Normen und Industriestandards aus dem „Handbuch der Chipkarten“

Version: September 2003

Dieses Verzeichnis der Normen und Industriestandards stammt aus dem „Handbuch der Chipkarten“ von Wolfgang Rankl und Wolfgang Effing, das 2002 in der 4. Auflage im Carl Hanser Verlag München Wien erschienen ist.

Verbesserungs- und Ergänzungsvorschläge sind jederzeit herzlich willkommen. Diese können an die e-mail-Adresse Rankl@gmx.de mit dem Stichwort „Normenverzeichnis“ gesendet werden. Sie werden dann in der jeweils nächsten Version dieses Dokuments berücksichtigt. In unregelmäßigen Abständen werden sowohl auf der Web-Site des Carl Hanser Verlages (www.hanser.de) als auch auf der Homepage von Wolfgang Rankl (www.wrankl.de) neue Versionen dieses Dokuments veröffentlicht.

Handbuch der Chipkarten
Wolfgang Rankl und Wolfgang Effing
4. Auflage 2002. Hanser
ISBN 3-446-22036-4

Smart Card Handbook
Wolfgang Rankl and Wolfgang Effing
3rd ed. 2003. John Wiley & Sons
ISBN 0-471-85668-8

16.5 Kommentiertes Normen- und Spezifikationsverzeichnis

Der folgende Abschnitt enthält ein ausführlich kommentiertes Verzeichnis der für Karten mit und ohne Chip relevanten Normen und Industriestandards. Das Verzeichnis nimmt vor allem Rücksicht auf internationale und nicht so sehr auf lokale, länderspezifische Normen. Es sind sowohl Normen von offiziellen Normungsorganisationen (z. B.: ANSI, CEN, ETSI, ISO) als auch kartenrelevante Quasi-Normen wie beispielsweise der EMV-Standard oder Internet-RFCs aufgeführt.

Zusätzlich zum kommentierten Verzeichnis zeigt die Tabelle 16.1 eine Übersicht von unter Umständen hilfreichen Aufstellungen, Überblicke und Quellen für themenspezifische Normen und Standards. Vor allem die Industriestandards sind oft kostenlos via WWW erhältlich, was bei Normen, die von Normungsinstituten herausgegeben werden, in der Regel leider nicht der Fall ist.

Die für Chipkarten wichtigsten Normen und Standards sind mit dem Symbol „☒“ gekennzeichnet. Alle Normen und Standards sind nach der herausgebenden Institution und ihrer Nummer, ohne Berücksichtigung von Präfixen (z. B.: „pr“) oder Zustandsbezeichnungen (z. B.: „DIS“) geordnet. Das aufgeführte Datum ist das Erscheinungsdatum der aktuell gültigen Ausgabe.

Tabelle 16.1 Aufstellung der wichtigsten Web-Server für den Download von Normen und Informationen über Chipkarten-relevante Normen

Normungs-/ Standardisierungsinstanz	**Web-Server**	**Bemerkung**
ANSI	[ANSI]	---
CEN	[CEN]	---
DIN	[DIN]	---
EMV	[EMVCO]	Die Standards sind kostenlos vom Web-Server downloadbar.
ETSI	[ETSI]	Alle ETSI-Normen (u.a. für GSM und UMTS) sind kostenlos vom Web-Server downloadbar.
FIPS	[NIST]	Alle FIPS-Normen sind kostenlos vom Web-Server downloadbar.
Global Platform	[Global Platform]	Die Standards sind kostenlos vom Web-Server downloadbar.
IEEE	[IEEE]	---
ISO/IEC	[ISO]	---
ITU	[ITU]	---
Java Card Forum		Die Standards sind kostenlos vom Web-Server downloadbar.
RFC	[RFC]	Die Standards sind kostenlos vom Web-Server downloadbar.
RSA Inc.	[RSA]	Die Standards sind kostenlos vom Web-Server downloadbar.
SEIS	[SEIS]	Die Standards sind kostenlos vom Web-Server downloadbar.

