

Identifikationskartensysteme
**Anforderungen an Chipkarten und Endgeräte
für Telekommunikationszwecke**
Teil 3: Applikationsunabhängige Anforderungen an die Karte
Deutsche Fassung EN 726-3:1994

DIN
EN 726-3

ICS 33.120.00; 35.240.60

Deskriptoren: Identifikationskarte, Chipkarte, Endgerät, Telekommunikation, Informationsverarbeitung

Identification card systems –

Telecommunications integrated circuit(s) cards and terminals –

Part 3: Application independent card requirements;

German version EN 726-3:1994

Systèmes de cartes d'identification –

Cartes à circuit intégré et terminaux pour les télécommunications –

Partie 3: Spécifications de la carte indépendantes des applications;

Version allemande EN 726-3:1994

Die Europäische Norm EN 726-3:1994 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 in Abschnitt 2 zitierten Internationalen Normen wird im folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO 9564-1 siehe DIN EN 29564-1

ISO 9564-2 siehe DIN EN 29564-2

ISO 9992-1 siehe DIN EN 29992-1

ISO 10202-1 siehe DIN EN 30202-1

Nationaler Anhang (informativ)

Literaturhinweise in nationalen Zusätzen

DIN EN 29564-1 Bankwesen – PIN-Ausgabe und -Verwaltung und PIN-Sicherheit – Teil 1: Grundsätze und Verfahren zum Schutz der PIN (ISO 9564-1:1991); Englische Fassung EN 29564-1:1993

DIN EN 29564-2 Bankwesen – PIN-Ausgabe und -Verwaltung und PIN-Sicherheit – Teil 2: Anerkannte Algorithmen zur PIN-Verschlüsselung (ISO 9564-2:1991); Englische Fassung EN 29564-2:1993

DIN EN 29992-1 Bankkarten – Nachrichten zwischen IC-Karte und Kartenendgerät – Teil 1: Grundsätze und Aufbau (ISO 9992-1:1990); Deutsche Fassung EN 29992-1:1993

DIN EN 30202-1 Bankkarten – Sicherheitsarchitektur in Zahlungsverkehrssystemen für Karten mit integrierten Schaltkreisen (IC-Karten) – Teil 1: Kartenzyklus (ISO 10202-1:1991); Deutsche Fassung EN 30202-1:1993

Fortsetzung 62 Seiten EN

Normenausschuß Informationstechnik (NI) im DIN Deutsches Institut für Normung e.V.

ICS 33.120.00; 35.240.60

Deskriptoren: Telekommunikation, Chipkarte, Endgeräte für Telekommunikation, Anforderungen, Eigenschaften

Deutsche Fassung

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

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

Diese Europäische Norm wurde von CEN am 1994-12-05 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	7.3 Kanalunterstützung	12
1 Anwendungsbereich	3	7.4 Verfahren zum Beenden der Applikation	12
2 Normative Verweisungen	4	7.5 Sicherheitsumgebung	12
3 Begriffe, Abkürzungen und Symbole	5	7.6 Allgemeine Beschreibung der Sicherheitsfunktionen	12
3.1 Begriffe	5	7.6.1 Mit Zugriffsbedingungen verknüpfte Sicherheitsfunktionen	13
3.1.1 Zugriffsbedingungen (AC)	5	7.6.2 Sicherheitsfunktionen in Verbindung mit der markierten Betriebsart	13
3.1.2 Zuweisbarer Speicher	5	7.6.3 Externe Authentifizierung (Echtheitsüberprüfung)	13
3.1.3 Anwendung (Applikation)	5	7.6.4 Interne Authentifizierung	13
3.1.4 Anwendungssitzung (Application session)	5	7.6.5 Algorithmus-Kennung	13
3.1.5 Applikationsspezifischer Befehlssatz (ASC)	5	8 Beschreibung der Funktionen	14
3.1.6 Anwendungsanbieter (AP)	5	8.1 SELECT	14
3.1.7 Karte	5	8.2 STATUS (Zustand)	15
3.1.8 Kartensitzung (Card session)	5	8.3 CREATE FILE	15
3.1.9 Aktuelles Verzeichnis	5	8.4 DELETE FILE	15
3.1.10 Aktuelle EF	5	8.5 EXTEND	15
3.1.11 Aktuelle Datei	5	8.6 EXECUTE	15
3.1.12 Zugeordnete Datei (DF)	5	8.7 UPDATE BINARY	16
3.1.13 Verzeichnis	5	8.8 UPDATE RECORD	16
3.1.14 Elementare Datei (Elementary file) (EF)	5	8.9 CREATE RECORD	16
3.1.15 Datei-Kennzeichen (ID)	5	8.10 READ BINARY	17
3.1.16 Datei-Unterkennzeichen	5	8.11 READ BINARY STAMPED	17
3.1.17 Version der Schlüsseldatei	5	8.12 READ RECORD	17
3.1.18 Hauptdatei (MF)	5	8.13 READ RECORD STAMPED	17
3.1.19 Betriebssystem	5	8.14 SEEK	17
3.1.20 Auffüllen	6	8.15 VERIFY CHV	18
3.1.21 Pfad	6	8.16 CHANGE CHV	18
3.1.22 Muster	6	8.17 DISABLE CHV	18
3.1.23 Datensatz	6	8.18 ENABLE CHV	19
3.1.24 Datensatznummer	6	8.19 UNBLOCK CHV	19
3.2 Abkürzungen	6	8.20 INVALIDATE	19
3.3 Symbole	6	8.21 REHABILITATE	19
3.4 Festlegungen	6	8.22 INTERNAL AUTHENTICATION	19
4 Physikalische Eigenschaften der Karte	6	8.23 ASK RANDOM	20
4.1 Anordnung	6	8.24 GIVE RANDOM	20
4.2 Temperaturbereich für den Betrieb der Karte ...	6	8.25 EXTERNAL AUTHENTICATION	20
5 Elektronische Signale und Übertragungsprotokolle	6	8.26 CLOSE APPLICATION	20
5.1 Versorgungsspannung	6	8.27 WRITE BINARY	20
5.2 Versorgungsstrom	6	8.28 WRITE RECORD	20
5.3 Programmierspannung	6	8.29 LOCK	21
5.4 Arbeitszyklus	7	8.30 DECREASE	21
5.5 Schutzzeit	7	8.31 DECREASE STAMPED	21
5.6 Betriebsart Reduzierter Energieverbrauch	7	8.32 INCREASE	22
6 Logisches Modell für Chipkarten	7	8.33 INCREASE STAMPED	22
6.1 Datei-Kennzeichen	7	8.34 LOAD KEY FILE	22
6.2 Strukturen der elementaren Datei (EF)	7	9 Beschreibung der Befehle	22
6.2.1 Transparente EF	7	9.1 Mapping-Prinzipien (Abbildungsgrundsätze)	22
6.2.2 EFs mit Programm	7	9.1.1 Befehl APDU	22
6.2.3 EF mit linear fester Struktur	7	9.1.2 Antwort APDU	22
6.2.4 EF mit linear variabler Struktur	8	9.1.3 Konventionen des Befehls APDU	23
6.2.5 EF mit zyklischer Struktur	8	9.2 Kodierung der Befehle	23
6.2.6 EFs mit ASC-Satz	8	9.2.1 SELECT	24
6.3 Inhalt der EF _{DIR}	8	9.2.2 STATUS	30
6.4 Verfahren zum Auswählen einer Datei	8	9.2.3 CREATE FILE	32
6.5 Applikationsspezifischer Befehlssatz (ASC)	8	9.2.4 DELETE FILE	33
6.6 Ungültigkeitserklärung/Rehabilitierung einer Datei	8	9.2.5 EXTEND	33
7 Sicherheitseinrichtungen für die Karte	8	9.2.6 EXECUTE	34
7.1 Zugriffsbedingungen	8	9.2.7 UPDATE BINARY	34
7.1.1 Grundbedingungen und Kombinationen von Bedingungen	10	9.2.8 UPDATE RECORD	34
7.1.2 EF, in der die geheimen Schlüssel enthalten sind	10	9.2.9 CREATE RECORD	34
7.1.3 EF, in der die CHVs enthalten sind	10	9.2.10 READ BINARY	35
7.1.4 Dateizugriffsbedingungen	10	9.2.11 READ BINARY STAMPED	35
7.2 Anwendbare Funktionen bei unterschiedlichen EF-Arten	12	9.2.12 READ RECORD	35
		9.2.13 READ RECORD STAMPED	36
		9.2.14 SEEK	36

	Seite		Seite		
9.2.15	VERIFY CHV	37	9.4.5	Antworten auf Befehle, die ordnungsgemäß ausgeführt wurden oder den Chaining-Mechanismus unterstützen	48
9.2.16	CHANGE CHV	37	9.4.6	Mögliche Statusantwort bei Befehlen	49
9.2.17	DISABLE CHV	37	10	Inhalt von besonderen EFs	50
9.2.18	ENABLE CHV	38	10.1	EF _{CHV}	51
9.2.19	UNBLOCK CHV	38	10.2	EF _{DIR}	51
9.2.20	INVALIDATE	38	10.3	EF _{IC}	52
9.2.21	REHABILITATE	39	10.4	EF _{ICC}	53
9.2.22	INTERNAL AUTHENTICATION	39	10.5	EF _{ID}	56
9.2.23	ASK RANDOM	39	10.6	EF _{KEY_MAN}	57
9.2.24	GIVE RANDOM	40	10.7	EF _{KEY_OP}	58
9.2.25	EXTERNAL AUTHENTICATION	40	10.8	EF _{LANG}	58
9.2.26	CLOSE APPLICATION	40	10.9	EF _{NAME}	59
9.2.27	WRITE BINARY	40	11	Kompatibilität von Chipkarten	59
9.2.28	WRITE RECORD	41	11.1	Genormte Anwendungen	59
9.2.29	LOCK	41	11.2	Nicht genormte Anwendungen	59
9.2.30	DECREASE	42	12	Sicherheitsaspekte für Kartenhersteller, Anwendungsanbieter und Kartenausgeber	59
9.2.31	DECREASE STAMPED	43	12.1	Herstellungsprozeß für Chip und Karte	59
9.2.32	INCREASE	43	12.1.1	Entwicklung des Halbleiterchips und der Software	60
9.2.33	INCREASE STAMPED	44	12.1.2	Herstellung des Halbleiterchips	60
9.2.34	LOAD KEY FILE	45	12.1.3	Modulherstellung	60
9.2.35	GET RESPONSE	45	12.1.4	Chipeinbettung	60
9.2.36	ENVELOPE PUT	45	Anhang A	(informativ)	
9.3	Kodierung der Zugriffsbedingungen	45		Beispiel für das Erstellen einer Anwendung in der Karte	60
9.3.1	Generierung eines EF	46	Anhang B	(informativ)	
9.3.2	Generierung eines DF	47		Beispiele für Zertifikationsmechanismen	60
9.3.3	Generierung einer Schlüsseldatei (EF _{KEY_MAN} oder EF _{KEY_OP})	47	Anhang C	(informativ)	
9.4	Von der Karte zurückgemeldete Statusbedingungen	47		Verwaltungsmaßnahmen	61
9.4.1	Sicherheitsverwaltung	47			
9.4.2	Speicherverwaltung	48			
9.4.3	Referenzverwaltung	48			
9.4.4	Applikationsunabhängige Fehler	48			

Vorwort

Diese Europäische Norm wurde von ETSI STC-TE9 erarbeitet und vom CEN/TC 224 "Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren", dessen Sekretariat von AFNOR betreut wird, angenommen. Das CEN/TC 224 hat beschlossen, diesen Schlußentwurf zur formellen Abstimmung vorzulegen. Das Ergebnis war positiv.

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

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

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

Diese Europäische Norm unter dem Haupttitel "Identifikationskartensysteme – 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 beschreibt applikationsunabhängige Merkmale von Multiapplikations-Chipkarten und einsteckbaren Modulen (Plug in Modul) für Telekommunikationszwecke, um die Kompatibilität für Kartenanwendungen im Telekommunikationsbereich in verschiedenen Systemen und Endgeräten zu gewährleisten. Monoapplikationskarten werden als eine Teilmenge von Multiapplikationskarten angesehen. Alle gebräuchlichen Merkmale, die für die Wechselwirkungen zwischen Karte und externer Welt notwendig sind, werden definiert.

Dieser Teil der EN 726 schließt Karten aus anderen Bereichen nicht aus, die Telekommunikationsanwendungen auf der Grundlage dieses Papieres beinhalten.

Applikationsspezifische Merkmale werden in diesem Teil der EN 726 nicht definiert. Sie sind in den entsprechenden Anwendungsanforderungen festgelegt.

