

Identifikationskartensysteme
Chipkarten und Endgeräte für Telekommunikationszwecke
 Teil 7: Sicherheitsmodul
 Deutsche Fassung EN 726-7 : 1999

DIN
EN 726-7

ICS 35.240.15

Identification card systems – Telecommunications integrated circuit(s)
 cards and terminals – Part 7: Security module;
 German version EN 726-7 : 1999

Systèmes de cartes d'identification – Cartes à circuit intégré et terminaux
 pour les télécommunications – Partie 7: Module de sécurité;
 Version allemande EN 726-7 : 1997

Die Europäische Norm EN 726-7 : 1999 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 STC-TE9 zurück. Zuständig in Deutschland ist NI-17 "Identifikationskarten".

Fortsetzung 57 Seiten EN

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

– Leerseite –

Deutsche Fassung

Identifikationskartensysteme

Chipkarten und Endgeräte für Telekommunikationszwecke

Teil 7: Sicherheitsmodul

Identification card systems – Telecommunications integrated circuit(s) cards and terminals –
Part 7: Security module

Systèmes de cartes d'identification – Cartes à circuit intégré et terminaux pour les télécommunications –
Partie 7: Module de sécurité

Diese Europäische Norm wurde von CEN am 1. Januar 1999 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, der Tschechischen Republik 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
Vorwort	3
1 Zweck	3
2 Normative Verweisungen	3
3 Begriffe und Abkürzungen	4
3.1 Begriffe	4
3.2 Abkürzungen	5
4 Physikalische Eigenschaften des SM	6
5 Elektronische Signale und Übertragungsprotokolle	6
6 Logisches Modell für ein SM	6
7 Allgemeine Konzeptionen	7
7.1 Allgemeine Sicherheitsprinzipien	7
7.1.1 Zugriffsbedingungen	7
7.1.2 Ablaufkontrolle	7
7.2 SM-Lebenszyklus	8
7.3 Konfiguration des Systems	8
7.4 SM-Sicherheitsfunktionen	9
8 Beschreibung der Funktionen eines SM	10
8.1 Funktionen ohne MAC	10
8.1.1 SELECT KEYSET	10
8.1.2 DIVERSIFY KEYSET	11
8.1.3 ASK PARAMETER	11
8.2 Funktionen zur Berechnung eines Kryptogramms oder der Codes für die Nachrichtenauthentikation (MAC)	12
8.2.1 COMPUTE LOAD KEY	12
8.2.2 COMPUTE MAC	13
8.2.3 COMPUTE CRYPTOGRAM	14
8.3 Funktionen zur Überprüfung von Kryptogrammen oder der Codes für die Nachrichtenauthentikation (MAC)	15
8.3.1 VERIFY MAC	15
8.3.2 UPDATE (SM)	16
8.3.3 INCREASE (SM)	17
8.3.4 DECREASE (SM)	18
8.3.5 VERIFY CRYPTOGRAM	19
8.4 Funktionen für das Herunterladen von Schlüsseln vom SM zur UC	19
8.5 Funktionalität der SM-EW-Schnittstelle	19
8.6 Anbindung von Funktionen an Schlüssel	20
8.7 Beschränkungen für die Benutzung von Schlüsseln	20
9 Datenelemente	21
9.1 Daten für die Identifizierung des SM	21
9.1.1 SM-Identifikator	21
9.2 UC-Daten	21
9.2.1 IC-Seriennummer der Nutzerkarte	21
9.2.2 Verfallsdatum der Anwendung	21
9.2.3 Anwendungs-Identifikator (AID)	21
9.2.4 Version der Schlüsseldatei	21
9.2.5 Algorithmus-Identifikator	21
9.2.6 Betrag	22
9.2.7 Wert	22
9.2.8 Typ der Einheiten	22
9.3 Vom SM zurückgesendete Statusbedingungen	22
9.3.1 Funktionen im Verhältnis zu möglichen Statusantworten	22
Anhang A (normativ) Ein SM in Form einer IC-Karte	26
Anhang B (informativ) Beispiele für Ablauffolgen für SMs in Form einer IC-Karte	42
Anhang C (informativ) Literaturhinweise	57

Vorwort

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

Diese Europäische Norm muß den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juli 1999, und etwaige entgegenstehende nationale Normen müssen bis Juli 1999 zurückgezogen werden.

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

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

1 Zweck

Dieser Teil von EN 726 legt fest:

- die Mindest-Sicherheitsanforderungen für ein Sicherheitsmodul (SM);
- die allgemeinen kartenbezogenen Funktionen, die in das SM integriert sind – Endgeräteprotokolle einschließlich eines minimalen Datenaustauschs; die in Anhang A beschriebenen Datenelemente und die kryptographische Verarbeitung, für den Fall, daß das SM eine ICC ist, sollten unterstützt werden, wenn das SM keine ICC oder keine Systemkonfiguration ist, z. B. wenn das SM mehr als ein Endgerät bzw. mehr als eine Nutzerkarte betrifft. Konfigurationen, bei denen das SM mehr als ein Endgerät bzw. mehr als eine Nutzerkarte betrifft, werden in dieser Norm nicht vollständig festgelegt. Zur Realisierung dieser Konfigurationen dürfen möglicherweise weitergehende Mechanismen erforderlich sein;
- die notwendigen Sicherheitsdienste und -mechanismen zur Bereitstellung von anwendungsbezogenen und kryptographischen Sicherheitsinformationen für die Verarbeitung von Transaktionen der Telekommunikation.

Dabei werden verschiedene Typen von SMs an unterschiedlichen Positionen im System und in unterschiedlichen Systemkonfigurationen betrachtet.

Dieser Teil von EN 726 läßt eine Interaktion zwischen der Chipkarte (IC-Karte) und dem SM über das Endgerät in einer Weise zu, die für das Endgerät und möglicherweise auch für das Netzwerk (die Netzwerke) funktionell transparent ist. Das bietet Flexibilität bei der Verwendung unterschiedlicher Techniken, Befehls- und Nachrichtenformate an der Schnittstelle Endgerät – SM.

Dieser Teil von EN 726 unterstützt IC-Karten mit Anwendungen für die Zahlungsfunktion nach EN 726-5 und alle Kartenanwendungen gemäß den Abschnitten 4 bis 7 dieses Teils von EN 726. Er unterstützt ebenfalls IC-Karten nach EN 726-3 : 1994. Andere Telekommunikationskarten, die nicht EN 726 entsprechen, z. B. einfache Speicherkarten, können auch durch das in diesem Teil beschriebene SM unterstützt werden.

2 Normative Verweisungen

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

EN 726-2 : 1995

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

EN 726-3 : 1994

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

EN 726-5

Identifikationskartensysteme – Anforderungen an Chipkarten und Endgeräte für Telekommunikationszwecke – Teil 5: Bezahlungsmethoden

EN 24217

Kodes für die Angaben von Währungen und Geldmitteln (ISO 4217 : 1990)

EN ISO/IEC 7816-4

Informationstechnologie – Identifikationskarten – Karten mit integrierten Schaltkreisen und Kontakten – Teil 4: Interindustrielle Kommandos (ISO/IEC 7816-4 : 1995)

EN ISO/IEC 7816-5

Identifikationskarten – Chipkarten mit Kontakten – Teil 5: Numerierungssystem und Registrierverfahren für Anwendungsbezeichner (ISO/IEC 7816-5 : 1994)

ISO 10202-4

Financial transactions cards – Security architecture of financial transaction systems using integrated circuit cards – Part 4: Secure application modules

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Teils der Norm gelten folgende Definitionen.