Im Folgenden noch einige kurze Anmerkungen zur Bezeichnung der jeweiligen Normen: Ergänzungen zu ISO- und ISO/IEC-Normen befinden sich in der Regel in einem Anhang (*Amendment, Amd.*). Bei der nächsten Revision dieser Norm, die üblicherweise alle fünf Jahre stattfindet, wird dann der Anhang bei Bedarf in die jeweilige Norm aufgenommen. Die revidierte Fassung der Norm unterscheidet sich von der vorherigen Norm dann nur durch eine neue Jahreszahl und eine laufende Nummer zur Auflage. Neue Versionen von CEN-Normen werden in analoger Art wie ISO-Normen bezeichnet. Bei FIPS-Normen ist die Nummer der revidierten Auflage Norm ein Bestandteil der Normungsbezeichnung (z. B. FIPS 140-2). Telekommunikationsnormen von ETSI benutzen eine dreistellige Versionsnummer als das ausschlaggebende Unterscheidungskriterium. Bei Industrie-Standards kommen je nach Herausgeber sowohl Jahreszahlen wie auch Versionsnummern als eindeutiges Merkmal für bestimmte Dokumentenstände zum Einsatz.

ANSI X9.8	Banking – Personal Identification Number Management and Security
– 1 : 1995	Part 1: PIN Protection Principles and Techniques
– 2 : 1995	Part 2: Approved Algorithms for PIN Encipherment
ANSI X9.9 : 1986	Financial Institution Message Authentication
ANSI X9.17 : 1985	Financial Institution Key Management
ANSI X9.19 : 1996	Financial Institution Retail Message Authentication
ANSI X9.30	Public Key cryptography using irreversible algorithms for the financial services industry
– 1 : 1997	Part 1: The Digital Signature Algorithm (DSA)
– 2 : 1997	Part 2: The Secure Hash Algorithm (SHA-1)
ANSI X9.31 : 1998	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry
ANSI X9.55 : 1997	Public Key Cryptography for the Financial Services Industry: Extensions to Public Key Certificates and Certificate Revocation Lists
ANSI X9.84 : 2001	Biometric Information Management and Security *Diese sehr umfangreiche Norm legt für die unterschiedlichsten biometrischen Identifizierungsverfahren die grundlegenden Architekturprinzipen, die Verwendung, Verwaltung und Sicherheitsanforderungen für biometrische Daten fest.*
ANSI X3.92 : 1981	Data Encryption Algorithm *Diese Norm beschreibt den DES-Algorithmus*.
ANSI X3.106 : 1983	American National Standard for Information Systems – Data Encryption Algorithm – Modes of Operation
ANSI / IEEE 829 : 1991	Standard for Software Test Documentation *Beschreibung der Vorgehensweise und notwendigen Dokumentation beim Test von Software*.
ANSI / IEEE 1008 : 1987	Standard for Software Unit Testing *Beschreibung der grundlegenden Vorgehensweisen beim Test von Software.*
ANSI / IEEE 1012 : 1992	Software Verification and Validation Plans *Festlegung der notwendigen Testaktivitäten und Testpläne für Softwareentwicklungen. Die Grundlage für diese Norm ist das Wasserfallmodell der Softwareproduktion.*