Auf die interne technische Realisierung wird im vorliegenden Teil der EN 726 nicht eingegangen. Dieser Teil beschreibt:

- Anforderungen an die physikalischen Eigenschaften der Karte, die elektronischen Signale und die Übertragungsprotokolle;

- das applikationsunabhängige logische Modell, das als Grundlage für die logische Struktur von wahlweise mehreren Anwendungen in der Karte verwendet werden muß;
- die Sicherheitseinrichtungen hinsichtlich des Zugriffs auf die unterschiedlichen Teile in der Karte sowie die möglichen Wechselwirkungen zwischen diesen Teilen. Ebenfalls beschrieben werden die Sicherheitsfunktionen, die im allgemeinen von den verschiedenen Applikationen angewendet werden sollten. Sie sollten als allgemeiner Datensatz verfügbar sein;
- die applikationsunabhängigen Funktionen zwischen Karte und externer Welt (Außenwelt), die als genormter Basissatz für alle Funktionen in internationalen Anwendungen benutzt werden sollten;
- die Abbildung dieser anwendungsbezogenen Meldungen (Befehle und Antworten) durch die verwendeten und genormten Protokolle;
- den Inhalt der Hauptdatei;
- die Kompatibilität von Chipkarten;
- die gesamten Sicherheitsaspekte für Kartenhersteller, Anwendungsanbieter und Kartenausgeber.

2 Normative Verweisungen

Dieser Teil der EN 726 verweist auf Festlegungen aus anderen Publikationen (mit oder ohne Datumsangabe). Die normativen Verweisungen sind an den jeweiligen Stellen im Text zitiert, und die Publikationen sind nachstehend aufgeführt. Bei Verweisungen mit Datumsangabe gelten spätere Änderungen oder Überarbeitungen dieser Publikationen für die vorliegende Norm nur dann, wenn sie als Änderung oder Überarbeitung in sie aufgenommen wurden. Bei Verweisungen ohne Datumsangabe gilt die neueste Ausgabe der zitierten Publikation.

- EN 726-1
Identifikationskartensysteme—Anforderungen an Chipkarten und Endgeräte für Kommunikationszwecke — Teil 1: Systemüberblick
- EN 726-2
Identifikationskartensysteme—Anforderungen an Chipkarten und Endgeräte für Kommunikationszwecke — Teil 2: Sicherheitsgrundgerüst¹⁾
- EN 726-4
Identifikationskartensysteme—Anforderungen an Chipkarten und Endgeräte für Kommunikationszwecke — Teil 4: Applikationsunabhängige, kartenrelevante Anforderungen an Endgeräte
- ENV 1375-1
Identifikationskartensysteme — Zusätzliche Formate von branchenübergreifenden Chipkarten — Teil 1: Kartengröße ID-000 und physikalische Eigenschaften¹⁾
- ENV 1375-2
Identifikationskartensysteme — Zusätzliche Formate von branchenübergreifenden Chipkarten — Teil 2: Kartengröße ID-00 und physikalische Eigenschaften¹⁾
- EN 27810 : 1989
Identifikationskarten — Physikalische Eigenschaften
- EN 27811-1 : 1989
Identifikationskarten — Aufzeichnungstechnik — Teil 1: Prägen von Schriftzeichen
- EN 27811-2 : 1989
Identifikationskarten — Aufzeichnungstechnik — Teil 2: Magnetstreifen
- EN 27812 : 1989
Identifikationskarten — Benummerungssystem und Registrierungsverfahren für die Kennzeichnung des Herausgebers
- EN 27816-1 : 1989
Identifikationskarten — Integrierte Schaltungen mit Kontakten — Teil 1: Physikalische Eigenschaften

- EN 27816-2 : 1989
Identifikationskarten — Integrierte Schaltungen mit Kontakten — Teil 2: Abmessungen und Lokalisation der Kontakte
- EN 27816-3 : 1992
Identifikationskarten — Integrierte Schaltungen mit Kontakten — Teil 3: Elektronische Signale und Übertragungsprotokolle
- EN 27816-3 : 1992/A1 : 1993
Identifikationskarten — Integrierte Schaltungen mit Kontakten — Teil 3: Elektronische Signale und Übertragungsprotokolle — Änderung 1: Protokolltyp T=1, Asynchrones blockorientiertes Übertragungsprotokoll im Halbduplexverfahren
- I-ETS 300045-1 : 1992
Europäisches, digitales, zellulares Telekommunikationssystem (Phase 1): Teilnehmerbezogenes Identitätsmodul — bewegliche Einrichtungen (SIM-ME) Schnittstellenbeschreibung (GSM 11.11)
- ISO 639 : 1988
Codes für die Darstellung von Sprachenbezeichnungen
- ISO/IEC 646 : 1991
Informationsverarbeitung — 7-Bit codierte Zeichensmenge für den Informationsaustausch
- ISO 3166 : 1988
Codes für die Darstellung von Ländernamen
- ISO/IEC 7816-4
Identifikationskarten — Integrierte Schaltungen mit Kontakten — Teil 4: Befehle für den Austausch zwischen Industriezweigen¹⁾
- ISO/IEC 7816-5
Identifikationskarten — Integrierte Schaltungen mit Kontakten — Teil 5: Registrierungssystem für Anwendungen mit Chipkarten¹⁾
- ISO 8859-1 : 1987
Informationsverarbeitung — 8-bit Einzel-Byte kodierter grafischer Zeichensatz — Teil 1: Lateinisches Alphabet Nr 1
- ISO 9564-1 : 1991
Bankwesen — Verwaltung und Sicherheit der Persönlichen Geheimzahl — Teil 1: Grundsätze und Techniken zum Schutz der PIN
- ISO 9564-2 : 1991
Bankwesen — Verwaltung und Sicherheit der Persönlichen Geheimzahl — Teil 2: Algorithmen
- ISO 9807 : 1991
Bankwesen — Anforderungen an die Authentifizierung einer Nachricht
- ISO 9992-1 : 1991
Bankkarten — Nachrichten zwischen einer Karte mit integriertem Schaltkreis und einem Kartenzugangsgerät — Teil 1: Begriffe und Strukturen
- ISO 9992-2
Bankkarten — Nachrichten zwischen einer Karte mit integriertem Schaltkreis und einem Kartenzugangsgerät — Teil 2: Funktionen, Nachrichten (Befehle und Antworten), Datenelemente und Strukturen
- ISO 10202-0
Bankkarten — Sicherheitsarchitekturen für finanzielle Transaktionen unter Verwendung von Karten mit integrierten Schaltkreisen — Teil 0: Systemüberblick¹⁾
- ISO 10202-1 : 1991
Bankkarten — Sicherheitsarchitekturen für finanzielle Transaktionen unter Verwendung von Karten mit integrierten Schaltkreisen — Teil 1: Lebenszyklus der Karte
- ISO 10202-2
Bankkarten — Sicherheitsarchitekturen für finanzielle Transaktionen unter Verwendung von Karten mit integrierten Schaltkreisen — Teil 2: Transaktionen¹⁾

¹⁾ Z. Z. Entwurf

ISO 10202-3

Bankkarten — Sicherheitsarchitekturen für finanzielle Transaktionen unter Verwendung von Karten mit integrierten Schaltkreisen — Teil 3: Verschlüsselungsbezeichnungen¹⁾

ISO 10202-4

Bankkarten — Sicherheitsarchitekturen für finanzielle Transaktionen unter Verwendung von Karten mit integrierten Schaltkreisen — Teil 4: Module für eine sichere Anwendung¹⁾

ISO 10202-5

Bankkarten — Sicherheitsarchitekturen für finanzielle Transaktionen unter Verwendung von Karten mit integrierten Schaltkreisen — Teil 5: Verwendung von Algorithmen¹⁾

ISO 10202-6

Bankkarten — Sicherheitsarchitekturen für finanzielle Transaktionen unter Verwendung von Karten mit integrierten Schaltkreisen — Teil 6: Karteninhaber-Verifizierung¹⁾

CCITT-Empfehlung E.118 : 1988

Automatisiertes internationales Kreditkartentelefon-System

CCITT-Empfehlung T.50 : 1988

Internationales Alphabet Nr 5

3 Begriffe, Abkürzungen und Symbole

3.1 Begriffe

Für diesen Teil der EN 726 werden die folgenden Begriffe festgelegt:

3.1.1 Zugriffsbedingungen (AC)

Menge von Sicherheitsmerkmalen für eine Datei.

3.1.2 Zuweisbarer Speicher

Speichergröße einer Datei, die momentan noch nicht zugewiesen ist.

3.1.3 Anwendung (Applikation)

Sie besteht aus einer Menge von Sicherheitsmechanismen, Dateien, Daten, Protokollen (mit Ausnahme von Übertragungsprotokollen), die in und außerhalb der Chipkarte (externe Anwendung) lokalisiert und angewendet werden.

3.1.4 Anwendungssitzung (Application session)

Verbindung zwischen den Anwendungsteilen der Karte und der externen Welt für dieselbe Anwendung.

3.1.5 Applikationsspezifischer Befehlssatz (ASC)

Mit einer DF kann wahlweise ein ASC-Satz (ein applikationsspezifischer Befehlssatz und/oder ein applikationsspezifisches Programm) verbunden werden. Das heißt, daß beim Auswählen dieser Anwendung der Basissatz durch diesen spezifischen Befehlssatz erweitert oder verändert wird. Der ASC ist für die gesamte Teilbaumstruktur der Anwendung gültig, falls es nicht andere, auf niedrigeren Stufen dieser Anwendung definierte ASCs gibt.

3.1.6 Anwendungsanbieter (AP)

Instanz, die nach erfolgter Zuordnung für die Anwendung verantwortlich ist. Ein Anwendungsanbieter darf mehrere Anwendungen in einer Karte haben. Einer Anwendung zugeordnete Dateien werden als Kartenanwendung bezeichnet. In einer Karte dürfen mehrere Anwendungen eines Anwendungsanbieters bestehen.

3.1.7 Karte

Eine Multiapplikationskarte kann als eine Menge von Dateien angesehen werden, von denen einige von unterschiedlichen Anwendungsanbietern und/oder Kartenausgebern gemeinsam genutzt werden, während andere Dateien ausschließlich den verschiedenen Anwendungsanbietern oder dem Kartenausgeber zugeordnet werden. Die Dateien können z. B. gelesen, geschrieben oder ausgeführt werden.

3.1.8 Kartensitzung (Card session)

Verbindung zwischen Karte und externer Welt, die mit ATR beginnt und mit nachfolgendem Rücksetzen oder Deaktivieren der Karte endet.

3.1.9 Aktuelles Verzeichnis

Zuletzt in der Karte ausgewähltes Verzeichnis (MF oder DF).

3.1.10 Aktuelle EF

Zuletzt in der Karte ausgewählte EF.

3.1.11 Aktuelle Datei

Zuletzt in der Karte ausgewählte Datei (MF, DF oder EF).

3.1.12 Zugeordnete Datei (DF)

Eine Datei mit AC und zuordenbarem Speicher. Die Datei kann als "Eltern" von elementaren Dateien und/oder zugeordneten Dateien auftreten.

3.1.13 Verzeichnis

Allgemeine Bezeichnung für die MF oder DF.

3.1.14 Elementare Datei (Elementary file) (EF)

Eine Datei, die AC, Daten oder ein Programm enthält. Die Datei kann nicht als "Eltern" von einer weiteren Datei auftreten.

— EF_{CHV} ist eine elementare Datei, die Informationen zur Verifizierung (Überprüfung) des Karteninhabers enthält.

— EF_{DIR} ist eine elementare Datei auf der Stufe der Hauptdatei oder der DF, die ein Verzeichnis aller oder eines Teils der in der Karte verfügbaren Anwendungen enthält (siehe ISO 7816-5 [4]).

— EF_{ID} ist eine elementare Datei auf der Stufe der Hauptdatei, die die Identifikationsnummer der Karte enthält.

— EF_{IC} ist eine elementare Datei auf der Stufe der Hauptdatei, die Informationen über den Chip (IC) enthält.

— EF_{ICC} ist eine elementare Datei auf der Stufe der Hauptdatei, die allgemeine Informationen über die ICC enthält.

— EF_{KEY_OP} ist eine elementare Datei, die Betriebs-Schlüssel enthält.

— EF_{KEY_MAN} ist eine elementare Datei, die Verwaltungs-Schlüssel enthält.

— EF_{LANG} ist eine elementare Datei auf der Stufe der Hauptdatei, auf der die bevorzugten Sprachen angegeben sind.

— EF_{NAME} ist eine elementare Datei auf der Stufe der Hauptdatei, die den Namen des Karteninhabers enthält.

3.1.15 Datei-Kennzeichen (ID)

Jede Datei hat ein Datei-Kennzeichen (file identifier), bestehend aus 2-Byte.

3.1.16 Datei-Unterkennzeichen

Erstes Byte des Datei-Kennzeichens.

3.1.17 Version der Schlüsseldatei

Zeigt die absolute Versionsnummer (BCD-kodiert) der Schlüsseldatei an.

3.1.18 Hauptdatei (MF)

Einzige zwingend vorgeschriebene Datei als Ausgangsbasis der Dateistruktur, die AC und zuordenbaren Speicher enthält. Die Hauptdatei darf als "Eltern" von elementaren Dateien und/oder zugeordnete Dateien auftreten.

3.1.19 Betriebssystem

System zur Verwaltung der logischen Ressourcen eines Systems einschließlich Prozeßplanung und Dateiverwaltung.