3.1.1 Zugriffsbedingungen (AC): Eine Menge von Sicherheitsattributen, die einer Datei zugeordnet sind.

3.1.2 Anwendung: Eine Anwendung besteht aus einer Menge von Sicherheitsmechanismen, Dateien, Daten und Protokollen (mit Ausnahme von Übertragungsprotokollen), die sich auf der IC-Karte und außerhalb der IC-Karte (externe Anwendung) befinden und dort verwendet werden.

3.1.3 Anwendungsanbieter (AP): Die Instanz, die für die Anwendung nach ihrer Zuteilung verantwortlich ist. Ein AP kann mehrere Anwendungen auf einer Karte haben. Die Dateien, die auf der Karte einer Einheit entsprechend zugeteilt werden, werden eine Kartenanwendung genannt. Auf einer gegebenen Karte können mehrere Anwendungen von demselben Anwendungsanbieter oder von verschiedenen Anwendungsanbietern existieren.

3.1.4 Anwendungssitzung: Eine Verbindung zwischen dem Anwendungsteil der Karte und dem Anwendungsteil der externen Welt derselben Anwendung.

3.1.5 Anwendungsspezifischer Befehlssatz (ASC): Zu einer DF kann wahlfrei ein ASC-Satz zugeordnet werden (ein anwendungsspezifischer Befehlssatz und/oder ein anwendungsspezifisches Programm). Das bedeutet, daß bei der Auswahl dieser Anwendung der allgemeine Befehlssatz durch diesen spezifischen Befehlssatz erweitert oder modifiziert wird. Der ASC ist für den gesamten Teilbaum dieser Anwendung gültig, wenn nicht andere ASCs auf niedrigeren Ebenen dieser Anwendung festgelegt sind.

3.1.6 Karte: Eine Karte für eine Mehrfachanwendung kann als eine Menge von Dateien betrachtet werden, von denen sich einige die unterschiedlichen Anwendungsanbieter und/oder der Kartenherausgeber teilen. Andere Dateien gehören ausschließlich den unterschiedlichen Anwendungsanbietern oder dem Kartenherausgeber. Dateien können z. B. gelesen, geschrieben oder ausgeführt werden.

3.1.7 Zugeordnete Datei (DF): Eine Datei, die AC und zuteilbaren Speicher enthält. Sie kann der Parent von Elementar-Dateien und/oder zugeordneten Dateien sein.

3.1.8 Elementar-Datei (EF): Eine Datei, die AC, Daten oder ein Programm und keine anderen Dateien enthält als:

- **EF_{DIR}** ist eine Elementar-Datei auf der Ebene der Haupt-Datei oder der DF, die eine Liste aller oder eines Teils aller verfügbaren Anwendungen auf der Karte enthält;
- **EF_{ID}** ist eine Elementar-Datei auf der Ebene der Haupt-Datei, die die Identifikationsnummer der Karte enthält;
- **EF_{ICC}** ist eine Elementar-Datei auf der Ebene der Haupt-Datei, die allgemeine Informationen enthält, die den IC und die IC-Karte betreffen;
- **EF_{KEY_OP}** ist eine Elementar-Datei, die Betriebs-Schlüssel enthält;
- **EF_{KEY_MAN}** ist eine Elementar-Datei, die Management-Schlüssel enthält;
- **EF_{DIK_OP}** ist eine Elementar-Datei, die diversifizierte Betriebs-Schlüssel enthält;
- **EF_{DIK_MAN}** ist eine Elementar-Datei, die diversifizierte Management-Schlüssel enthält.

3.1.9 Datei-Identifikator (ID): Jede Datei (MF, DF, EF) hat einen Identifikator, der aus 2 Bytes besteht.

3.1.10 Schlüsselkennzeichner: Eine eindeutige Datenmenge zur Auswahl einer spezifischen Schlüsselmenge im SM.

3.1.11 Haupt-Datei (MF): Die obligatorische, eindeutige Datei, die das Stammverzeichnis der Dateistruktur darstellt und AC und zuteilbaren Speicher enthält. Die Haupt-Datei können die Parent- oder Elementar-Dateien und/oder die zugeordneten Dateien sein.

3.1.12 Betriebssystem: System, das zur Verwaltung der logischen Ressourcen eines Systems einschließlich der Prozeßzeitplanung und des Dateimanagements notwendig ist.

3.1.13 Pfad: Verkettung von Datei-Identifikatoren ohne Begrenzung.

3.1.14 Sicherheitsinformationen: Algorithmus (Algorithmen), zugehörige(r) Schlüssel, Sicherheitsprozeduren und Informationen.

3.1.15 Sicherheitsmodul: Ein Gerät, das logisch und physikalisch geschützte geheime Informationen enthält – Algorithmus (Algorithmen), zugehörige(r) Schlüssel, Sicherheitsprozeduren und Informationen zum Schutz von Anwendungen in einer Weise, daß ein unberechtigter Zugriff nicht durchführbar ist. Um das zu erreichen, darf das Modul darüber hinaus physikalisch, elektrisch und logisch geschützt werden.

3.1.16 Sicherheitsmodulanbieter: Siehe ISO 10202-4.

3.1.17 Ablaufkontrolle: Eine Zusatzeinrichtung, die garantiert, daß durch Befehle aufgerufene Operationen durch das SM nur in zugelassener (zugelassenen), vordefinierter (vordefinierten) Reihenfolge(n) ausgeführt werden können.

3.2 Abkürzungen

AC	(Access Condition) Zugriffsbedingung	INV	(Invalidate) ungültig machen
AID	(Application IDentifier) Anwendungs-Identifikator	LEN	(Length) Länge
AUT	(Authenticated) authentiziert	MAC	(Message Authentication) Nachrichtenauthentikation
CHV	(Card Holder Verification Information) Information zur Überprüfung des Karteninhabers	MF	(Master File) Haupt-Datei
DF	(Dedicated File) zugeordnete Datei	NEV	(Never) nie
EF	(Elementary File) Elementar-Datei	PRO	(Protected) geschützt
EW	(External World) externe Welt	RAN	(Random) zufällig
IC	(Integrated Circuit) integrierter Schaltkreis	REH	(Rehabilitate) wieder einsetzen
ICC	(Integrated Circuit Card) Chipkarte	RFU	(Reserved for Future Use) für spätere Verwendung freigehalten
ID	(Identifier of a file) Identifikator einer Datei	SM	(Security Module) Sicherheitsmodul
IFD	(Interface Device) Kartenzugangsgerät	UC	(User Card) Nutzerkarte
INT. AUTH	(Internal Authentication) interne Authentikation		

4 Physikalische Eigenschaften des SM

Wenn das SM eine IC-Karte ist, müssen die physikalischen Eigenschaften Abschnitt 4, EN 726-3 : 1994, entsprechen.