CCITT Z.100 : 1993	CCITT Specification and Description Language (SDL)
CEPS, Version 2.1.3 : 2001	Joint Specification for Common Electronic Purse Cards *CEPS ist eine wichtige Norm für elektronische Geldbörsen, welche in Zukunft die Grundlage der meisten Börsensysteme in Europa sein wird bzw. schon ist und sich an EN 1546 orientiert.*
Common Criteria, Version 2.1 : 1999	identisch mit ISO/IEC 15 408, siehe dort
DIN 9781-10 : 1985	Büro- und Datentechnik; Identifikationskarten aus Kunststoff oder kunststofflaminiertem Werkstoff; Anforderungen an Echtheitsmerkmale *Diese sehr kurze Norm definiert die Begriffe im Umfeld von Echtheitsmerkmalen und zeigt generelle Anforderungen an Echtheitsmerkmale auf.*
DIN 44 300 – 1 …9 : 1988	Informationsverarbeitung – Begriffe *Definition vieler Begriffe aus der Informationstechnik.*
EMV 2000	Integrated Circuit Card Specification for Payment Systems ☒ *Dies ist die wichtigste Normenreihe für Chipkarten im Zahlungsverkehr und wird gemeinsam von EMVCo [EMV] veröffentlicht. Die Reihe besteht aus vier Teilen, Bücher genannt, die die Chipkarte und die dazugehörige Debit- oder Kredit-Zahlungsverkehrsanwendung sowie das dazugehörige Terminal festlegen.*[1]
Book 1 Version 4.0 : 2000	Application Independent ICC to Terminal Interface Requirements *Dieser Teil enthält die Spezifikation der mechanischen und elektrischen Eigenschaften von Chipkarten und Terminals. Definition der An- und Abschaltsequenz, der Datenübertragung auf elektrischer Ebene, des ATRs sowie der dazugehörigen Datenelemente. Außerdem sind die beiden Übertragungsprotokolle T = 0 und T = 1 sowie APDU-Aufbau, logische Kanäle, einige wenige grundlegende Kartenkommandos und Mechanismen zur Anwendungsselektion spezifiziert.*
Book 2 Version 4.0 : 2000	Security and Key Management *In diesem Teil sind statische und dynamische Datenauthentisierung, PIN-Verschlüsselung und Secure Messaging beschrieben. Er enthält auch generelle Rahmenbedingungen für das Schlüsselmanagement der Public Keys eines Zahlungsverkehrssystems und Anforderungen für die Terminalsicherheit inklusive dazugehörigem Schlüsselmanagement.*
Book 3 Version 4.0 : 2000	Application Specification *Dieser Teil der EMV-Spezifikation definiert eine Reihe von notwendigen Kommandos der Chipkarte und Chipkarten-Anwendung für Debit- und Kreditkarten. Des Weiteren Vorgaben für die Transaktionsabläufe. Im Anhang befindet sich unter anderem eine Beschreibung inklusive Codierung aller Datenelemente, Vorgaben zur TLV-Codierung von Daten und generelle Ansätze zur Integration von EMV-Chipkarten in SET-basierte Zahlungsverkehrssysteme.*
Book 4 Version 4.0 : 2000	Cardholder, Attendant and Acquirer Interface Requirements *In Book 4 sind die obligatorischen und optionalen Anforderungen für ein Terminal, das Chipkarten nach EMV unterstützt, aufgeführt. Dazu gehören denkbare Konfigurationen, funktionale und sicherheitstechnische Anforderungen an das Terminal, mögliche und erlaubte Benutzermeldungen inklusive verwendetem Zeichensatz sowie die Schnittstelle zum Acquirer. Dieser Standard definiert in den Grundzügen auch die Architektur der Terminalsoftware sowie das Modell eines Interpreters im Terminal für ausführbaren Programmcode. Im Anhang befindet sich eine Aufstellung*

[1] Siehe auch Abschnitt 12.4 „EMV-Anwendung“.