¹⁾ Z. Z. Entwurf

3.1.20 Auffüllen

Ein oder mehrere Bit(s), um die eine Nachricht ergänzt wird, damit sie die erforderliche Anzahl von Bits oder Bytes hat.

3.1.21 Pfad

Verkettung von Datei-Kennzeichen ohne Begrenzungen.

3.1.22 Muster

Folge von Bytes.

3.1.23 Datensatz

Folge von Bytes, die von der Karte als Einheit behandelt wird. Die Kennzeichnung erfolgt mittels einer Datensatznummer oder eines Datensatzzeigers.

3.1.24 Datensatznummer

Innerhalb einer EF sequentiell und einmalig. Sie wird durch die Karte verwaltet.

3.2 Abkürzungen

Für diesen Teil der EN 726 werden folgende Abkürzungen verwendet:

AC	Zugriffsbedingung
ALW	Always (Immer)
APDU	Anwendungsdateneinheit
ASC	Applikationsspezifischer Befehlssatz
ATR	Answer to reset (Antwort auf Zurücksetzen)
AUT	Authenticated (authentifiziert)
CHV	Card holder verification (Verifizierung des Karteninhabers)
DECT	Digitales, europäisches, schnurloses Telefon
DF	Dedicated File (dedizierte Datei)
EF	Elementary File (Elementare Datei)
etu	Elementare Zeiteinheit
IC	Integrierte Schaltung
ID	Datei-Kennzeichen
MF	Master File (Hauptdatei)
MII	Major Industry Identifier (Industrie-Hauptkennzeichen)
NEV	Never (nie)
PIN	Persönliche Identifikationsnummer
PRO	Protected (geschützt)
PTS	Protokollauswahl (Rückmeldung auf ATR)
RFU	Für zukünftige Zwecke reserviert

3.3 Symbole

Für diesen Teil der EN werden die folgenden Symbole festgelegt:

nAs	Nano Amperesekunde
ns	Nanosekunde
mA	Milliampere
MHz	Megahertz
V _{CC}	Versorgungsspannung
V _{PP}	Programmierspannung

3.4 Festlegungen

'0' bis '9' und 'A' bis 'F': die sechzehn hexadezimalen Stellen

4 Physikalische Eigenschaften der Karte

Die physikalischen Eigenschaften für das ID-1 Format müssen EN 27816-1:1989 und EN 27816-2:1989 entsprechen. Trotzdem gilt die EN 726 nicht nur für Karten des Formats ID-1, sondern auch für andere Kartenformate gemäß ENV 1375-1 und ENV 1375-2.

Die nachfolgenden zusätzlichen Anforderungen müssen eingehalten werden, um den ordnungsgemäßen Betrieb portabler batterie- als auch netzbetriebener und stationärer Geräte zu gewährleisten.

4.1 Anordnung

Die Kontakte der in Europa verwendeten Karten müssen auf folgende Weise angeordnet sein:

- die Kontakte sind auf einer beliebigen Seite anzuordnen, wenn keine geprägten Zeichen und keine Magnetstreifen vorhanden sind,
- die Kontakte liegen, wenn geprägte Zeichen vorhanden sind, auf der Seite mit den Zeichen,
- die Kontakte liegen, wenn Magnetstreifen vorhanden sind, auf der Seite ohne Magnetstreifen,
- die Kontakte befinden sich auf der Seite mit den Zeichen, wenn geprägte Zeichen und Magnetstreifen vorhanden sind.

Die Identifikationsnummer und die Kartenfolgennummer (falls vorhanden) gemäß Festlegungen der elementaren Datei EF_{ID} (siehe Abschnitt 10) können auf der Außenseite der Karte sichtbar sein (falls geprägt, dann gemäß EN 27811).

4.2 Temperaturbereich für den Betrieb der Karte

Der Temperaturbereich für den vollen Betriebseinsatz liegt zwischen - 25 °C und + 65 °C, wobei gelegentliche Spitzenwerte bis zu 70 °C zulässig sind.

Diese Werte dürfen dabei jeweils nicht länger als 4 Stunden anstehen sowie während der Lebensdauer der Karte nicht öfter als 100mal auftreten.

Für Multiapplikationskarten, die auch in portablen batteriebetriebenen Geräten verwendet werden dürfen, liegt der Temperaturbereich für den Betriebseinsatz zwischen - 25 °C und + 70 °C, wobei gelegentliche Spitzenwerte bis zu + 85 °C zulässig sind.

Diese Werte dürfen dabei jeweils nicht länger als 4 Stunden anstehen sowie während der Lebensdauer der Karte nicht öfter als 100mal auftreten.

5 Elektronische Signale und Übertragungsprotokolle

Elektronische Signale und Übertragungsprotokolle müssen EN 27816-3 entsprechen.

Die im folgenden aufgeführten zusätzlichen Anforderungen sind einzuhalten, um vereinfachte Endgeräte einzusetzen und einen ordnungsgemäßen Betrieb in mobilen Einrichtungen einschließlich portabler batterie- und netzbetriebener sowie stationärer Geräte zu gewährleisten.

5.1 Versorgungsspannung

Die Karte muß mit einer Versorgungsspannung V_{CC} von 5V ± 10 % betrieben werden.

5.2 Versorgungsstrom

Der Stromverbrauch der Karte darf 20 mA bei keiner von der Karte zugelassenen Frequenz überschreiten. Wenn damit zu rechnen ist, daß die Karte in mobilen Einrichtungen einschließlich portabler batterie- oder netzbetriebener Geräte verwendet wird, darf der Strom 10 mA bei keiner Frequenz überschreiten.

Technisch bedingt können Versorgungsstromspitzen auftreten, deren Amplitude ein Mehrfaches des mittleren Stromes betragen kann. Während des Betriebes der Karte darf eine Spitzenladung von über 40 nAs mit einer Amplitude von 200 mA keinesfalls länger als 400 ns von der Karte entnommen werden.

5.3 Programmierspannung

Eine von V_{CC} abweichende Programmierspannung muß intern erzeugt werden.

ANMERKUNG: Bei europäischen Telekommunikationskarten muß der V_{PP}-Kontakt die gleiche Spannung wie der V_{CC}-Kontakt liefern (siehe EN 726-4). Bei mobilen Geräten können besondere Bedingungen auftreten (siehe relevante Spezifikation I-ETS 300045-1 : 1992 und DECT-Spezifikation).

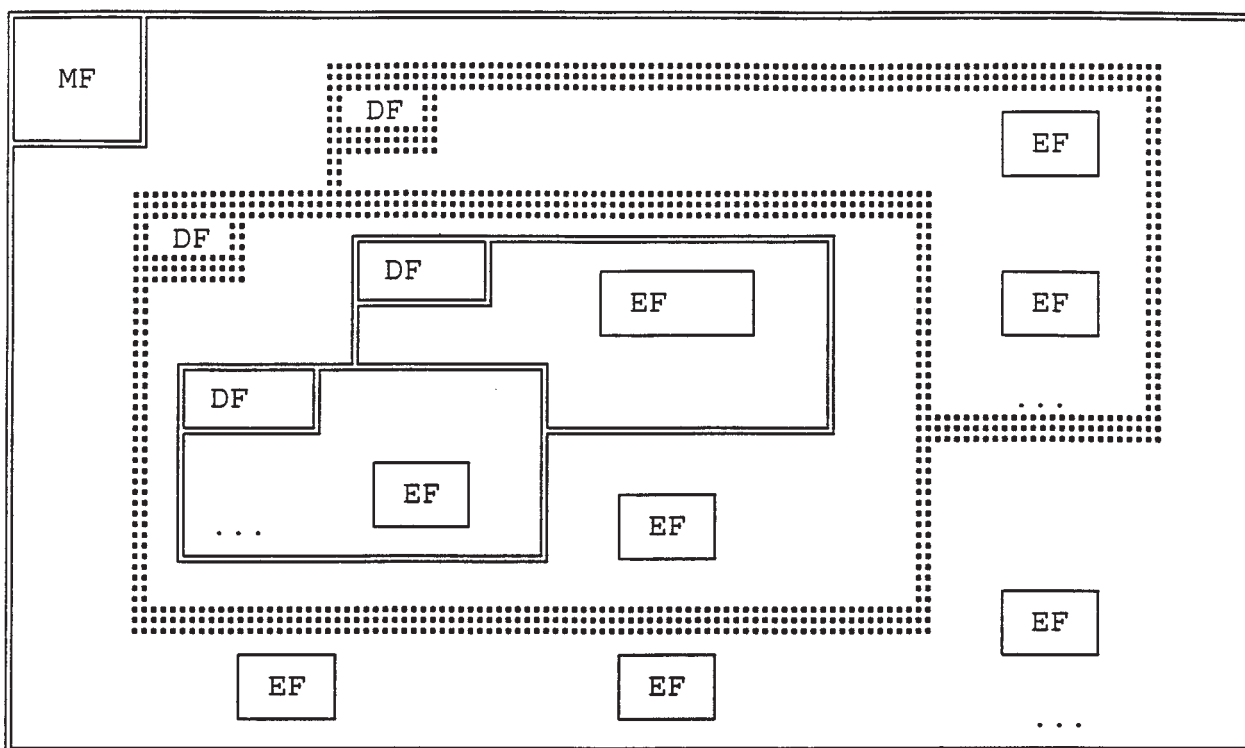


Bild 1: Modell für die Datenstruktur einer Chipkarte

5.4 Arbeitszyklus

Der Arbeitszyklus für Asynchronbetrieb muß während des stabilen Betriebszustandes zwischen 40% und 60% der Gesamtperiode liegen.

5.5 Schutzzeit

Für die Übertragung zwischen Karte und Endgerät gibt es zwei zusätzliche Schutzzeiten in bezug auf die Zeichendauer. Die Zeichendauer muß auf 12 elementare Zeiteinheiten (etu) festgelegt sein. Die zusätzliche Schutzzeit für die Übertragung vom Endgerät zur Karte wird durch TC1, den Parameter N im Answer-to-Reset festgelegt, der einen Wert von 255 (außer für T=0), 0 oder 4 haben muß. Die Schutzzeit für die Übertragung von der Karte zum Endgerät wird in der PTS2 angezeigt und muß einen Wert von 255, 0 oder 12 aufweisen.

5.6 Betriebsart Reduzierter Energieverbrauch

Karten dürfen einen Modus mit reduziertem Energieverbrauch aufweisen, insbesondere bei Mobilgeräten. Der Modus wird gekennzeichnet durch das Byte Taktunterbrechung in EF_{ICC}.

6 Logisches Modell für Chipkarten

Die logische Organisation der Karte, die Speicherverwaltung in der Karte beschreibt, ist in Bild 1 erläutert.

6.1 Datei-Kennzeichen

Siehe ISO 7816-4.

Das Datei-Kennzeichen (ID) ist bei Erstellen der jeweiligen Datei festzulegen und muß für zwei gleichartige Dateien vom gleichen Ursprung unterschiedlich sein. Die Erfüllung dieser Anforderung muß durch das Betriebssystem sichergestellt werden.

6.2 Strukturen der elementaren Datei (EF)

Auf der Grundlage der ISO/IEC 7616-4, werden die folgenden unterschiedlichen Strukturen der elementaren Datei definiert:

6.2.1 Transparente EF

Eine EF mit einer transparenten Struktur besteht aus einer Folge von Bytes. Eine zu lesende, zu schreibende oder zu aktualisierende Folge von Bytes wird auf eine relative Adresse (Offset) und eine Längenangabe (in Bytes) bezogen. Das erste Byte einer EF mit transparenter Struktur hat die relative Adresse '00'. Die gesamte Datenlänge der EF wird im Vorderteil der EF angegeben.

6.2.2 EFs mit Programmen

Wenn eine transparente EF erstellt wird, die ein Programm enthält, muß der Kartenausgeber eine mögliche Beeinträchtigung zwischen den Anwendungen ausschließen.

Für den Befehlssatz gibt es zwei Möglichkeiten:

- der allgemeine Befehlssatz ist ausreichend; es besteht kein Bedarf, diese DF mit einem ASC-System zu verknüpfen,
- der allgemeine Befehlssatz ist nicht ausreichend; mit dieser DF muß ein ASC-System verknüpft werden. Das ASC-System muß definiert und vereinbart werden.

In einer EF enthaltene Programme sind in bezug auf einige spezifische Benutzer-Merkmale stärker applikationsbezogen.

BEISPIEL 1:

In einigen Anwendungen könnte das in der Chipkarte eine Berechnung des Limits sein, welches auf verschiedenen spezifischen, in der Karte gespeicherten Benutzer-Merkmalen basiert.

Durch den spezifischen ASC-Satz gesteuerte Programme sind stärker applikationsbezogen.

BEISPIEL 2:

Ein spezifischer verschlüsselter Algorithmus, der zur Authentifizierung (Echtheitsprüfung) der Anwendung dient.