Für alle anderen Fälle liegen die physikalischen Eigenschaften außerhalb des Anwendungsbereiches dieser Norm.

5 Elektronische Signale und Übertragungsprotokolle

Wenn das SM eine IC-Karte ist, müssen die elektronischen Signale und das (die) Übertragungsprotokoll(e) Abschnitt 5, EN 726-3 : 1994, entsprechen.

Für alle anderen Fälle liegen die elektronischen Signale und das Übertragungsprotokoll außerhalb des Anwendungsbereiches dieser Norm.

6 Logisches Modell für ein SM

Ein SM, das dieser Norm entspricht, umfaßt:

- permanente Sicherheitsinformationen (Masterschlüssel);
- temporäre Sicherheitsinformationen (diversifizierte(r) Schlüssel);
- ein Saldo (wahlfrei);
- ein Betriebssystem zur Handhabung eines sicheren Zugriffs auf die oben erwähnten Sicherheitsinformationen. Solange sie die Grundinhalte nicht beeinträchtigen, sind zusätzliche wahlfreie Angaben möglich, aber diese liegen außerhalb des Anwendungsbereiches dieser Norm.

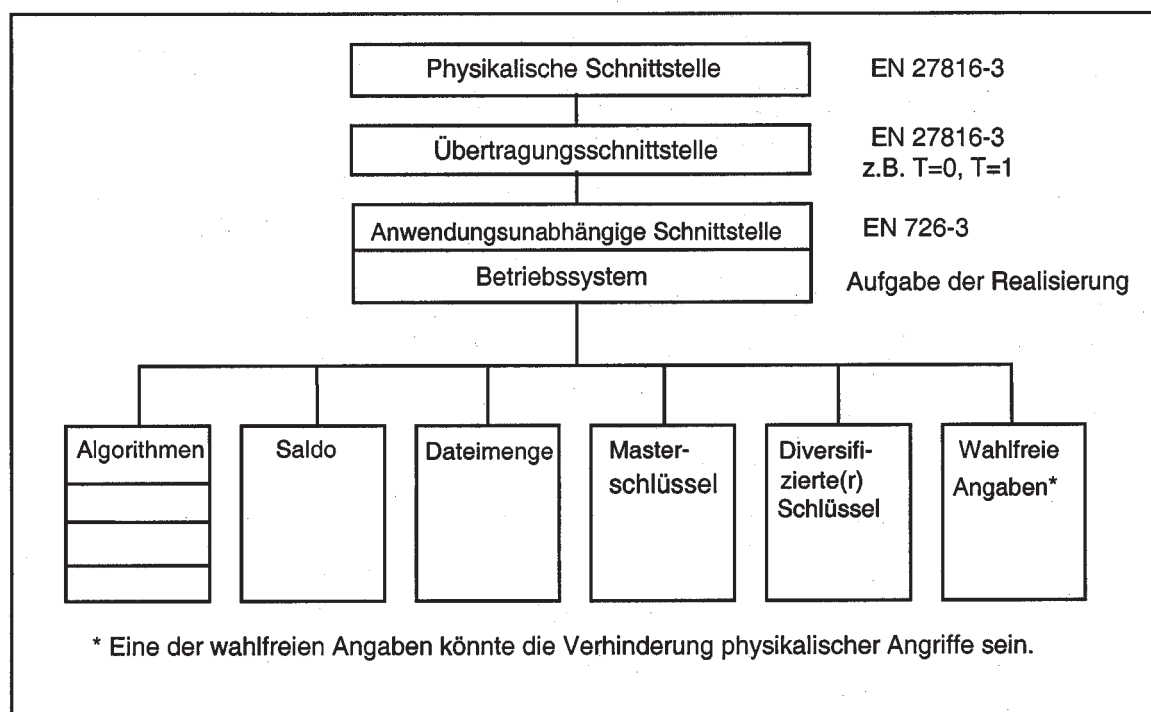


Bild 1: Allgemeine Struktur eines SM

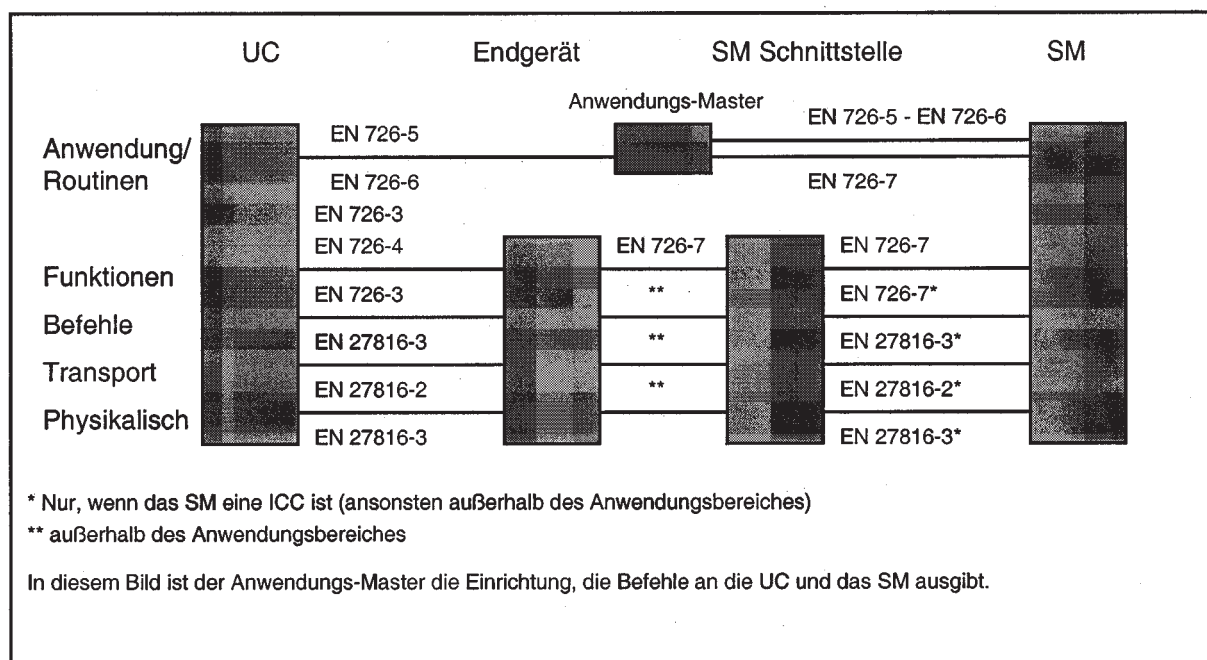


Bild 2: Genormte Kommunikation zwischen einer UC und einem SM

7 Allgemeine Konzeptionen

7.1 Allgemeine Sicherheitsprinzipien

Der SM-Anbieter muß für den Lebenszyklus des SM verantwortlich sein.

Weder ein Aspekt beim Betrieb eines SM noch Daten, die von einem SM erhältlich sind, dürfen die Sicherheit des Systems gefährden.

Im SM und der UC verwendete kryptographische Schlüssel müssen auf solche Weise verwaltet werden, daß die Sicherheit eines Systems, das SMs oder UCs verwendet, nicht gefährdet wird.