	von Terminal-relevanten Datenelementen und Hinweise zur technischen Gestaltung der Terminals sowie Beispiele für Terminals am Point-of-Sale, an Geldausgabe- und Warenausgabeautomaten.
EN 726	Identification card systems – Telecommunications integrated circuit(s) card and terminals *Diese Normenreihe war bis Mitte der 90er Jahre führend hinsichtlich der Beschreibung der Funktionalität von Chipkarten-Betriebssystemen. Sie wurde aber mittlerweile vollständig von der ISO/IEC 7816-Normenreihe, den UICC-Normen und EMV-Standards substituiert, so dass sie keine Bedeutung mehr hat.*
– 1 : 1994	Part 1: System overview
– 2 : 1995	Part 2: Security framework
– 3 : 1994	Part 3: Application independent card requirements ☒ *Definition von Dateistrukturen, Kommandos, Returncodes, Dateien für allgemein verwendbare Funktionen und der grundlegenden Mechanismen von Chipkarten für Anwendungen im Bereich der Telekommunikation. Diese Norm ist das ETSI-Gegenstück zur ISO/IEC 7816-4 und der korrespondierende Rahmen zur GSM 11.11.*
– 4 : 1994	Part 4: Application independent card related terminal requirements
– 5 : 1999	Part 5: Payment methods *Definition von verschiedenen Zahlungsmethoden mit dazugehörigen Dateistrukturen, Datenelementen und Abläufen für Chipkarten. Die Zahlungsmethoden sind für Anwendungen im Bereich der Telekommunikation konzipiert.*
– 6 : 1995	Part 6: Telecommunication features
– 7 : 1999	Part 7: Security Module
EN 753	Identification card systems – Intersector thin flexible cards
– 1 : 1997	Part 1: General technical specifications
– 2 : 1997	Part 2: Magnetic recording technique
– 3 : 1999	Part 3: Test methods
EN 1038 : 1995	Identification card systems – Telecommunication applications – Integrated circuit(s) card payphone *Definition der Grundlagen für die Anwendung von Chipkarten an öffentlichen Kartentelefonen. Die Norm enthält vor allem Verweise auf bestehende Normen und legt die sinnvollen Varianten fest, an welcher Stelle im System sich das Sicherheitsmodul zur Authentisierung der Telefonkarte befinden soll.*
prEN 1105 : 1995	Identification card systems – General concepts applying to systems using IC cards in inter-sector environments – Rules for inter-application consistency *Definition von grundlegenden Forderungen an eine Chipkarte, um einen anwendungsübergreifenden Einsatz sicherzustellen. Enthält vor allem Verweise auf bestehende Normen sowie diverse Festlegungen für Chipkarten und Terminals.*
prEN 1292 : 1995	Additional Test Methods for IC Cards and Interface Devices *Definition von Tests für die elektrischen Rahmenwerte und die grundlegende Datenübertragung von Chipkarte und Terminal. Diese Norm ist eine Ergänzung zur ISO/IEC 10 373.*

EN 1332	Identification card systems – Man-Machine Interface
– 1 : 1999	Part 1: Design principles and symbols for the user interface
– 2 : 1998	Part 2: Definition of a Tactile Identifier for ID-1 cards *Festlegung einer fühlbaren Aussparung für ID-1 Karten zur Erkennung der Ausrichtung der Karte.*
– 3 : 1999	Part 3: Key pads
– 4 : 1999	Part 4: Coding of user requirements for people with special needs
EN 1362 : 1997	Identification card systems – Device interface characteristics – Classes of device interfaces
EN 1387 : 1996	Machine readable cards – Health care applications – Cards: General characteristics
EN 1545-1 : 1998	Identification card systems – Surface transport applications – Part 1: General data elements
EN 1545-2 : 1998	Identification card systems – Surface transport applications – Part 2: Transport payment
prEN 1545-3 : 1995	Identification card systems – Surface transport applications – Part 3: Tachograph
prEN 1545-4 : 1995	Identification card systems – Surface transport applications – Part 4: Vehicle and driver licencing
EN 1546	Identification card systems – Inter-sector electronic purse ☒ *Die weltweit wichtigste Norm für elektronische Geldbörsen, welche die Grundlage der meisten Börsensysteme darstellt. Die Normenreihe ist relativ allgemein gehalten, enthält somit viele Optionen, ist aber eine sehr gute und auch vollständige Beschreibung einer elektronischen Geldbörse.*
– 1 : 1999	Part 1: Definition, concepts and structures *Definition der Begriffe für die gesamte Normenreihe und Beschreibung der grundlegenden Konzepte und Strukturen für die branchenübergreifende elektronische Geldbörse.*
– 2 : 1999	Part 2: Security architecture *Beschreibung der verwendeten Notationen für Sicherheitsmechanismen, der Sicherheitsarchitektur und der dazugehörigen Abläufe und Mechanismen bei der branchenübergreifenden elektronischen Geldbörse.*
– 3 : 1999	Part 3: Data elements and interchanges *Beschreibung der Datenelemente, Dateien, Kommandos und Returncodes zwischen allen Komponenten der branchenübergreifenden elektronischen Geldbörse.*
– 4 : 1999	Part 4: Data objects *Beschreibung des TLV-Mechanismus zum Lesen beliebiger Datenelemente aus Dateien sowie detaillierte Darstellung der Komponenten und der Zustände für die Zustandsautomaten der branchenübergreifenden elektronischen Geldbörse. Inklusive eine Liste der Kennzeichen (tags) für alle verwendeten Datenelemente.*
EN 1867 : 1997	Machine-readable cards – Health care applications – Numbering system and registration procedure for issuer identifiers
EN 13 343	Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-3
– 1 prEN : 1998	Part 1: Implementation Conformance Statement (ICS) proforma specification
– 2 prEN : 1998	Part 2: Test Suite Structure and Test Purposes (TSS & TP)
– 3 prEN : 1998	Part 3: Abstract Test Suite (ATS) and Implementation extra Information for Testing (IXIT) proforma specification