6.2.3 EF mit linear fester Struktur

Eine EF mit dieser Struktur besteht aus einer Folge von Datensätzen mit fester Länge. Der erste Datensatz in dieser EF wird als Datensatznummer 1 definiert. Im Vorderteil dieser Struktur wird angegeben:

- die Gesamtlänge der Daten,
- die Nummer der erstellten Datensätze,
- die Länge des Datensatzes.

Innerhalb einer EF diesen Typs gibt es drei Zugriffsverfahren auf Datensätze:

- Verwendung der Datensatznummer,
- bei einer Positionierung auf dem aktuellen (durch das Betriebssystem bekannten) Datensatz muß es möglich sein, eine Aktion auf den aktuellen, den nächsten (mit Ausnahme des letzten Datensatzes), den vorherigen (mit Ausnahme des ersten Datensatzes), den ersten oder letzten in der EF vorhandenen Datensatz auszuüben,
- durch Suche nach einem Muster, beginnend vom Anfang zum Ende (vorwärts), vom Ende zum Anfang (rückwärts), vom nächsten Datensatz vorwärts und vom vorherigen Datensatz rückwärts.

Es ist nicht möglich, mehr als 255 Datensätze in einer Datei zu erzeugen.

6.2.4 EF mit linear variabler Struktur

Eine EF mit dieser Struktur besteht aus einer Folge von Datensätzen mit variabler Länge. Der erste Datensatz in dieser EF wird als Datensatz Nr 1 bezeichnet.

Im Vorderteil dieser Struktur wird angezeigt:

- die Gesamtlänge der Daten,
- die Nummer der erstellten Datensätze.

Jeder Datensatz hat seine eigene Längenanzeige, die nach Erstellung des Datensatzes nicht verändert werden kann. Der Zugriff auf diesen Typ einer EF erfolgt auf die gleiche Weise wie für EFs mit linear fester Struktur.

Es ist nicht möglich, mehr als 255 Datensätze in einer Datei zu erzeugen.

6.2.5 EF mit zyklischer Struktur

Eine EF dieser Struktur besteht aus einer Folge von Datensätzen mit jeweils identischer Länge, wobei die Daten ringförmig organisiert werden. Zum Zeitpunkt der Generierung müssen alle Datensätze mit '00' belegt werden.

In jeder zyklisch aufgebauten Datei merkt sich die Karte den Bezugspunkt des zuletzt geschriebenen Datensatzes. In einer EF mit zyklischer Struktur bekommt der zuletzt geschriebene Datensatz die Datensatznummer 1 (# 1). Der älteste Datensatz hat die höchste Datensatznummer.

Bei Schreiboperationen ist das Adressieren eines Datensatzes nur durch PREVIOUS möglich. In diesem Fall wird der älteste Datensatz überschrieben.

Bei Operationen zur Vergrößerung und Verkleinerung ist der zu verändernde Wert in der aktuellen Datensatznummer 1, und das Ergebnis der Berechnung muß in den ältesten Datensatz geschrieben werden. Nach einer INCREASE oder DECREASE-Durchführung, muß der geänderte Datensatz die aktuelle Datensatznummer 1 erhalten. Bei Leseoperationen besteht die Möglichkeit des Adressierens eines Datensatzes durch FIRST, LAST, NEXT, PREVIOUS, CURRENT oder durch die Satznummer.

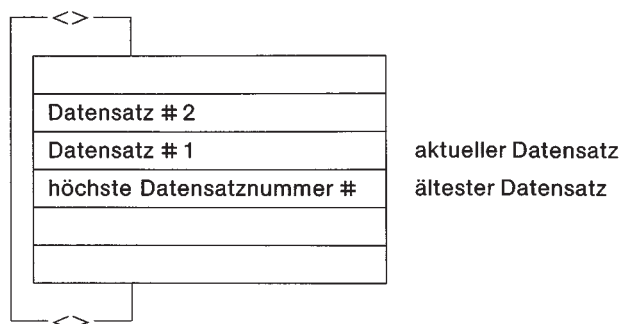


Bild 2: Struktur der zyklischen EF

Nach der Ansteuerung einer zyklischen EF zeigt die Datensatznummer automatisch auf den zuletzt geschriebenen Datensatz.

Es ist nicht möglich, mehr als 255 Datensätze in einer Datei zu erzeugen.

6.2.6 EFs mit ASC-Satz

Eine EF, die einen Satz applikationsspezifischer Befehle (ASC) enthält, ist eine Art Filter, der Befehle umadressiert und/oder Programme unter Verwendung von Verfahren startet, die im allgemeinen Befehlssatz nicht enthalten sind. Ein ASC kann die Bedeutung des allgemeinen Befehlssatzes erweitern oder verändern.

Ein ASC kann nur mit einer bestimmten DF verbunden werden, die eine Anwendung enthält und beim Arbeiten auf ihrem Teilbaum verfügbar wird. Beim Erstellen einer DF muß eine Information an die Karte gegeben werden, ob eine EF mit einem ASC-Satz verfügbar ist oder nicht.

Es kann nur ein ASC-Satz mit einer DF verbunden sein.

6.3 Inhalt der EF_{DIR}

EF_{DIR} kann auf jeder Stufe vorhanden sein. Entsprechend geschäftlicher Vereinbarungen kann EF_{DIR} Bezugspunkte zu DFs auf beliebigen Stufen aufweisen.

In der Hauptdateiebene (MF) enthält EF_{DIR} für jede nicht versteckte Anwendung die folgenden Informationen:

- Anwendungskennzeichen,
- verbale Beschreibung (Anwendungsetikett) der nach ISO 8859-1 : 1982 codierten Anwendung (maximal 16 Zeichen),
- Pfad (beliebige Daten) (Folge der aus 2 Bytes bestehenden Datei-ID).

Die Codierung dieses EF_{DIR} muß nach ISO/IEC 7816-5 erfolgen.

6.4 Verfahren zum Auswählen einer Datei

Gemäß ISO/IEC 7816-4.

Wenn der Channel-Mechanismus zur Auswahl von Dateien anzuwenden ist, muß sich das Betriebssystem die aktuelle Datei, das aktuelle Verzeichnis und die aktuelle EF für jeden verwendeten Kanal merken.

Bei diesem Channel-Mechanismus muß eine ausschließliche Auswahl der Datei (für einen Kanal) eingeführt werden. Damit werden unterschiedliche Anwendungen daran gehindert, zur gleichen Zeit auf Daten zuzugreifen.

6.5 Applikationsspezifischer Befehlssatz (ASC)

Nicht zum Geltungsbereich dieser Norm gehören der Vorgang des Hinzufügens eines ASC-Satzes zur Karte und die Garantie, daß der zugefügte ASC-Satz die vorhandenen Funktionen und die Software nicht beeinträchtigt; dafür sind der Anwendungsanbieter und der Kartenausgeber verantwortlich.

6.6 Ungültigkeitserklärung/Rehabilitierung einer Datei

Eine Datei kann für ungültig erklärt werden. Diese Datei ist danach außer für die Funktionen SELECT, DELETE und REHABILITATE (die Funktion REHABILITATE ist die Umkehrfunktion von INVALIDATE) nicht mehr verfügbar.

Eine für ungültig erklärte EF kann gelesen werden, sofern diese im Datei-Status angezeigt wird.

7 Sicherheitseinrichtungen für die Karte

7.1 Zugriffsbedingungen

Auf jeder Ebene der Dateistruktur in der Karte sind Zugriffsbedingungen (AC) definiert. Die AC werden für Funktionsgruppen festgelegt, die mit jeweils identischen Zugriffsbedingungen auf Dateien zugreifen. Die AC der aktuellen Datei müssen erfüllt werden, bevor durch die Funktionen ein Zugriff auf die Datei möglich ist.

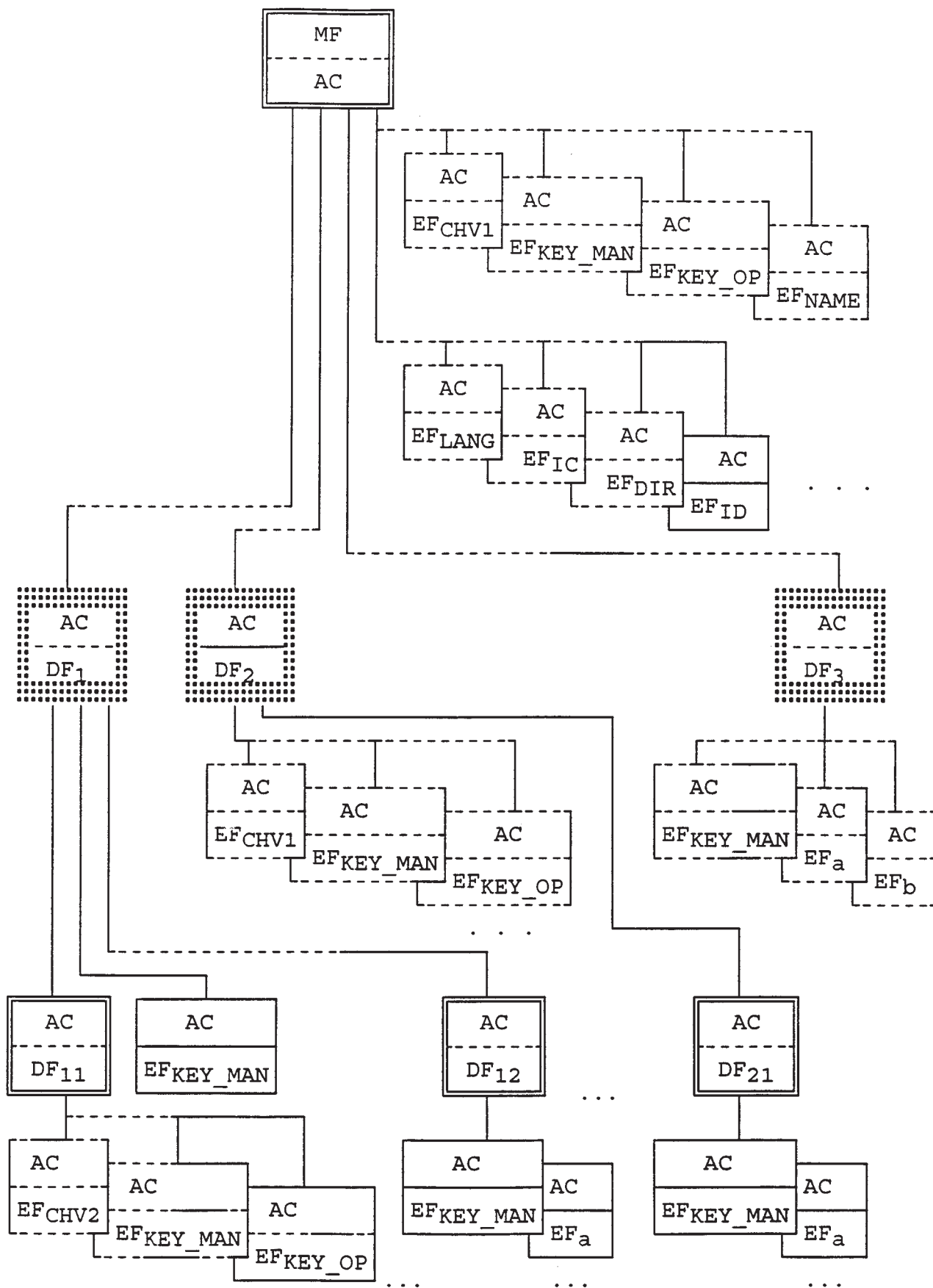


Bild 3: Beispiel der allgemeinen Struktur mit Zugriffskontrollen

BEISPIEL:

Wenn im Bild 3 auf die EF_a unterhalb von DF₁₂ zugegriffen wird, müssen nur die AC der EF_a erfüllt werden. Die für DF₁₂ und DF₁ festgelegten AC sind für den Zugriff zu dieser EF_a nicht relevant.

7.1.1 Grundbedingungen und Kombinationen von Bedingungen

Grundbedingungen sind:

- ALW: Eine Aktion muß immer möglich sein. Sie kann ohne jede Einschränkung ausgeführt werden.
- NEV: Eine Aktion darf niemals möglich sein. Sie kann nur intern ausgeführt werden.
- CHV1: Verifizierung des Karteninhabers. Die Aktion darf nur nach einer ordnungsgemäßen CHV-Darstellung und/oder nach einer biometrischen Überprüfung möglich sein. Die CHV und/oder die biometrischen Informationen müssen in der relevanten EF_{CHV} gespeichert werden. Die Benennung "relevant" bedeutet, daß die EF_{CHV} für die aktuelle Datei eine Sohndatei (eine Stufe niedrigere Datei) sein kann, oder falls die EF_{CHV} dort nicht vorhanden oder für ungültig erklärt ist, die relevante EF_{CHV} der Ursprungsdatei sein muß. Für eine CHV mit einer Länge von mehr als 8 Bytes (z. B. ein biometrischer Speicher) wird der Pfad zu der EF, in der die CHV enthalten ist, in der EF_{CHV} angegeben.
- CHV2: Siehe CHV1; CHV und/oder biometrische Informationen sind jedoch in der EF_{CHV2} zu speichern, die auf einer anderen Stufe der EF_{CHV1} vorhanden sein kann.
- PRO: Die Aktion darf nur auf geschützte Weise möglich sein. (Authentifikation der Herkunft und Integrität der Daten, siehe Abschnitt 7.6).
- AUT: Die Aktion darf nur nach einer externen Authentifikation (d.h. Authentifikation durch die Karte des Endgerätes/der Anwendung) möglich sein.