Während des Lebenszyklus der Anwendung kann die Notwendigkeit auftreten, Schlüssel auf der UC auszutauschen. Um das zu unterstützen, darf das SM mehrere Versionen einer Schlüsselmenge enthalten.

Die Fähigkeit zur Zusammenarbeit vom Telekommunikations-SMs in Europa beruht auf dem Austausch von geheimen Schlüsseln. Die Mechanismen für das Herunterladen von Schlüsseln in das SM werden in diesem Teil der EN 726 nicht beschrieben. Die Trennung der Schlüsselmanagement-Systeme zwischen verschiedenen Betreibern erfordert den Einsatz einer Vertrauensstelle.

7.1.1 Zugriffsbedingungen

Für die in diesem Teil der Norm beschriebenen Funktionen sind keine ACs im SM zu erfüllen, aber der Gebrauch der Schlüssel kann eingeschränkt sein. Das SM verwendet diversifizierte Schlüssel für Funktionen auf der UC, bei denen die ACs eine Schlüsseloperation erfordern. Für das Management des SM durch die Externe Welt müssen die in EN 726-3 : 1994 festgelegten ACs nur gelten, wenn das SM eine IC-Karte ist.

Das SM darf auch eine Schlüsseldiversifikation für Anwendungsspezifische Funktionen auf der UC ausführen, die nicht in EN 726-3 : 1994 festgelegt sind. In diesem Fall müssen die Anwendungsbeschränkungen für den (die) Schlüssel für diese spezifische Funktion im SM eingehalten werden.

7.1.2 Ablaufkontrolle

Eine Ablaufkontrolle kann durch Verwendung der ACs der UC auf das SM erreicht werden. Ablaufkontrollfunktionen, bei denen das SM prüft, ob es zugelassen ist, Befehle und Statusantworten auszuführen, können wahlfrei hinzugefügt werden, falls sie in der Anwendung benötigt werden. Die Realisierung liegt außerhalb des Anwendungsbereiches dieser Norm. Trotzdem gilt folgendes, falls der Befehl zulässig ist, wird die Operation ausgeführt und die Ergebnisse sind das Resultat des Befehls. Falls der Befehl nicht zulässig ist, wird die Operation nicht ausgeführt und die Statusbedingungen werden enthalten "Befehl außerhalb der Reihenfolge". Die interne Reaktion des SM ist anwendungsabhängig.

7.2 SM-Lebenszyklus

Siehe ISO 10202-4.

7.3 Konfiguration des Systems

Die allgemeinen kartenbezogenen Funktionen bei der Schnittstelle Endgerät – SM schließen den minimalen Datenaustausch mit ein und dürfen nicht betroffen werden. Die Nutzerkarte-Endgerät-Schnittstelle darf durch den SM-Realisierungstyp nicht betroffen werden.

In den Bildern 3 bis 6 sind vier mögliche Konfigurationen des SM gezeigt.

Im Interesse der Vollständigkeit sind alle vier Positionen dargestellt. Es ist jedoch wahrscheinlich, daß für entferntere Positionen ein Transportprotokoll einer höheren Ebene geeignet sein kann. Solche Transportprotokolle höherer Ebenen liegen außerhalb des Anwendungsbereiches dieser Norm.