EN 13 344	Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-4
– 1 prEN : 1998	Part 1: Implementation Conformance Statement (ICS) proforma specification
– 2 prEN : 1998	Part 2: Test Suite Structure (TSS) and Test Purposes (TP)
– 3 prEN : 1998	Part 3: Abstract Test Suite (ATS) and Implementation extra Information for Testing (IXIT) proforma specification
EN 13 345	Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-7
– 1 prEN : 1998	Part 1: Implementation Conformance Statement (ICS) proforma specification
– 2 prEN : 1998	Part 2: Test Suite Structure and Test Purposes (TSS & TP)
– 3 prEN : 1998	Part 3: Abstract Test Suite (ATS) and Implementation extra Information for Testing (IXIT) proforma specification
EN 1750 : 1999	Identification card systems – Inter-sector messages between devices and hosts – Acceptor to acquirer messages
PC/SC V 1.0	*Interoperability Specification for ICCs and Personal Computer Systems*
Dezember 1997	*Diese umfangreiche und detaillierte Spezifikation ist die Grundlage der Anbindung von Chipkarten und Terminals an das Ressourcenmanagement der 16-Bit- und 32-Bit-Betriebssysteme von Microsoft.*
– 1	Part 1: Introduction and Architecture Overview
– 2	Part 2: Interface Requirements for Compatible IC Cards and Readers
– 3	Part 3: Requirements for PC-Connected Interface Devices
– 4	Part 4: IFD Design Considerations and Reference Design Information
– 5	Part 5: ICC Resource Manager Definition
– 6	Part 6: ICC Service Provider Interface Definition
– 7	Part 7: Application Domain and Developer Design Considerations
– 8	Part 8: Recommendations for ICC Security and Privacy Devices
prEN 13 344 : 1998	Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-4
– 1	Part 1: Implementation Conformance Statement (ICS) proforma specification
– 2	Part 2: Test Suite Structure (TSS) and Test Purposes (TP)
– 3	Part 3: Abstract Test Suite (ATS) and Implementation extra Information for Testing (IXIT) proforma specification
prEN 13 345-1 : 1998	Identification card systems – Telecommunications IC cards and terminals – Test methods and conformance testing for EN 726-7
– 1	Part 1: Implementation Conformance Statement (ICS) proforma specification
– 2	Part 2: Test Suite Structure and Test Purposes (TSS & TP)
– 3	Part 3: Abstract Test Suite (ATS) and Implementation extra Information for Testing (IXIT) proforma specification
ENV 13 729 : 2000	Health informatics – Secure user identification – Strong authentication using microprocessor cards