ANMERKUNG 1: Beispiel für die Anwendung der CHV1/CHV2 für unterschiedliche Zwecke: Einem Kartenausgeber ist lediglich erlaubt, die Festwahl-Tabelle (Liste der feststehenden Nummern, deren Anwendung zulässig ist) in der Karte unter Verwendung einer CHV2 zu aktualisieren, während der Kartenbenutzer die CHV1 eingeben muß, um die Festwahl-Tabelle zu lesen.

ANMERKUNG 2: Der Verschlüsselungsmodus (ENC) muß optional möglich sein (gemäß ISO/IEC 7816-4).

Mögliche Kombinationen der Grundbedingungen werden in der folgenden Zusammenstellung von Bedingungen angegeben:

ALW
CHV1
CHV2
PRO
AUT
CHV1/PRO
CHV2/PRO
CHV1/AUT
CHV2/AUT

Bild 4: Mögliche Zugriffsbedingungen

7.1.2 EF, in der die geheimen Schlüssel enthalten sind

Es gibt 2 Funktionsarten, dies sind Managementfunktionen und Betriebsfunktionen (siehe Abschnitt 7.1.4). Für jede

dieser Funktionen ist es gegebenenfalls erforderlich eine der zwei nachfolgenden Zugriffsbedingungen zu erfüllen: Geschützt (PRO) oder Authentifiziert (AUT). Die erforderlichen geheimen Schlüssel zusammen mit der Version der Schlüsseldatei, Schlüssellänge und Algorithmuskennzeichen sollen in den relevanten Schlüsseldateien EF_{KEY_MAN} und EF_{KEY_OP} gespeichert werden.

Für die MF oder eine DF ist die relevante Schlüsseldatei immer EF_{KEY_MAN}, welche eine Unterdatei von MF oder DF darstellt.

Nach der Generierung ist EF_{KEY_MAN} leer (Schlüssellänge des ersten Schlüssel ist '00'). In diesem Fall findet man temporäre Schlüssel in der relevanten Datei EF_{KEY_MAN} der nächstniedrigeren Ebene.

Zur aktuellen EF findet man die Schlüssel – in Abhängigkeit von der benutzten Funktion – in den Dateien EF_{KEY_MAN} oder EF_{KEY_OP}. EF_{KEY_OP} kann nur mit Schlüsseln der zugehörigen DFs erzeugt und geladen werden, wobei die Schlüsseldatei EF_{KEY_MAN} benutzt wird.

EF_{KEY_OP} kann ungültig gemacht werden. Dabei ist es möglich die Datei EF_{KEY_OP} einer höheren Ebene zu benutzen. Falls in der angesteuerten Ebene keine EF_{KEY_OP} vorhanden ist, muß EF_{KEY_OP} einer höheren Ebene benutzt werden.

7.1.3 EF, in der die CHVs enthalten sind

Für die Funktionen, die der CHV-Bedingung zu entsprechen haben, müssen die entsprechenden CHVs in der relevanten EF_{CHV} gespeichert sein.

Diese EF_{CHV} enthält ferner:

- Art der anzuwendenden Benutzeridentifikation (siehe Abschnitt 10.1);
- Art und Weise (verschlüsselt oder unverschlüsselt), in der die CHV und die UNBLOCK CHV der Karte angeboten werden müssen;
- die relevante Schlüsselnummer, falls die Eingabeart verschlüsselt ist;
- der voreingestellte Wert N für den Zähler der CHV-Versuche;
- der Zähler für die Anzahl der restlichen CHV-Versuche im Fall von fehlerhaften CHV-Eingaben. Dieser Dekrementier-Zähler muß jedesmal zurückgestellt werden, wenn eine ordnungsgemäße CHV eingegeben wird. Ist der Wert Null erreicht, muß die CHV gesperrt werden;
- die UNBLOCK CHV (eine Art CHV, die das Rücksetzen des CHV-Fehlerzählers auf N ermöglicht und die CHV entsperrt);
- ein Zähler verbleibender UNBLOCK CHV-Versuche, der jedesmal dekrementiert wird, wenn der Entsperrungsmechanismus nicht ordnungsgemäß angewendet wurde. Nach einem korrekten Gebrauch des Entsperrungsmechanismus muß es erneut voreingestellt werden. Wenn dieses Zählwerk den Wert 0 erreicht, muß die entsprechende Anwendung gesperrt werden;
- ein Zähler verbleibender UNBLOCK-Benutzungen, der die restliche Anzahl der noch zulässigen Anwendungen des Entsperrungsmechanismus anzeigt. Es ist ebenfalls ein Zähler, der bei jeder Anwendung des Entsperrungsmechanismus dekrementiert werden muß und nicht zurückgesetzt werden darf.

7.1.4 Dateizugriffsbedingungen

Managementfunktionen mit Auswirkungen auf alle Dateiarten (MF, DF und EF), sind:

- DELETE FILE;
- CREATE FILE; EXTEND FILE;
- UPDATE BINARY; LOAD KEY FILE;
- INVALIDATE; REHABILITATE.

Die folgenden Gruppen mit Managementfunktionen mit gleichartigen AC-Anforderungen und den gleichen Zugriffsbedingungen sind definiert:

Tabelle 1: Funktionen, die auf eine DF anwendbar sind

RFU	RFU
DELETE FILE	CREATE FILE EXTEND FILE
REHABILITATE	INVALIDATE

Tabelle 2: Funktionen, die auf Schlüsseldateien anwendbar sind

LOAD KEY FILE	UPDATE
RFU	RFU
REHABILITATE	INVALIDATE

Betriebsfunktionen, die nur auf EFs Auswirkungen haben, sind:

READ; SEEK;
UPDATE; WRITE;

INCREASE; DECREASE;
EXECUTE; CREATE RECORD;
INVALIDATE; REHABILITATE.

Die folgenden Gruppen mit Betriebsfunktionen mit gleichartigen AC-Anforderungen und den gleichen Zugriffsbedingungen sind definiert:

Tabelle 3: Funktionen, die auf EFs anwendbar sind

READ/SEEK	UPDATE DECREASE
WRITE INCREASE	CREATE RECORD EXECUTE
REHABILITATE	INVALIDATE

Die WRITE- und INCREASE-Funktionen befinden sich in der gleichen Gruppe der Zugriffsbedingungen. Jedoch ist für eine vorgegebene Datei nur eine der Funktionen gültig (siehe Abschnitt 9.3.1).

Die UPDATE- und DECREASE-Funktionen befinden sich in der gleichen Gruppe der Zugriffsbedingungen. Jedoch ist für eine vorgegebene Datei nur eine der Funktionen gültig (siehe Abschnitt 9.3.1).

Für andere Funktionen sind keine ACs festgelegt.

Tabelle 4: Mögliche Funktionen mit Dateien

Funktion	Aktuelle Datei				
	MF	DF	EF	Schlüssel-datei	EF _{CHV}
CLOSE APPLICATION	×	×			
CREATE FILE	×	×			
CREATE RECORD			×		
DECREASE			×		
DECREASE STAMPED			×		
DELETE FILE	×	×			
EXECUTE			×		
EXTEND	×	×			
INCREASE			×		
INCREASE STAMPED			×		
INVALIDATE	×	×	×	×	×
LOAD KEY FILE				×	
LOCK	×	×	×	×	×
READ BINARY			×		
READ BINARY STAMPED			×		
READ RECORD			×		
READ RECORD STAMPED			×		
REHABILITATE	×	×	×	×	×
SEEK			×		
SELECT	×	×	×	×	×
STATUS	×	×	×	×	×
UPDATE BINARY			×	×	×
UPDATE RECORD			×		
WRITE BINARY			×		
WRITE RECORD			×		

Die Tabelle 4 erklärt welche Funktionen möglich sind, wenn die aktuell angesteuerte Datei die MF, eine DF, eine EF, eine Schlüsseldatei (EF_{KEY_MAN} oder EF_{KEY_OP}) oder eine EF_{CHV} darstellt.

ANMERKUNG 1: Die Aktionen CREATE FILE, DELETE FILE und EXTEND können nur auf Sohndateien des aktuellen Verzeichnisses angewendet werden.

ANMERKUNG 2: Die Aktionen VERIFY CHV, CHANGE CHV, DISABLE CHV, ENABLE CHV, UNBLOCK CHV, INTERNAL AUTHENTICATION, EXTERNAL AUTHENTICATION, ASK RANDOM und GIVE RANDOM sind unabhängig von der aktuellen Datei möglich.

7.2 Anwendbare Funktionen bei unterschiedlichen EF-Arten

Tabelle 5: EF-Arten

Funktionen	EXTEND	INVAL REHAB	CREATE RECORD	UPDATE RECORD	READ REC.	SEEK	READ BIN.	UPDATE BIN.
Dateiart								
linear feste Struktur	ja	ja	ja	ja	ja	ja	nein	nein
linear variable Struktur	ja	ja	ja	ja	ja	ja	nein	nein
transparent	ja	ja	nein	nein	nein	nein	ja	ja
zyklisch	nein	ja	ja	ja ¹⁾	ja	ja	nein	nein

¹⁾ Nur für die nächste, zu schreibende Schreiboperation.

Tabelle 5: EF-Arten (Fortsetzung)

Funktionen	WRITE RECORD	WRITE BIN.	LOCK	EXEC.	SELECT STATUS	INCREASE DECREASE
Dateiart						
linear feste Struktur	ja	nein	ja	nein	ja	nein
linear variable Struktur	ja	nein	ja	nein	ja	nein
transparent	nein	ja	ja	ja	ja	nein
zyklisch	ja ¹⁾	nein	ja	nein	ja	ja

¹⁾ Nur für die nächste, zu schreibende Schreiboperation.

UPDATE RECORD bedeutet eine Löschoption, gefolgt von einer Schreiboperation.

ANMERKUNG: Auf der EF-Ebene gibt es keine DELETE-Funktion, um das Betriebssystem und die Speicherbehandlung zu vereinfachen. Es ist Sache der Anwendung, beispielsweise eine DELETE-Datei in Verbindung mit einer Wiederherstellung eines Teils der Datei zu verwenden, um einige Aufzeichnungen zu löschen.

7.3 Kanalunterstützung

Siehe ISO 7816-4.

7.4 Verfahren zum Beenden der Applikation

Bei einigen Anwendungsfällen kann es erforderlich sein, die Speicherung der bereits erfüllten Zugangsbedingungen zu löschen. Diese Möglichkeit besteht durch die CLOSE APPLICATION-Funktion (siehe Abschnitt 8.26).

BEISPIEL:

Auf einem Heimterminal kann nach einer sicherheitsempfindlichen Sitzung die Karte im Terminal bleiben, doch die Anwendung selbst sollte nicht zugänglich sein. Das geschieht mit der CLOSE APPLICATION-Funktion.

7.5 Sicherheitsumgebung

Das Betriebssystem muß sich an die bereits erfüllten Zugangsbedingungen CHV und AUT bis zum Ende der Kartensitzung oder dem ausdrücklichen Schließen der Anwendung erinnern.

Der Zweck besteht darin, nicht zweimal nach derselben Benutzeridentifikation (CHV und/oder biometrisch) und/oder nach der externen Authentifikation zu fragen. Wenn

mehrere Sitzungen unterstützt werden, muß für jede Sitzung die Zugriffsbedingung AUT erfüllt werden. Die benutzerbezogene Zugriffsbedingung CHV wird als eine allgemeine AC angesehen (falls dieselbe EF_{CHV} verwendet wird) und kann daher einmal für alle Sitzungen erfüllt werden. Wenn jede Wechselwirkung zwischen der externen Welt und der Karte authentifiziert werden muß, dürfen die AC = PRO (anstelle der externen Authentifikation) benutzt werden.

ANMERKUNG: Das Betriebssystem muß alle CHV und alle verfügbaren Schlüssel überwachen, die den Status von CHV oder AUT aufweisen.

7.6 Allgemeine Beschreibung der Sicherheitsfunktionen

Unter Sicherheitsaspekten wurde die AC PRO nur für die folgenden Arten von Funktionen definiert:

- Funktionen, wobei die mit dem Kommando übergebenen Daten den Dateninhalt der Karte verändern;
- Funktionen ohne Eingangsdaten, die aber den Datei-Status verändern.

Funktionen ohne Beeinflussung des Dateistatus, die Daten aus der Karte senden, benötigen keine AC PRO. In diesem Fall wird der markierte Modus benutzt, wobei die externe Welt bestimmt ob die ausgesandten Karten mit einem Kryptogramm gesichert werden. Dies erfolgt mittels besonderer Befehle.