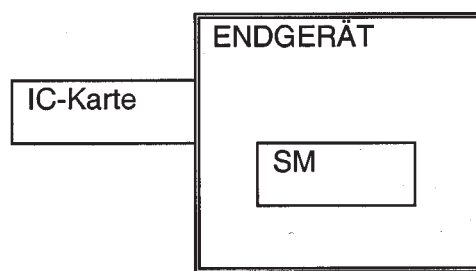


Bild 3: Im ENDGERÄT eingeschlossenes SM

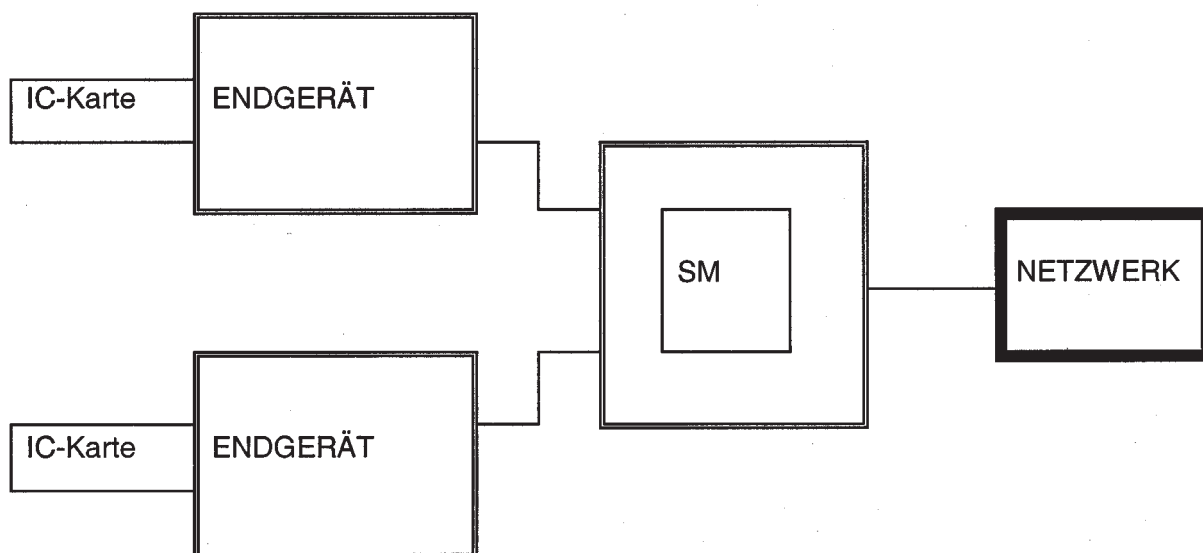


Bild 4: In einem lokalen Konzentrator eingeschlossenes SM

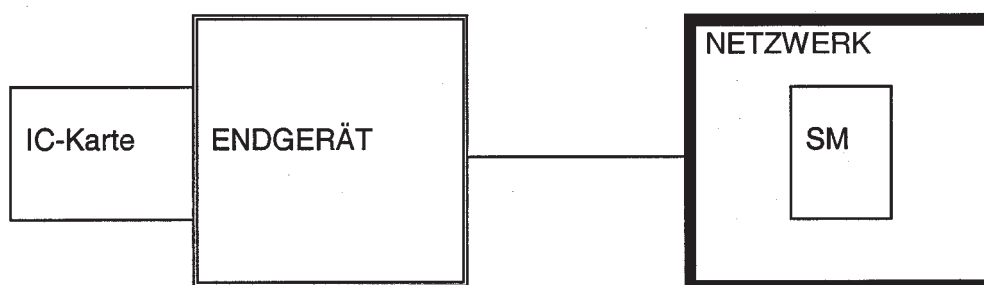


Bild 5: SM im Netzwerk

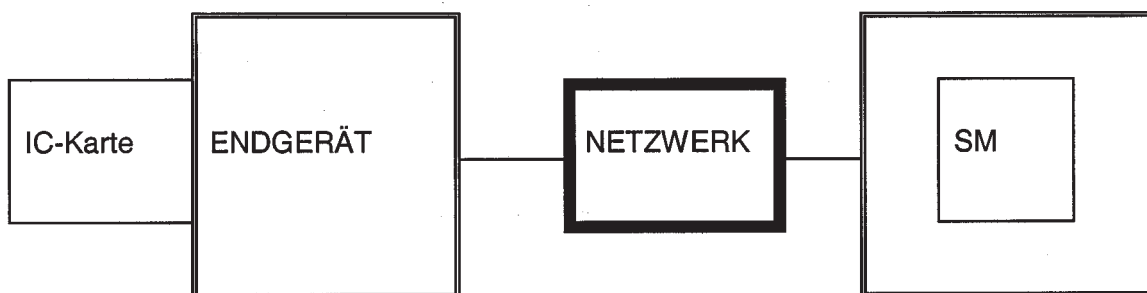


Bild 6: Entferntes SM

Eine Unterscheidung zwischen üblichen Operationen (Transfer von sensiblen Daten wie Zahlungstransaktionen) und sensitiveren Operationen (wie die Erzeugung von sensiblen Daten) kann notwendig sein. In diesem Fall können zwei Arten von SMs existieren. SM1, das sich in einer offenen Umgebung befindet, läßt nur übliche Operationen zu, und SM2 (und Endgerät), das sich in einer geschützten Umgebung befindet und zusätzlich z. B. Personalisierung zuläßt.

Für SMs, die sensitivere Operationen umfassen, sind als physikalischer Schutz besondere Sicherheitstools notwendig. Diese Anforderungen liegen außerhalb des Anwendungsbereiches dieser Norm.

7.4 SM-Sicherheitsfunktionen

Ein SM enthält:

- Sicherheitsinformationen, die zulassen, daß das Endgerät auf geschützte Teile der UC zugreift;
- Sicherheitsinformationen, die die Prüfung auf die Echtheit der UC zulassen;
- wahlfrei einen Saldo, der auf geschützte Weise im SM erhöht und vermindert werden kann, gekoppelt an eine zugehörige Umkehroperation auf der UC.

Ein SM muß logisch und physikalisch gegen Angriffe geschützt werden, die darauf abzielen, Sicherheitsinformationen während des ganzen Lebenszyklus eines SM offenzulegen oder zu mißbrauchen.

Alle Funktionen müssen unabhängig von Übertragungsprotokollen sein. Das kann an der Schnittstelle Endgerät – UC und an der Schnittstelle Endgerät – SM unterschiedlich sein.

Um für Dateien auf der UC AC = AUT oder PRO zu erfüllen, müssen alle zugehörigen Funktionen auf der UC und im SM dieselben Schlüssel und Algorithmen verwenden.

Im Sinne dieser Norm basiert die Funktionalität auf:

- symmetrischen Algorithmen;
- diversifizierten Schlüsseln.

Die Verwendung von asymmetrischen oder hybriden Kryptosystemen darf jedoch später festgelegt werden.

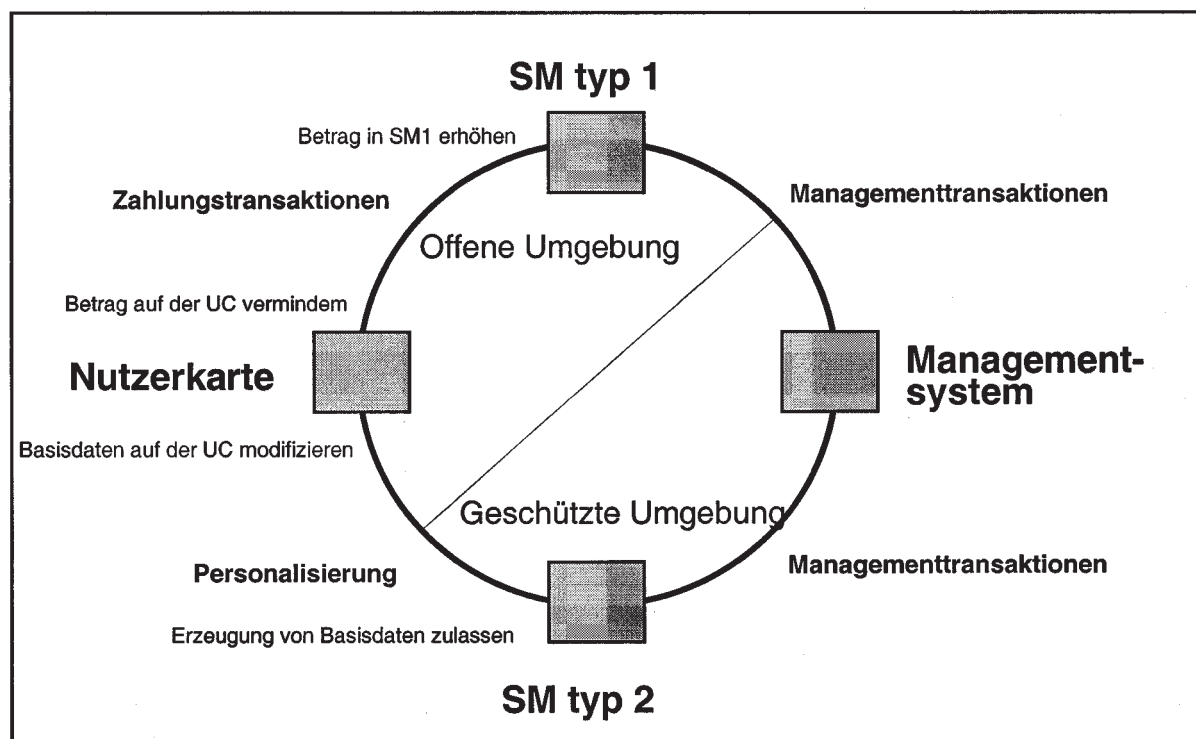


Bild 7: Ein Beispiel für eine Systemkonfiguration

8 Beschreibung der Funktionen eines SM

Dieser Abschnitt beschreibt nur die zusätzlichen spezifischen Funktionen, die für ein SM notwendig sind. Wenn das SM eine IC-Karte ist, gelten der restliche Teil dieses Abschnittes und Anhang A. Zusatzfunktionen zur Unterstützung anderer Anwendungen außerhalb des Bereichs der EN 726 sind nicht ausgeschlossen. Diese Funktionen dürfen nicht mit dem Inhalt der EN 726 kollidieren. Die in diesem Abschnitt angesprochenen Command-Header und Command-Nachsätze sind Datenelemente, die zur Steuerung der Datenverarbeitung durch das SM je nach spezifizierter Funktion verwendet werden.

8.1 Funktionen ohne MAC

8.1.1 SELECT KEYSET

Der Zweck dieser Funktion ist die eindeutige Adressierung einer spezifischen Schlüsselmenge in einem SM, die zu einem spezifischen Befehl, einer Datei, einer AC und einer Anwendung der UC gehört und die mindestens für die nächste kryptographische Berechnung verwendet werden muß. Falls eine UC nach EN 726-3 : 1994 verwendet wird, muß das SM eine Schlüsselmenge auswählen, die mit der von der UC angezeigten Schlüsseldatei-Version übereinstimmt.

