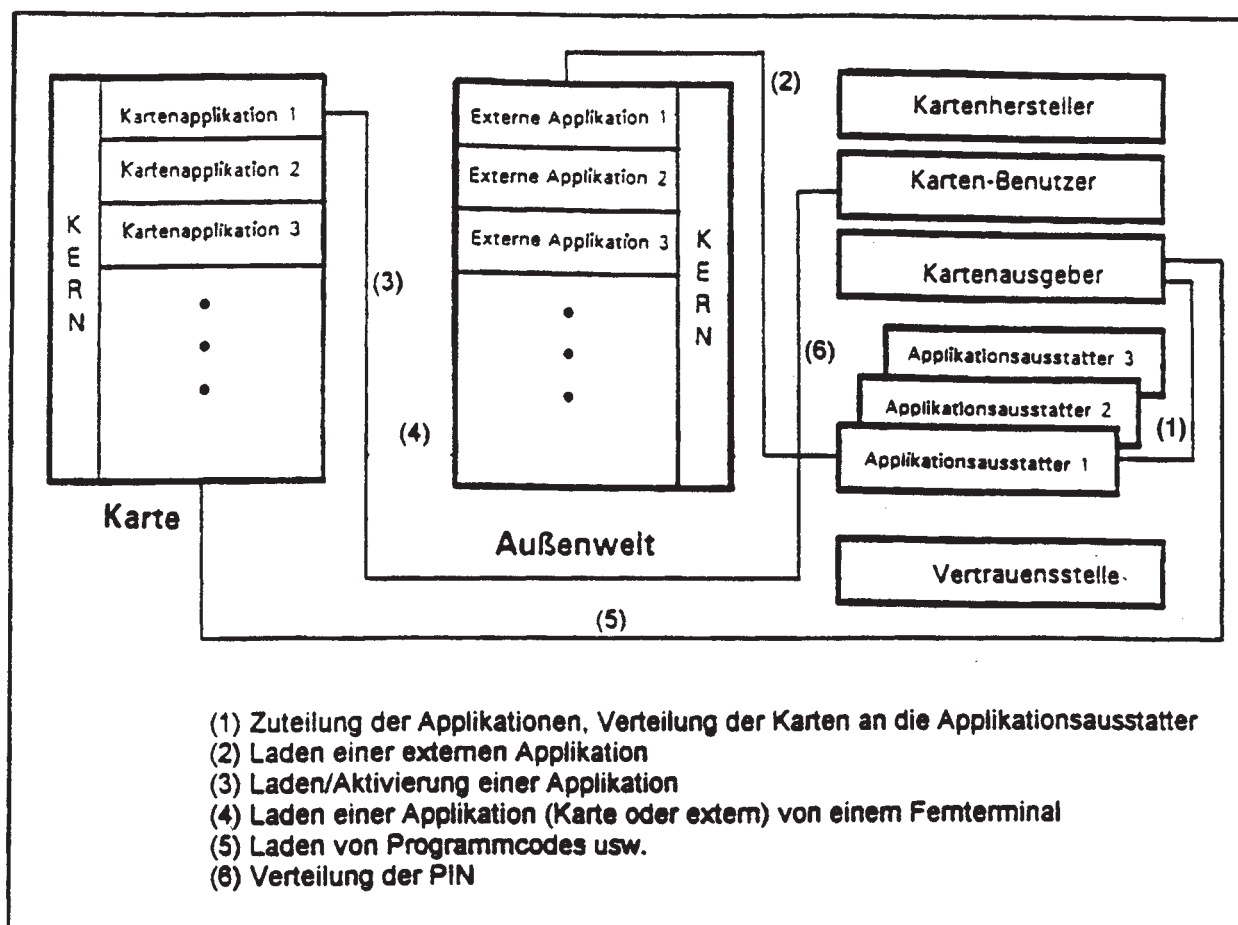


Bild 4: Bezugsmodell für die Phase der Vorbereitung der Applikation

Das Laden der externen Applikation parallel zur Vorbereitung der Chipkarte für die Applikation kann als Bestandteil dieser Phase angesehen werden.

Für jede der drei Phasen (Zuteilung, Personalisierung und Aktivierung) bei der Vorbereitung der Applikation müssen die folgenden Anforderungen berücksichtigt werden:

#### Zuteilung:

- a) Der auf der Karte vorhandene Speicherplatz wird unter der Kontrolle des Kartenausgebers den spezifischen Applikations-Ausstattern zugeteilt, und die Karten werden auf sicherem Wege an die Applikations-Ausstatter verteilt.
- b) Der einmal einem Applikations-Ausstatter zugeteilte Speicherplatz kann von keinem anderen Applikations-Ausstatter verwendet werden.

#### Personalisierung:

- c) Unter der Verantwortung des Applikations-Ausstatters werden applikationsspezifische Schlüssel und Daten in den dafür zugeteilten Platz des Chip-Speichers auf sichere Weise geladen.
- d) Die applikationsspezifische PIN, falls vorhanden, wird vom Applikations-Ausstatter erzeugt und sicher zum Kartenbenutzer transportiert.
- e) Falls an irgendeiner Stelle ein Programmcode in die Karte eingegeben werden muß, ist der Ausgeber der Karte dafür verantwortlich. Womöglich wird eine Vertrauensstelle für die Beglaubigung des Programmcodes eingeschaltet. Das Laden geschieht auf sichere Weise.

#### Aktivierung:

- f) Die Aktivierung der Kartenapplikation kann zur gleichen Zeit oder auch nach der Personalisierung durchgeführt werden, stets wird sie jedoch auf sichere Weise durchgeführt.

#### Allgemein:

- g) Die Vorbereitung einer Applikation muß in der Weise geschehen, daß die Beeinträchtigung der Implementierung einer Chipkarte nicht die einer anderen beeinträchtigt.
- h) Das Kopieren von Originalkarten soll nicht möglich sein.
- i) Ein Applikations-Ausstatter hat weder Zugang zu Informationen anderer Applikations-Ausstatter, des Kartenausgebers oder des Kartenbenutzers (Privatdaten), noch darf er diese verändern, offenlegen oder löschen.
- j) Ein Applikations-Ausstatter darf keine andere Applikation auf der Karte blockieren oder Speicherplatz, der einer anderen Applikation zugeteilt ist, entfernen oder zuteilen.