7.6.1 Mit Zugriffsbedingungen verknüpfte Sicherheitsfunktionen

Mehrere Funktionen können mit der AC = PRO ausgeführt werden. Dabei ist das Kryptogramm ein Teil der Daten, die zur Karte gesendet werden.

Ein Kryptogramm ist das Ergebnis eines kryptografischen Prozesses basierend auf einem Algorithmus und einem geheimen Schlüssel. Beide sind verbunden mit der Schlüsselnummer der AC-Kodierung für die jeweils aktuell selektierte Datei (siehe Abschnitt 9.3). Der geheime Schlüssel und die benutzte Algorithmus-Kennung sind in der Schlüsseldatei (EF_{KEY_MAN} oder EF_{KEY_OP}) gespeichert (siehe Abschnitte 10.6 und 10.7).

Wenn in der geschützten Betriebsart ein Befehl zur Karte gesendet wird, muß die externe Welt zuerst eine Zufallszahl von der Karte anfordern, um danach das Kryptogramm mit den folgenden Eingangsdaten zu berechnen:

- Zufallszahl;
- Teil des Vorderteils der Daten des Befehls (INS, P1, P2);
- Länge des Datenfelds und Daten oder keine Daten.

Das Kryptogramm ist an das Ende der zur Karte gesandten Daten anzufügen.

Nach dem Empfang des Befehls überprüft die Karte die Konsistenz des Kryptogramms mit den Eingabedaten (Zufallszahl, Vorderteil der Daten, Daten falls vorhanden). Bei Übereinstimmung wird der Befehl akzeptiert und ausgeführt. Andernfalls wird der Befehl abgewiesen.

7.6.2 Sicherheitsfunktionen in Verbindung mit der markierten Betriebsart

Die Funktionen (READ BINARY, READ RECORD, INCREASE, DECREASE) können in dem markierten (stamped) Modus ausgeführt werden. Dabei ist ein Kryptogramm ein Teil der von der Karte übergebenen Antwortdaten.

Das ausgesendete Kryptogramm ist das Ergebnis eines kryptografischen Prozesses auf der Basis eines Algorithmus und eines geheimen Schlüssels, die bei der aktuell angesteuerten Datei mit der jeweiligen Funktion und der Schlüsselnummer in der AC-Kodierung (siehe Abschnitt 9.3) verknüpft sind. Der geheime Schlüssel und die benutzte Algorithmus-Kennung sind in der relevanten Schlüsseldatei (EF_{KEY_MAN} oder EF_{KEY_OP}), siehe Abschnitte 10.6 und 10.7, festgelegt.

Um das Kryptogramm für die Antwort-Daten zu berechnen, muß die Karte die vorherige übergebene Anforderung

(Zufallszahl) benutzen. Das Kryptogramm wird mit den folgenden Eingangsdaten berechnet:

- Anforderung (Zufallszahl);
- abhängig von der Betriebsart;
- kein Vorderteil;
- Teil des Vorderteils (INS, P1, P2) des invertierten Befehles;
- Teil des Kopfteils (INS, P1, P2) des aktuellen Befehles;
- Teil des Kopfteils (INS, P1, P2) des invertierten Befehles in der markierten Betriebsart;
- Teil des Kopfteils (INS, P1, P2) des aktuellen Befehles in der markierten Betriebsart;
- maximale Datenlänge der Antwortdaten;
- Daten.

Das Kryptogramm ist an das Ende der von der Karte übermittelten Daten anzufügen.

7.6.3 Externe Authentifizierung (Echtheitsüberprüfung)

Diese Funktion muß vom Endgerät/ von der Anwendung zur Authentifizierung durch die Karte angewendet werden. Zu diesem Zweck muß die Karte eine Zufallszahl (eine Abfrage) an das Endgerät weitergeben, das an die Karte mit einem Kryptogramm antwortet. Diese Antwort muß durch die Karte verifiziert werden, wozu ein kryptographischer Algorithmus abläuft, der die zuvor ausgesendete Abfragezahl und einen Schlüssel verwendet. Der Schlüssel und die ID-Nummer des für diesen Vorgang zu verwendeten Algorithmus müssen in der diesbezüglichen EF_{KEY} angegeben sein (siehe Unterabschnitt 8.25). Die Schlüsselnummer ist ein durch das Endgerät/die Anwendung vorgegebener Parameter. Bei positiver Verifikation des Kryptogramms ist die AUT-Bedingung erfüllt, und das Betriebssystem muß sich für jeden beliebigen Schlüssel an diese bis an das Ende der Sitzung erinnern (siehe Abschnitt 7.5).

7.6.4 Interne Authentifizierung

Diese Funktion muß vom Endgerät/von der Anwendung zur Authentifizierung der Karte angewendet werden. Zu diesem Zweck muß das Endgerät eine Zufallszahl (eine Abfrage) an die Karte weitergeben, die mit einem Kryptogramm auf die Abfrage antwortet. Die Antwort muß durch das Endgerät verifiziert werden, wozu ein kryptographischer Algorithmus, die zuvor ausgesendete Abfragezahl und ein Schlüssel verwendet werden. Der geheime Schlüssel und die benötigte Algorithmus-Kennung müssen in der relevanten Schlüsseldatei stehen (siehe Abschnitt 8.22). Die Schlüsselnummer wird als Parameter des Endgerätes/Anwendung zur Karte übergeben.

ANMERKUNG: Die Anforderung soll in der Regel eine Zufallszahl sein. Jedoch kann anstatt der Zufallszahl ein anderer Authentifizierungsparameter benutzt werden (z. B. die Uhrzeit oder eine Folgenummer).

7.6.5 Algorithmus-Kennung

Tabelle 6: Algorithmus-Kennungen (ID)

Algorithmus	ID	AUTHENTIF.	PRO	Markiert	Lade-Schlüssel
DSSA	'1'	×			
COMP NAT	'2'	×			
TESA-7	'4'	×	×	×	×
COMP 128	'40'	×			
Ausstieg für eigene Algorithmen	"7F"				

ANMERKUNG 1: Verfügbare Verschlüsselungsalgorithmen für den allgemeinen Gebrauch werden nicht in diesem Teil der EN 726 beschrieben. Jedoch können diese Algorithmen für eigene Anwendungen eingesetzt werden.

ANMERKUNG 2: DSAA bedeutet ein von DECT standardisierter Authentifikations-Algorithmus.

8 Beschreibung der Funktionen

Die folgenden allgemeinen Funktionen sind festgelegt:

1	SELECT	(wähle aus)
2	STATUS	(Status)
3	CREATE FILE	(Datei erstellen)
4	DELETE FILE	(Datei löschen)
5	EXTEND	(erweitern)
6	EXECUTE	(ausführen)
7	UPDATE BINARY	(binäres Update)
8	UPDATE RECORD	(Datensatz-Update)
9	CREATE RECORD	(Datensatz erstellen)
10	READ BINARY	(binäres Lesen)
11	READ BINARY STAMPED	(markiertes binäres Lesen)
12	READ RECORD	(Datensatz lesen)
13	READ RECORD STAMPED	(markierten Datensatz lesen)
14	SEEK	(suchen)
15	VERIFY CHV	(CHV verifizieren)
16	CHANGE CHV	(CHV ändern)
17	DISABLE CHV	(CHV sperren)
18	ENABLE CHV	(CHV freigeben)
19	UNBLOCK CHV	(CHV-Blockierung freigeben)
20	INVALIDATE	(ungültig setzen)
21	REHABILITATE	(wieder einsetzen)
22	INTERNAL AUTHENTICATION	(interne Authentifizierung)
23	AKS RANDOM	(Zufallsabfrage)
24	GIVE RANDOM	(Zufallswert einsetzen)
25	EXTERNAL AUTHENTICATION	(äußere Authentifizierung)
26	CLOSE APPLICATION	(Anwendung schließen)
27	WRITE BINARY	(binäres Schreiben)
28	WRITE RECORD	(Datensatz schreiben)
29	LOCK	(verriegeln)
30	DECREASE	(erhöhe)
31	DECREASE STAMPED	(erhöhe markiert)
32	INCREASE	(vermindere)
33	INCREASE STAMPED	(vermindere markiert)
34	LOAD KEY FILE	(lade Schlüsseldatei)

Es ist nicht Pflicht für alle mit dieser Norm übereinstimmen- den Karten, daß sie alle beschriebenen Funktionen dieser Norm unterstützen. Aus diesem Grunde sind Kartenprofile festgelegt worden (siehe Abschnitt 10.5).

Nach dem Senden der entsprechenden Funktion werden die erwarteten Ergebnisse einer Funktion oder die mög- lichen Fehlerbedingungen immer wieder von der Karte zurückgemeldet. Sie werden in den Statusinformations-

bytes ausgedrückt, die nach jedem Befehl von der Karte zurückgemeldet werden. Im Abschnitt 9.4 sind alle mög- lichen Statusinformationsbedingungen und ihre entspre- chende Kodierung für jeden möglichen Befehl aufgeführt.

In allen Darstellungen ist das äußerste linke Bit das höchst- wertigste Bit des höchstwertigsten Bytes und das äußerste rechte Bit das niedrigstwertigste Bit des niedrigstwertig- sten Bytes.

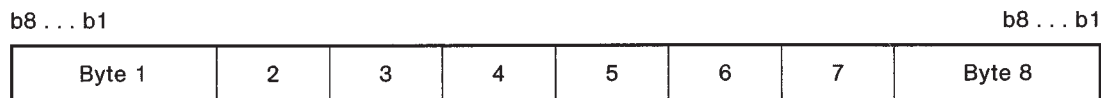


Bild 5: Festlegung für eine Bytefolge

8.1 SELECT

Diese Funktion ermöglicht nach den bereits weiter oben beschriebenen Verfahren die Auswahl einer Datei, gemäß ISO/IEC 7816-4.

Folgende Bewegungen sind durch Anwendung des Datei- ID, des Pfades oder des Anwendungskennzeichens mög- lich:

- nach unten;
- horizontal;
- nach oben;
- aus der MF.

Nach einer erfolgreichen Auswahl wird die ausgewählte Datei zur neuen aktuellen Datei, wobei der Zeiger auf den Speicherplatz nicht definiert wird (außer in zyklischen

Dateien, siehe Abschnitt 6.2.5). Um einen Datensatz zu lesen, ist die Festlegung des aktuellen Speicherplatzes durch Anwendung der Betriebsarten next, previous, first und last für die Funktionen SEEK, READ, UPDATE oder WRITE zwingend vorgeschrieben.

Eingabe: Beschreibung der Eingabeparameter siehe Abschnitt 9.2.1;

Ausgabe: Beschreibung der Ausgabeparameter siehe Abschnitt 9.2.1, sofern die selektierte Datei eine DF, eine EF, eine EF_{CHF} oder eine Schlüsseldatei ist.

ANMERKUNG: Für diese Funktion sind keine ACs definiert.

8.2 STATUS (Zustand)

Diese Funktion gibt Informationen in bezug auf das aktuelle Verzeichnis. Die aktuelle Datei wird von der STATUS-Funktion nicht beeinflusst.

Eingabe: Keine.

Ausgabe: Beschreibung der Ausgabedaten siehe Abschnitt 9.2.2.

ANMERKUNG: Für diese Funktion sind keine ACs definiert.

8.3 CREATE FILE

Diese Funktion ermöglicht die Erstellung einer neuen Datei unter dem aktuellen Verzeichnis. Die AC für die CREATE FILE-Funktion des aktuellen Verzeichnisses muß erfüllt werden.

Der Kartenausgeber trägt die Verantwortung, die EF_{DIR} im Fall der Erstellung einer neuen Anwendung zu aktualisieren. Wenn eine EF, eine EF_{CHF} oder eine Schlüsseldatei (EF_{KEY_MAN} oder EF_{KEY_OP}) generiert werden, muß der zugewiesene Datenbereich mit '00' initialisiert werden, um die Datenfelder als leer zu kennzeichnen.

Wenn eine ablauffähige EF zu erstellen ist, müssen die für die MF gültigen AC erfüllt werden, weil für das Erstellen einer ablauffähigen Datei der Kartenausgeber verantwortlich ist. Für eine EF, die ein Programm enthält, müssen die AC für die READ-Funktion auf NEV oder AUT und für die UPDATE-Funktion auf PRO gesetzt werden. Andere Optionen dürfen nicht möglich sein.

Falls AC = PRO ist, authentifiziert die Karte die Herkunft und den Inhalt des Befehls durch Verifizierung des Kryptogramms (Eingabe b), das durch das Endgerät aus dem Eingabeparameter (a) und der zuvor von der Karte nach der ASK RANDOM-Funktion angegebenen Zufallszahl erzeugt wird. Die CREATE-Funktion darf von der Karte nicht ausgeführt werden, wenn die Verifizierung des Kryptogramms nicht ordnungsgemäß ist. Der für die Verifizierung verwendete Schlüssel ist in der AC für das aktuelle Verzeichnis für die CREATE FILE-Funktion angegeben.

Nach Erstellen einer DF muß das aktuelle Verzeichnis auf der neu erstellten Datei sein. Im Fall einer EF-Erstellung muß die aktuelle EF auf der neu erstellten Datei und das aktuelle Verzeichnis unverändert sein.