Eingabe: a/ Command Header;
b/ Schlüsselkennzeichner:

Tabelle 1: Schlüsselkennzeichner (im Fall einer MF der UC)

Bytes	Beschreibung	Länge
1 bis 4	Herstellungshinweise der IC-Karte (codiert nach EN 726-3 : 1994)	4 Bytes
5	ID der personalisierenden Stelle der Karte (codiert nach EN 726-3 : 1994)	1 Byte
6 bis 7	Datei-ID von EF _{KEY}	2 Bytes
8	Version der Schlüsseldatei (codiert nach EN 726-3 : 1994)	1 Byte

Tabelle 2: Schlüsselkennzeichner (im Fall einer DF der UC)

Bytes	Beschreibung	Länge
1 – X	AID (codiert nach EN 726-3 : 1994)	1 bis 16 Bytes
(X + 1) – (X + 2)	Datei-ID von EF _{KEY}	2 Bytes
X + 3	Version der Schlüsseldatei (codiert nach EN 726-3 : 1994)	1 Byte

Ausgabe: a/ Daten: keine;
b/ Status.

8.1.2 DIVERSIFY KEYSSET

Der Zweck dieser Funktion ist die Ableitung temporärer Schlüssel aus allen in der vorhergehend ausgewählten Schlüsselmenge enthaltenen Masterschlüsseln unter Verwendung spezifischer Diversifikationsdaten. Die temporären Schlüssel werden in eine spezifische temporäre Datei geschrieben. Nach der Schlüsseldiversifikation wird diese temporäre Datei für die DF auf der UC wichtig.

Diese diversifizierte Schlüsselmenge wird im SM erhalten und ist gültig, bis die nächste Diversifikation unter Verwendung derselben Masterschlüsselmenge stattfindet.

ANMERKUNG: Um den Schutz vor Mißbrauch von diversifizierten Schlüsseln zu erhöhen, kann eine Ablaufkontrolle verwendet werden.

Alle geheimen Schlüssel, die ebenso wie Masterschlüssel diversifiziert werden, dürfen niemals vom SM ausgelesen werden.

Vorbedingungen: Bevor die Funktion DIVERSIFY KEYSSET ausgeführt wird, muß die entsprechende Schlüsselmenge durch Verwendung der Funktion SELECT KEYSSET ausgewählt werden.

Eingabe: a/ Command Header;
b/ Diversifikationsdaten;
c/ ID-Algorithmus.

Tabelle 3: Diversifikationsdaten

Bytes	Beschreibung	Länge
1 – X	Diversifikationsdaten (anwendungsabhängig)	1 bis 16 Bytes

Ausgabe: a/ Daten: keine;
b/ Status.

8.1.3 ASK PARAMETER

Der Zweck dieser Funktion ist die Übertragung eines Parameters vom SM zum Endgerät.

Dieser Parameter wird an das Endgerät übergeben und innerhalb des SM verwendet, um das nächste eingehende Kryptogramm zu berechnen.

Dieser Parameter muß gültig bleiben, bis die nächste Funktion im SM ausgeführt wird, die einen Challenge anfordert, außer bei VERIFY MAC.

Arten von Parametern:

- 1) Challenge (Zufallszahl);
- 2) Challenge (Zähler).

Es kann mehrere Zähler für die Bereitstellung von Challenges, verknüpft in verschiedenen Schlüsselmenge, geben. Im Falle mehrerer Zähler ist zur Bereitstellung der Challenge der an die vorher gewählte Schlüsselmenge gebundene Zähler zu verwenden, anderenfalls ein gemeinsamer SM-Zähler.

ANMERKUNG 1: Falls das SM eine ICC ist, wird vorgeschlagen, die Zählerstruktur nicht anzugeben, um eine gewisse Flexibilität in der Funktion des Systems zu ermöglichen.

ANMERKUNG 2: Für einige Anwendungen darf ein Zähler, z. B. eine Transaktionsnummer, anstelle einer Zufallszahl verwendet werden.

Ist das SM keine IC-Karte, entspricht die Funktion der in A.5.3.1 beschriebenen Funktion.

Eingabe: a/ Command Header;
b/ Parametertyp;
c/ Länge.

Ausgabe: a/ Parameter:

Tabelle 4: Parameter

Bytes	Beschreibung	Länge
1 – X	Challenge	X Bytes

b/ Status.

8.2 Funktionen zur Berechnung eines Kryptogramms oder der Codes für die Nachrichtenauthentikation (MAC)

Wenn TESA 7 verwendet wird, wird ein Kryptogramm entsprechend dem Tesa 7-Mode "Authentikation" (siehe A.3.1 und A.3.2 von EN 726-2 : 1995) berechnet; die Nachrichtenauthentikation (MAC) wird nach dem Tesa 7-Mode "MAC" (siehe A.2.3 und A.2.4 von EN 726-2 : 1995) berechnet.

ANMERKUNG: In anderen Teilen dieser Norm darf das Ergebnis aus der MAC-Berechnung auch als "Kryptogramm" bezeichnet werden.

8.2.1 COMPUTE LOAD KEY

Der Zweck dieser Funktion ist die Bereitstellung eines verschlüsselten Schlüssels und des dazugehörigen Kryptogramms für die UC. Das SM muß eine Verschlüsselung des Schlüssels (angezeigt in den Eingabeparametern) der vorhergehend ausgewählten Schlüsselmenge vornehmen. Der Schlüssel, der zur Ausführung der Verschlüsselung verwendet wird, muß im Command Header von COMPUTE LOAD KEY angezeigt werden. Der verschlüsselte Schlüssel, die Inhalte des Datenfeldes und das vorher von der UC übergebene Challenge müssen verwendet werden, um ein Kryptogramm bereitzustellen. Die Eingabedaten für diese Funktion enthalten die notwendigen Parameter, die auf der UC zur Überprüfung des Kryptogramms verwendet werden.

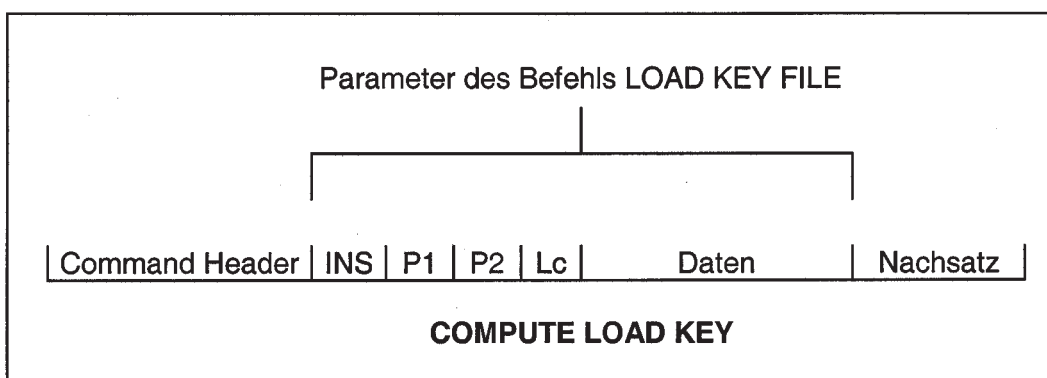


Bild 8: Allgemeine Struktur von COMPUTE LOAD KEY

Vorbedingungen: Das zur Berechnung des Kryptogramms verwendete Challenge muß von der UC durch eine Funktion ASK RANDOM erhalten werden und unter Verwendung eines GIVE RANDOM vom Endgerät zum SM übertragen werden.