ENV 1257	Identification card systems – Rules for Personal Identification Number handling in intersector enviroments *Darstellung und Erläuterung der Sicherheitsaspekte im Umgang mit der PIN, von der Übergabe der PIN zum Kartenbesitzer (PIN-Brief) bis hin zur Eingabe der PIN an einer Tastatur (PIN-Pad).*
– 1 prENV : 1997	Part 1: PIN presentation
– 2 prENV: 1997	Part 2: PIN protection
– 3 prENV : 1997	Part 3: PIN verification
ETS 300 331 : 1995	Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM) *Beschreibung der Chipkarte (DAM) für das DECT-System. Sie umfasst alle dazugehörigen Kommandos, Dateien, Zugriffsbedingungen und Authentisierungsabläufe. Die Abmessungen der Kartenformate Mini ID-Karte und Plug-In-Karte sind ebenfalls definiert. Diese Norm lehnt sich stark an die GSM 11.11 Norm an.*
EN 300 812, Version 2.1.1 : 2001	Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIMME) interface
FIPS 46-3 : 1999	Data Encryption Standard (DES) ☒ *Diese Norm beschreibt den DES- und Triple-DES-Algorithmus.*
FIPS 74 : 1981	Guidelines for Implementing and Using the NBS Encryption Standard
FIPS 81 : 1980	DES Modes of Operation
FIPS 140-2 : 2001	Security Requirements for Cryptographic Modules ☒ *Diese Norm ist eine weltweit eingesetzte Grundlagennorm bezüglich der Sicherheitsanforderungen von Sicherheitsmodulen, zu denen auch Chipkarten gezählt werden können. Sie definiert vier unterschiedliche hohe Sicherheitsniveaus für Sicherheitsmodule und beschreibt detailliert sieben sicherheitsrelevante Anforderungsbereiche. Der Inhalt dieser Norm ist sehr praxisbezogen und geht auch auf technische Realisierungsdetails wie beispielsweise Kriterien für die Qualität von Zufallszahlengeneratoren ein.*
FIPS 180-1 : 1995	Secure Hash Standard (SHA) ☒ *Diese Norm beschreibt die SHA-1 Hash-Funktion.*
FIPS 186-2 : 2000	Digital Signature Standard (DSS) ☒ *Diese Norm beschreibt den DSS-Algorithmus.*
FIPS 197 : 2001	Advanced Encryption Standard (AES) ☒ *Diese Norm beschreibt den AES-Algorithmus.*
GSM 01.02, Version 6.0.1 : 2001	Digital cellular telecommunications system (Phase 2+) (GSM); General description of a GSM Public Land Mobile Network (PLMN) *Dies ist die Grundlage der Architektur aller GSM-Mobilfunknetzwerke.*
GSM 01.04, Version 8.0.0 : 1999	Digital cellular telecommunications systems (Phase 2) (GSM); Abbreviations and acronyms
GSM 01.60, Version 6.0.0 : 1998	Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS) Requirements specification of GPRS
GSM 02.09, Version 7.0.1 : 1998	Digital cellular telecommunications systems (Phase 2) (GSM); Security Aspects

GSM 02.17, Version 8.0.0 : 1999

Digital cellular telecommunications systems (Phase 2) (GSM); SIM Functional Characteristics
Kurze Norm mit den Festlegungen der grundsätzlich notwendigen Funktionalitäten eines Sicherheitsmoduls, d. h. einer SIM, für ein GSM-Mobilfunknetzwerk. Diese Norm ist das GSM-Äquivalent zur UMTS-Norm TS 21.111.

GSM 02.19, Version 7.1.0 : 1998

Digital cellular telecommunications system (Phase 2+) (GSM); Subscriber Identity Module Application Programming Interface (SIM API); Service description; Stage 1
Kurze Norm mit der Aufstellung aller grundlegenden Dienste eines sprachunabhängigen API für ausführbaren Programmcode (z.B. Java) in der SIM. Aufbauend auf dieser Norm spezifiziert die GSM 03.19 eine detaillierte Umsetzung für die Realisierung eines Java Card APIs für SIMs.

GSM 02.22, Version 7.0.0 : 1999

Digital cellular telecommunications system (Phase 2+) (GSM);); Personalisation of GSM Mobile Equipment (ME); Mobile functionality specification
Beschreibung der Mechanismen für Personalisierung und Depersonalisierung des Mobile Equipments über spezifische Daten der SIM. Dies wird im Allgemeinen als SIM-Lock bezeichnet.

GSM 02.34, Version 6.0.0 : 1997

Digital cellular telecommunications system (Phase 2+); High Speed Circuit Switched Data (HSCSD); Stage 1

GSM 02.48, Version 8.0.0 : 2000

Digital cellular telecommunications system (Phase 2+) (GSM); Security mechanisms for the SIM application toolkit; Stage 1
Kurze Norm mit der Beschreibung der grundlegenden anwendungsunabhängigen Sicherheitsmechanismen in Verbindung mit dem SIM Application Toolkit nach GSM 11.14. Aufbauend auf dieser Norm spezifiziert die GSM 03.48 eine detaillierte Umsetzung für die Realisierung.