Für das Erstellen der MF müssen die relevanten Sicherheitsschritte vom Kartenhersteller definiert werden (siehe Anhang C).

Der zugeordnete Speicherplatz muß definitiv reserviert werden.

Eingabe: a/ Datei-Parameter;
b/ ein Kryptogramm.

Falls die generierte Datei eine DF, eine EF, eine EF_{CHF} oder eine Schlüsseldatei ist, siehe Abschnitt 9.2.3 für die Beschreibung der Eingabeparameter.

Ausgabe: Keine.

8.4 DELETE FILE

Diese Funktion gestattet das Löschen einer Datei unter dem aktuellen Verzeichnis.

Die AC für die Ursprungsdatei der zu löschenden Datei muß erfüllt werden (AC für die Funktion DELETE FILE).

Löschen heißt, daß die Datei (Vorderteil und Daten) definitiv zerstört wird und von der externen Welt kein Zugriff mehr auf sie möglich ist. Eine DF kann nur gelöscht werden, wenn sie keine Dateien enthält.

Falls eine Datei mit Anwendungskennzeichen gelöscht wird, muß der Ausgeber den entsprechenden Eintrag in der EF_{DIR} löschen.

Falls AC = PRO, besteht die Eingabe aus (a, b), wobei (b) das Kryptogramm ist, das durch das Endgerät aus dem Eingabeparameter (a) und der zuvor von der Karte nach der ASK RANDOM-Funktion angegebenen Zufallszahl berechnet wird.

Eingabe: a/ Datei-ID;
b/ Kryptogramm.
Beschreibung der Eingabedaten siehe Abschnitt 9.2.4.

Ausgabe: Keine.

8.5 EXTEND

Die Funktion EXTEND gestattet die Erweiterung des der Datei unter dem aktuellen Verzeichnis zugeordneten Speicherplatzes. Diese Funktion darf nur ausgeführt werden, wenn in der Ursprungsdatei genügend Platz für die Erweiterung vorhanden ist.

Die Funktion darf für eine EF des zyklischen Typs oder des Programmtyps und natürlich ebenso für die MF nicht gestattet werden. Für die EXTEND-Funktion sind die AC der Ursprungsdatei zu erfüllen.

Die Eingabe darf außer für AC = PRO nur aus der Eingabe (a, b) bestehen (siehe unten).

Falls AC = PRO ist, besteht die Eingabe aus (a, b und c). Die Karte muß die Herkunft und den Inhalt des Befehls durch Verifizierung des Kryptogramms (Eingabe c) authentifizieren, das durch das Endgerät aus dem Eingabeparameter (a und b) und der zuvor von der Karte nach der ASK RANDOM-Funktion angegebenen Zufallszahl berechnet wird. Die EXTEND-Funktion darf von der Karte nicht ausgeführt werden, wenn die Verifizierung des Kryptogramms nicht ordnungsgemäß ist. Für die EXTEND-Funktion muß der für die Verifizierung verwendete Schlüssel in den AC des aktuellen Verzeichnisses angegeben sein.

Eingabe: a/ Datei-ID;
b/ Anzahl der zu erweiternden Einheiten (Datensätze/Bytes);
c/ Kryptogramm.
Beschreibung der Eingabedaten siehe Abschnitt 9.2.5.

Ausgabe: Keine.

8.6 EXECUTE

Diese Funktion ermöglicht den Ablauf eines in einer EF gespeicherten Programms nach dessen Selektierung. Die Funktion darf nur für eine EF gestattet werden, die ein Programm enthält. Für die EXTEND-Funktion sind die ACs der aktuellen EF zu erfüllen.

Die Eingabe darf nur aus der Eingabe (a) bestehen, die Ausgabe muß außer für AC = PRO aus Ausgabe (a) bestehen, (siehe unten).

Falls AC = PRO ist, besteht die Eingabe aus (a, b). Die Karte authentifiziert die Herkunft und den Inhalt des Befehls durch Verifizierung des Kryptogramms (Eingabe b), das durch das Endgerät aus dem Eingabeparameter (a) und der zuvor von der Karte nach der ASK RANDOM-Funktion ange-

gebenen Zufallszahl berechnet wird. Die EXECUTE-Funktion darf von der Karte nicht ausgeführt werden, wenn die Verifizierung der Kryptogramms nicht ordnungsgemäß ist. Der für diese Verifizierung zu verwendende Schlüssel ist in den ACs der aktuellen EF für die EXECUTE-Funktion angegeben.

Eingabe: a/ Keine oder Daten;
b/ Kryptogramm.
Beschreibung der Eingabedaten siehe Abschnitt 9.2.6.

Ausgabe: a/ Keine oder Daten;

8.7 UPDATE BINARY

Diese Funktion erlaubt die Aktualisierung der aktuellen EF (die eine transparente EF sein muß) mit einer Folge von Bytes. Die Funktion kann nach den für diese EF für die UPDATE-Funktion definierten ACs ausgeführt werden. Für EFs, die ein Programm enthalten²⁾ (angezeigt durch die Dateiart in der SELECT RESPONSE) müssen die ACs verwendet werden, die für die CREATE FILE-Funktion auf der MF-Stufe definiert wurden.

Eine Aktualisierung kann als ein "Auswechseln" von Bits betrachtet werden (Löschen und nachfolgendes Neuschreiben), wobei die durch die im UPDATE-Befehl angegebenen Bits die bereits im Kartenspeicher vorhanden ersetzen.

Die Eingabe darf nur aus den Eingabedaten a, b bestehen, außer wenn AC = PRO ist (siehe unten).

Falls AC = PRO ist, besteht die Eingabe aus den Eingabedaten a, b und c. Die Karte muß die Herkunft und den Inhalt des Kommandos nach der Verifizierung des Kryptogramms (Eingabe c) authentifizieren, das durch Endgerät/Anwendung aus den Eingabeparametern (a, b) und der zuvor von der Karte nach der ASK RANDOM-Funktion angegebenen Zufallszahl errechnet wird. Die UPDATE-Funktion darf von der Karte nicht ausgeführt werden, wenn die Verifizierung des Kryptogramms nicht ordnungsgemäß ist. Der für diese Verifizierung verwendete Schlüssel muß in den AC der aktuellen EF für die UPDATE-Funktionen angegeben sein.

Eingabe: a/ relative Adresse (Offset) vom Beginn des EF und die Länge (in Bytes) der zu aktualisierenden Folge;
b/ zu aktualisierende Daten;
c/ Kryptogramm.
Beschreibung der Eingabedaten siehe Abschnitt 9.2.7.

Ausgabe: Keine.

8.8 UPDATE RECORD

Diese Funktion erlaubt das Aktualisieren eines Datensatzes in der aktuellen EF. Es muß sich um eine lineare oder zyklische EF handeln. Bei einer linearen EF kann der zu aktualisierende Datensatz der aktuelle, der nächste oder der vorherige Datensatz (das bezieht sich auf die zuvor ausgeführten Funktionen READ, UPDATE oder SEEK), der erste, der letzte oder der durch seine Satznummer angezeigte Datensatz sein. Falls eine EF des zyklischen Typs vorliegt, muß nur der vorherige Datensatz (vor dem zuletzt geschriebenen Datensatz – ist zugleich der älteste Datensatz) mittels der PREVIOUS-Betriebsart aktualisiert werden. Das UPDATE kann als ein "Auswechseln" von Bytes betrachtet werden (Löschen und nachfolgendes Neuschreiben), wobei die durch die im Befehl angegebenen Bytes, die bereits im Kartenspeicher befindlichen ersetzen.

Sechs Betriebsarten sind definiert:

- CURRENT-Modus und ABSOLUTE-Modus: Der Datensatzzeiger wird von dieser Funktion nicht beeinflusst;

- NEXT-Modus: Der Datensatzzeiger wird vor Durchführung der UPDATE RECORD-Funktion inkrementiert. Wenn der aktuelle Speicherplatz innerhalb der ausgewählten EF zuvor nicht festgelegt wurde, dann muß UPDATE (next) den ersten Datensatz in der EF aktualisieren und den Datensatzzeiger auf diesen Datensatz festlegen. Falls der aktuelle Datensatzzeiger bereits auf den letzten Datensatz in der EF angeordnet ist, darf das UPDATE (next) keine Verschiebung des Datensatzzeigers bewirken, und es dürfen keine Satzdaten aktualisiert werden;

- PREVIOUS-Modus: Der Datensatzzeiger wird vor der Durchführung der UPDATE RECORD-Funktion dekrementiert. Falls der Datensatzzeiger innerhalb der ausgewählten EF zuvor nicht festgelegt wurde, dann muß das UPDATE (previous) den letzten Datensatz in der EF aktualisieren und den Datensatzzeiger für diesen Datensatz festlegen. Wenn der Datensatzzeiger bereits auf dem ersten Datensatz in der EF lokalisiert ist, darf das UPDATE (previous) keine Verschiebung des aktuellen Speicherplatzes bewirken, und es dürfen keine Satzdaten aktualisiert werden (außer bei einer zyklischen Datei);

- FIRST-Modus und LAST-Modus: Der Datensatzzeiger wird zum ersten oder letzten Datensatz, bevor die UPDATE RECORD-Funktion ausgeführt wird.

Die Funktion wird nach den ACs durchgeführt, die für diese EF bei der UPDATE-Funktion definiert sind.

Sofern für eine EF die UPDATE-Funktion zugelassen ist, ist die DECREASE-Funktion für diese EF nicht zugelassen (siehe Abschnitte 7.1.4 und 9.3.1).

Die Eingabe darf nur aus den Eingabedaten a, b bestehen, außer, wenn AC = PRO (siehe unten).

Falls AC = PRO ist, muß die Eingabe aus den Eingabedaten a, b und c bestehen. Die Karte muß die Herkunft und den Inhalt des Befehls durch Verifizierung des Kryptogramms (Eingabe c) authentifizieren, das vom Endgerät/von der Anwendung aus den Eingabeparametern (a, b) und der Zufallszahl berechnet wird, die zuvor von der Karte nach einer ASK RANDOM-Funktion angegeben wurde. Die UPDATE-Funktion darf von der Karte nicht ausgeführt werden, wenn die Verifizierung des Kryptogramms nicht ordnungsgemäß ist. Der für diese Verifizierung verwendete Schlüssel muß für die UPDATE-Funktionen in den ACs der aktuellen EF angegeben sein.

Eingabe: a/ Anzeige erste/letzte/nächste/vorherige/aktuelle oder absolute (Datensatznummer) und die Länge der zu ändernden Daten (in Byte);
b/ die zu ändernden Daten des Datensatzes;
c/ Kryptogramm.
Beschreibung der Eingabedaten siehe Abschnitt 9.2.8.

Ausgabe: Keine.

8.9 CREATE RECORD

Die Funktion ermöglicht das Anfügen (und Auffüllen) eines Datensatzes am logischen Ende einer EF des linearen oder zyklischen Typs. Diese Funktion kann nach den ACs ausgeführt werden, die für diese EF für die CREATE RECORD-Funktion definiert sind.

Die Eingabe darf nur aus (a) bestehen, außer bei AC = PRO (siehe unten).

Wenn AC = PRO ist, muß die Eingabe nur aus den Eingabedaten a, b bestehen. Die Karte muß die Herkunft und den Inhalt des Befehls durch Verifizierung des Kryptogramms (Eingabe b) authentifizieren, das vom Endgerät/von der Anwendung aus dem Eingabeparameter (a) und der zuvor

²⁾ Der Kartenausgeber muß gewährleisten, daß es keine Beeinträchtigung zwischen den Anwendungen gibt.

von der Karte nach einer ASK RANDOM-Funktion angegebenen Zufallszahl berechnet wird. Die CREATE RECORD-Funktion darf von der Karte nicht ausgeführt werden, wenn die Verifizierung des Kryptogramms nicht ordnungsgemäß ist. Der für die Verifizierung verwendete Schlüssel muß in der AC der aktuellen EF für die CREATE RECORD-Funktion angegeben sein.

Der Datensatzzeiger verweist auf den neu generierten Datensatz in der aktuellen EF:

Eingabe: a/ Inhalt des Datensatzes;
b/ Kryptogramm.
Beschreibung der Eingabedaten siehe Abschnitt 9.2.9.

Ausgabe: Keine.

ANMERKUNG: Es ist bei dieser Funktion möglich, daß lineare Dateien vorliegen, die nur einmal geschrieben und nicht mehr überschrieben werden können (wie ein EPROM-Speicher). Das kann erreicht werden, indem die AC für WRITE oder UPDATE auf NEVER gesetzt werden. Folglich besteht die einzige Schreibmöglichkeit in einer derartigen EF in der Ausführung der CREATE RECORD-Funktion, die einer Datei einen neuen Datensatz anfügt.

8.10 READ BINARY

Diese Funktion ermöglicht das Lesen einer Folge von Bytes in der aktuellen EF (die eine transparente EF sein muß). Die Funktion kann nach den AC durchgeführt werden, die für die READ-Funktionen für diese EF definiert wurden.