Die Schlüsselmenge muß unter Verwendung der Funktion SELECT KEYSET ausgewählt werden. Die entsprechende Schlüsseldatei muß diejenige sein, die die Schlüssel nach der Diversifikation enthält.

Eingabe: a/ Command Header/Nachsatz (COMPUTE LOAD KEY);
b/ Daten (Parameter des folgenden UC-Befehls):

Tabelle 5: Daten

Bytes	Beschreibung	Länge
1	INS-Byte des folgenden an die UC gesendeten Befehls LOAD KEY FILE (codiert nach EN 726-3 : 1994)	1 Byte
2	P1 des folgenden an die UC gesendeten Befehls LOAD KEY FILE (codiert nach EN 726-3 : 1994)	1 Byte
3	P2 des folgenden an die UC gesendeten Befehls LOAD KEY FILE (codiert nach EN 726-3 : 1994)	1 Byte
4	L _c des folgenden an die UC gesendeten Befehls LOAD KEY FILE (codiert nach EN 726-3 : 1994)	1 Byte
5	Version der Schlüsseldatei (nur bei Schlüsselnummer 1 vorhanden)	1 Byte
6	Schlüssellänge	1 Byte
7	Identifikator des Algorithmus	1 Byte

c/ Schlüsselnummer (angezeigt im Command Header des Befehls LOAD KEY (P2));
d/ Typ von EF_{KEY} (EF_{KEY_MAN} oder EF_{KEY_OP}), angezeigt im Command Header des Befehls LOAD KEY FILE (P1).

Ausgabe: a/ Antwortdaten:

Tabelle 6: Antwortdaten

Bytes	Beschreibung	Länge
1 bis 16	Verschlüsselter Schlüssel	16 Bytes
17 bis 24	MAC	8 Bytes

b/ Status.

8.2.2 COMPUTE MAC

Für Funktionen auf der UC, die zur Erfüllung der ACs einen MAC benötigen, muß im SM die allgemeine Funktion COMPUTE MAC verwendet werden, um den MAC zu berechnen. Die Eingabedaten für diese Funktion enthalten die auf der UC verwendeten notwendigen Parameter zur Überprüfung des MAC (Command Header und Daten).

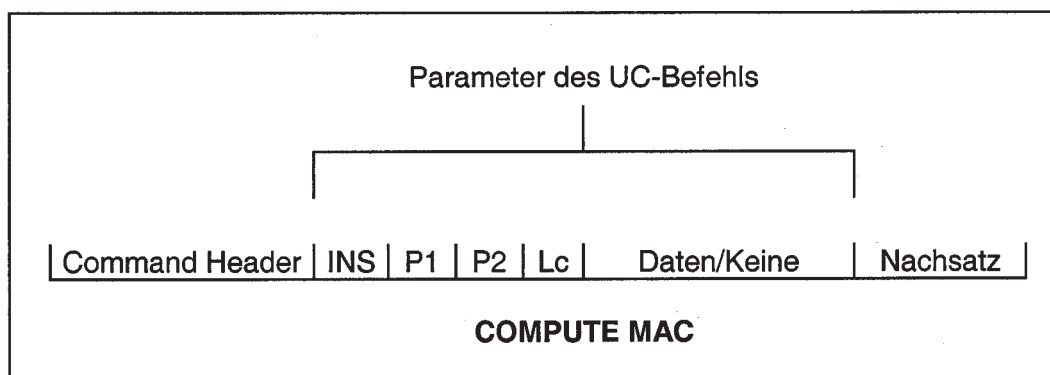


Bild 9: Allgemeine Struktur von COMPUTE MAC

Vorbedingungen: Das zur Berechnung des Kryptogramms verwendete Challenge muß von der UC durch eine Funktion ASK RANDOM erhalten werden und unter Verwendung eines GIVE RANDOM vom Endgerät zum SM übertragen werden.

Die Schlüsselmenge muß unter Verwendung der Funktion SELECT KEYSET ausgewählt werden. Die entsprechende Schlüsseldatei muß diejenige sein, die die Schlüssel nach der Diversifikation enthält.

Eingabe: a/ Command Header/Nachsatz (COMPUTE MAC);
b/ Daten (Parameter des folgenden UC-Befehls):

Tabelle 7: Daten

Bytes	Beschreibung	Länge
1	INS-Byte des folgenden an die UC gesendeten Befehls (codiert nach EN 726-3 : 1994)	1 Byte
2	P1 des folgenden an die UC gesendeten Befehls (codiert nach EN 726-3 : 1994)	1 Byte
3	P2 des folgenden an die UC gesendeten Befehls (codiert nach EN 726-3 : 1994)	1 Byte
4	L_c des folgenden an die UC gesendeten Befehls (codiert nach EN 726-3 : 1994)	1 Byte
5 – (4 + X)	Datenfeld des folgenden an die UC gesendeten Befehls (codiert nach EN 726-3 : 1994)	X Bytes

c/ Schlüsselnummer (angezeigt im Command Header, wenn das SM eine IC-Karte ist).

Ausgabe: a/ MAC (UC-Command Header, Daten):

Tabelle 8: Kryptogramm

Bytes	Beschreibung	Länge
1 – X	MAC	X Bytes

b/ Status.

ANMERKUNG: Die Länge X ist von der kryptographischen Algorithmus-Anwendung abhängig.
Bei TESA 7 : X = 8

Für folgende Funktionen auf der UC ist die Funktion COMPUTE MAC anwendbar, wenn AC = PRO ist:

CREATE FILE
DELETE FILE
EXTEND
EXECUTE
UPDATE BINARY
UPDATE RECORD
CREATE RECORD
INVALIDATE
REHABILITATE
WRITE BINARY
WRITE RECORD
DECREASE
CREATE RECORD

Der Zweck dieser Funktionen ist der Nachweis, daß das SM in eine gegebene Transaktion einbezogen worden ist und daß die Funktion, die auszuführen war, vollendet worden ist.

8.2.3 COMPUTE CRYPTOGRAM

Diese Funktion muß zur Berechnung des in der Nutzerkarte im Befehl EXTERNAL AUTHENTICATION verwendeten Kryptogramms eingesetzt werden.

Vorbedingungen: Das zur Berechnung des Kryptogramms verwendete Challenge muß von der UC durch eine Funktion ASK RANDOM erhalten werden und unter Verwendung eines GIVE RANDOM vom Endgerät zum SM übertragen werden.

Die Schlüsselmenge muß unter Verwendung der Funktion SELECT KEYSET ausgewählt werden. Die entsprechende Schlüsseldatei muß diejenige sein, die die Schlüssel nach der Diversifikation enthält.

