

DIN EN 726-7:2000-01 (D)

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

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 Übertragungsprotolle	6
6 Logisches Modell für ein SIV	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 IVIAC.....	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 VERIFYMAC	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