Eingabe: a/ relative Adresse (Offset) zu Beginn der EF und die Länge (in Bytes) der zu lesenden Folge;

Ausgabe: Daten;
Beschreibung der Ein- und Ausgabedaten siehe Abschnitt 9.2.10.

ANMERKUNG: AC = PRO ist bei dieser Funktion nicht anwendbar.

8.11 READ BINARY STAMPED

Die Funktionalität ist identisch mit READ BINARY des Abschnittes 8.10. Ergänzend fügt READ BINARY STAMPED den Ausgangsdaten ein Kryptogramm hinzu.

Vor Aussendung und der Berechnung eines Kryptogramms durch die Karte, muß mittels der Funktion GIVE RANDOM eine Anforderung an die Karte übergeben werden.

Die Eingaben bestehen aus (a) und die Ausgaben müssen aus (a,b) bestehen. Der zu benutzende, relevante Schlüssel ist in den AC der READ-Funktion definiert.

Eingabe: a/ relative Adresse (Offset) vom Beginn des EF und die Länge (in Bytes) der zu lesenden Folge;

Ausgabe: a/ Daten;
b/ Kryptogramm.
Beschreibung der Ein- und Ausgabedaten siehe Abschnitt 9.2.11.

ANMERKUNG: AC = PRO ist bei dieser Funktion nicht anwendbar.

8.12 READ RECORD

Diese Funktion erlaubt es, einen Datensatz aus der aktuellen EF zu lesen. Es muß sich um eine lineare oder zyklische EF handeln. Der zu lesende Datensatz kann der aktuellen, der nächste oder der vorherige Datensatz sein, was sich auf die zuvor ausgeführten Funktionen READ, UPDATE oder SEEK bezieht. Es kann sich auch um den ersten, letzten oder den durch seine Satznummer angezeigten Datensatz handeln.

Sechs Betriebsarten sind definiert:

- CURRENT-Modus und ABSOLUTE-Modus: Der Datensatzzeiger wird durch diese Funktion nicht beeinflusst;

- NEXT-Modus: Der Datensatzzeiger wird vor Durchführung der READ RECORD-Funktion inkrementiert. Wenn der Datensatzzeiger innerhalb der ausgewählten EF zuvor nicht festgelegt wurde, dann muß READ (next) den ersten Datensatz in der EF lesen und den Datensatzzeiger auf diesen Datensatz setzen. Falls der Datensatzzeiger bereits auf den letzten Datensatz in der EF zeigt, darf das READ (next) keine Verschiebung des Datensatzzeigers bewirken, und es dürfen keine Satzdaten zurückgesendet werden (außer bei einer zyklischen Datei);

- PREVIOUS-Modus: Der Datensatzzeiger wird vor Durchführung der READ RECORD-Funktion dekrementiert. Falls der Datensatzzeiger innerhalb der ausgewählten EF zuvor nicht festgelegt wurde, dann muß READ (previous) den letzten Datensatz in der EF lesen und den Datensatzzeiger auf diesen Datensatz setzen. Wenn der Datensatzzeiger bereits auf den ersten Datensatz in der EF zeigt, darf das READ (previous) keine Verschiebung des Datensatzzeigers bewirken, und es dürfen keine Datensätze zurückgesendet werden (außer bei einer zyklischen Datei);

- FIRST-Modus und LAST-Modus: Der Datensatzzeiger zeigt auf den ersten oder den letzten Datensatz, bevor die READ RECORD-Funktion ausgeführt wird.

Die Funktion kann nach den für diese EF für die READ-Funktionen definierten ACs durchgeführt werden.

Eingabe: Anzeige aktuelle/vorherige/nächste/erste/letzte oder absolute (Datensatznummer).

Ausgabe: die Daten des gelesenen Datensatzes;
Beschreibung der Ein- und Ausgabedaten siehe Abschnitt 9.2.12.

ANMERKUNG: AC = PRO ist auf diese Funktion nicht anwendbar.

8.13 READ RECORD STAMPED

Die Funktionalität ist identisch mit READ RECORD des Abschnittes 8.12. Ergänzend fügt READ RECORD STAMPED den Ausgangsdaten ein Kryptogramm hinzu.

Vor Aussendung und der Berechnung eines Kryptogramms durch die Karte, muß mittels der Funktion GIVE RANDOM eine Anforderung an die Karte übergeben werden.

Die Eingaben bestehen aus (a) und die Ausgaben müssen aus (a) und (b) bestehen. Der zu benutzende, relevante Schlüssel ist in den ACs der READ-Funktion definiert.

Eingabe: a/ zeigt auf aktuelle/ vorherige/ nächste/ erste/ letzte, oder absolute Datensatznummer;

Ausgabe: a/ Daten des gelesenen Datensatzes;
b/ Kryptogramm.
Beschreibung der Ein- und Ausgabedaten siehe Abschnitt 9.2.13.

ANMERKUNG: AC = PRO ist bei dieser Funktion nicht anwendbar.

8.14 SEEK

Diese Funktion gestattet die Lagebestimmung eines Datensatzes, der ein bestimmtes Muster innerhalb der aktuellen EF enthält. Die Funktion gilt für alle EF-Arten, die Datensätze enthalten.

Nach einem erfolgreichen SEEK wird der gefundene Datensatz durch den Datensatzzeiger gekennzeichnet. Nach einem nicht erfolgreichen SEEK muß der Datensatzzeiger unverändert bleiben.

Eingabe: a/ Offset, Antwortart, Such-Betriebsart, Länge des Musters;
b/ Muster.
Beschreibung der Eingabedaten siehe Abschnitt 9.2.14.

Ausgabe: Keine oder Datensatznummer.
Beschreibung von eventuellen Ausgabedaten siehe Abschnitt 9.2.14.

ANMERKUNG 1: Das SEEK wird über die Länge des Musters durchgeführt. Wenn keine Bedingungen übereinstimmen, wird angegeben, daß der Datensatz nicht gefunden wurde (Datensatz kürzer als die Musterlänge = keine Übereinstimmung).

SEEK vom nächsten Speicherplatz nach vorne: wenn der Positionsanzeiger zuvor nicht innerhalb der ausgewählten Datei war, beginnt die Suche beim ersten Datensatz der ausgewählten Datei.

SEEK vom vorherigen Speicherplatz nach hinten: wenn der Positionsanzeiger zuvor nicht innerhalb der ausgewählten Datei war, beginnt die Suche beim letzten Datensatz der ausgewählten Datei.

ANMERKUNG 2: AC = PRO ist auf diese Funktion nicht anwendbar.

8.15 VERIFY CHV

Diese Funktion ermöglicht die Verifizierung der CHV, die in der für die aktuelle Datei relevanten EF_{CHV} definiert ist (siehe Abschnitt 7.1).

Diese Funktion muß vor einer Aktion auf die aktuelle Datei verbindlich angewendet werden, falls die AC für diese Datei die Bedingungen CHV1 oder CHV2 einschließt. Wenn die angebotene CHV falsch ist, muß der Zähler für die Anzahl der restlichen CHV-Versuche dekrementiert werden. Wenn die vorhandene CHV ordnungsgemäß ist, muß der Zähler der restlichen CHV-Versuche auf N zurückgesetzt werden.

Nach N aufeinanderfolgenden falschen CHV-Eingaben muß die jeweilige CHV gesperrt werden, und die AC (CHV1 oder CHV2) können so lange nicht erfüllt werden, bis die Funktion UNBLOCK CHV erfolgreich ausgeführt wurde.

Die CHV kann entsprechend dem Darstellungstyp, der für diese CHV definiert und in der zugehörigen EF_{CHV} angegeben wurde, als Klartext oder verschlüsselt eingegeben werden. Es ist Aufgabe des Betriebssystems, die Art und Weise der Darbietung der CHV entsprechend der EF_{CHV} zu verwalten.

Wenn die zugehörige EF_{CHV} anzeigt, daß die CHV verschlüsselt anzubieten ist, muß die Eingabe aus a und b, und zwar aus verschlüsselten Eingabedaten bestehen. Die Verschlüsselung ist vom Endgerät/von der Anwendung durchzuführen, bevor die CHV der Karte angeboten wird. Der Verschlüsselungsvorgang bezieht die Zufallszahl (zur Berechnung des Kryptogramms) ein, die zuvor von der Karte nach einer ASK RANDOM-Funktion übergeben wird, während der relevante Schlüssel für die verschlüsselte CHV-Darbietung in der entsprechenden EF_{CHV} definiert sein muß.

Eingabe: a/ Anzeige CHV1/CHV2 (P2 des Vorderteils);
b/ die CHV (verschlüsselt oder nicht verschlüsselt) muß 8 Bytes lang sein. Bei biometrischen CHV kann die Länge davon abweichen. Falls die CHV keine 8 Bytes enthält, muß das Endgerät die fehlenden Bytes der CHV nach rechts mit binären Einsen auffüllen (siehe prEN 726-4, Abschnitt 10.3.3).
Beschreibung der Eingabedaten siehe Abschnitt 9.2.15.

Ausgabe: Keine.

ANMERKUNG: Für diese Funktion werden keine ACs definiert.

8.16 CHANGE CHV

Diese Funktion ermöglicht es den CHV (der die aktuelle Datei schützt) zu ändern, jedoch nur bei Erfüllung folgender Bedingungen:

- 1) Die Anzeige 'CHV-Änderung zulässig oder nicht' (angegeben in der SELECT-Antwort usw.) ist positiv.
- 2) Die CHV ist nicht deaktiviert.
- 3) Die CHV ist nicht gesperrt.

Die alte und die neue CHV können im Klartext oder verschlüsselt angeboten werden, abhängig von der Definition dieser EF, welche im relevanten EF_{CHV} (siehe Abschnitt 7.1) der aktuellen Datei angegeben ist. Die jeweilige Schlüsselnummer für eine verschlüsselte CHV-Darstellung ist ebenfalls in dieser EF_{CHV} definiert.

Falls die dargebotene CHV nicht ordnungsgemäß ist, muß der CHV-Zähler für verbleibende Versuche dekrementiert werden. Nach N aufeinanderfolgenden falschen CHV-Darstellungen muß die jeweilige CHV gesperrt werden, und die AC (CHV1 oder CHV2) können so lange nicht erfüllt werden, bis die Funktion UNBLOCK CHV erfolgreich ausgeführt wurde.

Falls die relevante EF_{CHV} anzeigt, daß die CHVs verschlüsselt dargestellt werden müssen, ist die Verschlüsselung durch das Endgerät/die Anwendung auszuführen, bevor die CHVs der Karte angeboten werden. Der Verschlüsselungsvorgang bezieht die Zufallszahl ein, die vorher von der Karte nach einer ASK RANDOM-Funktion (zur Berechnung des Kryptogramms) übergeben wurde, während der jeweilige Schlüssel für die verschlüsselte CHV-Darstellung in der jeweiligen EF_{CHV} definiert sein muß.

Eingabe: a/ Anzeige CHV1/CHV2 (P2 des Vorderteils);
b/ alte CHV, neue CHV (beide verschlüsselt oder nicht verschlüsselt), beide mit einer Länge von 8 Byte (bei biometrischem CHV kann die Länge davon abweichen). Falls die CHV keine 8 Bytes enthält, muß das Endgerät die fehlenden Bytes der CHV nach rechts mit binären Einsen auffüllen (siehe prEN 726-4, Abschnitt 10.3.3).

Beschreibung der Eingabedaten siehe Abschnitt 9.2.16.

Ausgabe: Keine.

ANMERKUNG: Für diese Funktion sind keine ACs definiert.

8.17 DISABLE CHV

Diese Funktion wirkt auf die jeweilig relevante EF_{CHV} . Die Absicht ist es, die Überprüfung der jeweiligen CHV auszuschalten. Eine erfolgreiche CHV-Überprüfung ist zur Erfüllung der AC = CHV nicht erforderlich.

Diese Funktion darf nur möglich sein, wenn DISABLE/ENABLE CHV für die jeweilige CHV zulässig ist (siehe SELECT RESPONSE im Falle von EF_{CHV}). Die Deaktivierung von CHV bleibt solange gültig, bis sie mit der Funktion ENABLE CHV wieder eingeschaltet wird.

Falls die relevante EF_{CHV} anzeigt, daß die CHV verschlüsselt zu übergeben ist, muß die Verschlüsselung durch das Endgerät/die Anwendung ausgeführt werden, bevor die CHV der Karte übergeben wird. Der Verschlüsselungsvorgang bezieht die Zufallszahl ein, die vorher von der Karte nach einer ASK RANDOM-Funktion (zur Berechnung des Kryptogramms) übergeben wurde, während der jeweilige Schlüssel für die verschlüsselte CHV-Darstellung in der jeweiligen EF_{CHV} definiert sein muß.

Die Funktion DISABLE CHV darf nicht ausgeführt werden, wenn die CHV bereits deaktiviert oder gesperrt ist. Falls die angebotene CHV nicht ordnungsgemäß ist, muß der CHV-Versuchszähler dekrementiert werden. Nach N aufeinanderfolgenden falschen CHV-Darstellungen ist die jeweilige