Eingabe: a/ Command Header/Nachsatz (COMPUTE CRYPTOGRAM);
b/ Schlüsselnummer (angezeigt im Command Header, wenn das SM eine IC-Karte ist).

Ausgabe: a/ Kryptogramm;

Tabelle 9: Kryptogramm

Bytes	Beschreibung	Länge
1 – X	MAC	X Bytes

b/ Status.

8.3 Funktionen zur Überprüfung von Kryptogrammen oder der Codes für die Nachrichtenauthentikation (MAC)

Wenn Tesa 7 verwendet wird, wird ein Kryptogramm entsprechend dem Tesa 7-Mode "Authentikation" (siehe A.3.1 und A.3.2 von EN 726-2 : 1995) berechnet; die Nachrichtenauthentikation (MAC) wird nach dem Tesa 7-Mode "MAC", wie in A.2.3 und A.2.4 von EN 726-2 : 1995 beschrieben, berechnet. In anderen Teilen dieser Norm kann das Ergebnis aus der MAC-Berechnung auch als "Kryptogramm" bezeichnet werden.

8.3.1 VERIFY MAC

Der Zweck dieser Funktion ist die Überprüfung eines MAC, der auf der UC ausgeführt wird. Das SM muß prüfen, ob der angegebene Schlüssel diese Funktion ausführen darf.

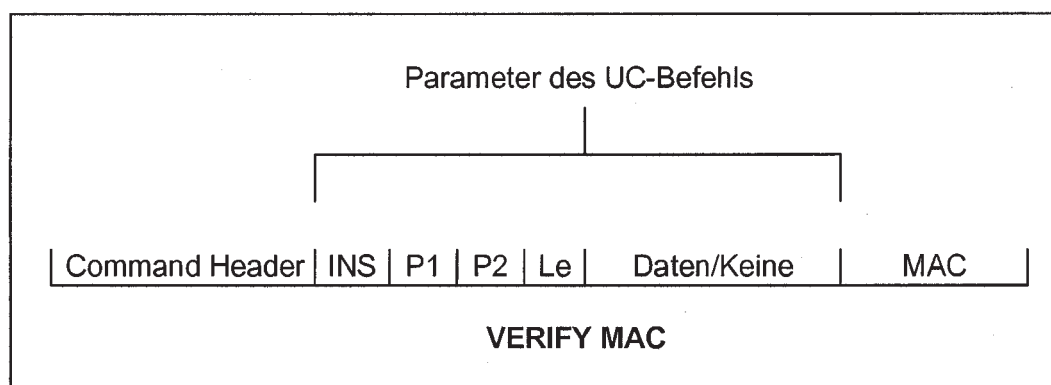


Bild 10: Struktur von VERIFY MAC

Vorbedingungen: Das verwendete Challenge muß vom SM unter Verwendung einer Funktion ASK PARAMETER erhalten werden und unter Verwendung eines GIVE RANDOM zur UC übertragen werden.

Die Schlüsselmenge muß unter Verwendung der Funktion SELECT KEYSET ausgewählt werden. Die entsprechende Schlüsseldatei muß diejenige sein, die die Schlüssel nach der Diversifikation enthält.

Eingabe: a/ Command Header/Nachsatz (VERIFY MAC);
b/ Schlüsselnummer (im Command Header angezeigt);
c/ Daten (Parameter des/der vorhergehenden UC-Befehls/Antwort).

Tabelle 10: Daten

Bytes	Beschreibung	Länge
1	INS-Byte des vorhergehenden an die UC gesendeten Befehls (codiert nach EN 726-3 : 1994)	1 Byte
2	P1 des vorhergehenden an die UC gesendeten Befehls (codiert nach EN 726-3 : 1994)	1 Byte
3	P2 des vorhergehenden an die UC gesendeten Befehls (codiert nach EN 726-3 : 1994)	1 Byte
4	L _e des vorhergehenden an die UC gesendeten Befehls (codiert nach EN 726-3 : 1994)	1 Byte
5 – (4 + X)	Datenfeld der vorhergehenden von der UC gesendeten Antwort (codiert nach EN 726-3 : 1994)	X Bytes

Ausgabe: a/ Daten: keine;
b/ Status.

Für folgende Funktionen auf der UC, die MACs bereitstellen, ist die Funktion VERIFY MAC anwendbar:

READ BINARY STAMPED
READ RECORD STAMPED

Das Kryptogramm muß mit EN 726-3 : 1994 übereinstimmen. Der im Command Header angezeigte Schlüssel der Funktion VERIFY MAC muß derselbe sein wie derjenige, der zur Berechnung des MAC auf der UC verwendet wird.

8.3.2 UPDATE (SM)

Der Zweck dieser Funktion ist die Aktualisierung von Informationen im SM. Die Information darf nur nach der Verifizierung eines in der UC berechneten MAC mit einem READ RECORD STAMPED aktualisiert werden. Das SM muß prüfen, ob der angegebene Schlüssel diese Funktion ausführen darf.

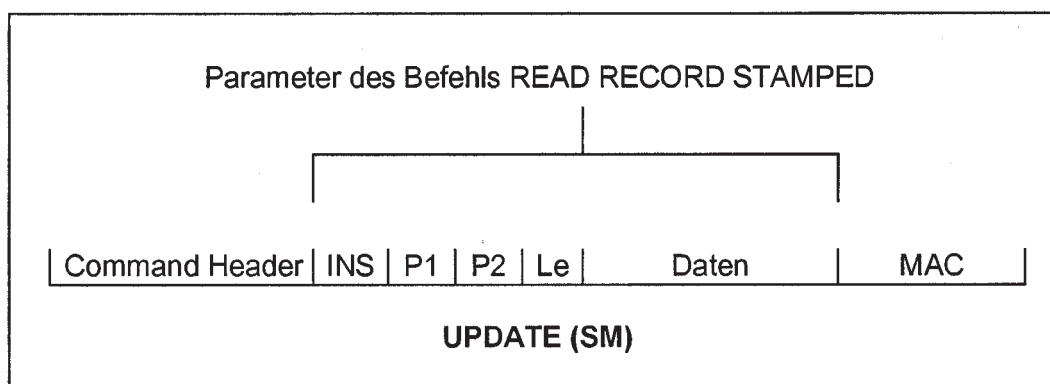


Bild 11: Struktur von UPDATE (SM)

Vorbedingungen: Das verwendete Challenge muß vom SM unter Verwendung einer Funktion ASK PARAMETER erhalten werden und unter Verwendung eines GIVE RANDOM zur UC übertragen werden.

Die Schlüsselmenge muß unter Verwendung der Funktion SELECT KEYSET ausgewählt werden. Die entsprechende Schlüsseldatei muß diejenige sein, die die Schlüssel nach der Diversifikation enthält.

Die im SM zu aktualisierende Datei muß ausgewählt werden.

Eingabe: a/ Command Header/Nachsatz (UPDATE (SM));
b/ Schlüsselnummer (im Command Header enthalten);
c/ Daten (Parameter des/der vorhergehenden Befehls/Antwort von READ RECORD STAMPED (UC)).