GSM 02.60, Version 6.3.0 : 1997

Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 1

GSM 03.19, Version 8.2.0 : 2001

Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card; Stage 2
☒ *Spezifikation einer Java-Card-Variante für den Einsatz als SIM mit SIM Application Toolkit auf der Basis der Java Card 2.1-Spezifikationen. Diese Norm ist das zentrale Dokument für den Einsatz von Java Card bei GSM. Die Grundlage dazu bildet die GSM 02.19.*

GSM 03.20, Version 8.1.0 : 1999

Global System for Mobile communication (GSM) (Phase 2+); Security related network functions

GSM 03.38, Version 7.2.0 : 1999

Digital cellular telecommunications system (Phase 2+) (GSM); Alphabets and language-specific information
In dieser Norm ist der an ASCII angelehnte GSM-Zeichensatz festgelegt.

GSM 03.40, Version 7.4.0 : 2000

Digital cellular telecommunications system (Phase 2+) (GSM); Technical realization of the Short Message Service (SMS)

GSM 03.48, Version 8.7.0 : 2001

Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit; Stage 2
☒ *Diese Norm enthält die Spezifikation aller Sicherheitsmechanismen für eine abhör- und manipulationssichere Verbindung zwischen Hintergrundsystem und SIM. Außerdem ist der grundsätzliche Mechanismus eines Remote File Management, auch durch SMS, beschrieben. Die Grundlage dieses Dokuments ist die GSM 02.48*.

GSM 09.91 : 1995 — European digital cellular telecommunications system (Phase 2); Interworking aspects of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface between Phase 1 and Phase 2

GSM 11.10 Version 8.2.0 : 2000

Digital cellular telecommunications system (Phase 2+) (GSM) – Mobile Station (MS) conformance specification
Sehr umfangreiche Testspezifikation für die GSM Mobilstationen.

GSM 11.11 Version 8.5.0 : 2001

Digital cellular telecommunications system (Phase 2+) – Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface
☒ *Spezifikation der physikalischen und logischen Eigenschaften einer SIM, wobei diese durch eine Beschreibung der Schnittstelle zwischen SIM und dem GSM-Mobiltelefon realisiert ist. Die Spezifikation beinhaltet die Definition der Kartengrößen ID-1 und Plug-In, der mechanischen Rahmenparameter für die Karte und die Kontakte. Weiterhin sind in GSM 11.11 die Festlegung aller elektrischen Rahmenwerte sowie Struktur und Dateninhalt von ATR und PPS enthalten, sowie die Festlegung der möglichen Dateistrukturen, Sicherheitsmechanismen, Kommandos und Returncodes. Zusätzlich sind alle für eine SIM notwendigen Datenelemente und Dateien aufgeführt sowie typische Kommandosequenzen. Diese Norm ist das GSM-Äquivalent zu den UMTS-Normen TS 31.101 und TS 31.102.*

GSM 11.12 Version 4.3.1 : 1998

Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module – Mobile Equipment (SIM – ME) interface
Spezifikation für 3 Volt SIMs inklusive einer Kompatibilitätsliste für SIMs, die nach den Vorgängerspezifikationen programmiert wurden. Diese Norm beinhaltet lediglich Unterschiede und Ergänzungen zu GSM 11.11 in Bezug auf 3 Volt SIMs.

GSM 11.13 Version 7.2.0 : 2000

Digital cellular telecommunications system (Phase 2+); Test specification for SIM API for Java card
Festlegung von Testumgebung, Testanwendungen, Testabläufen, Testabdeckung und der einzelnen Testfälle für des SIM API für Java Card nach GSM 03.19. Die beschriebenen Tests zielen ausnahmslos auf die informationstechnischen Aspekte einer Java Card für GSM. Diese Norm zeigt sehr gut und ausführlich, wie Tests für eine Java Card beschrieben, aufgebaut und durchgeführt werden können.

GSM 11.14 Version 8.8.0 : 2001

Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface
Definition und ausführliche Beschreibung des SIM Application Toolkits für SIMs. SAT beschreibt eine Schnittstelle zwischen Mobiltelefon und SIM zur teilweisen Steuerung des Mobiltelefons von Zusatzanwendungen der SIM aus. Die Norm führt proaktive Kommandos für die SIM ein und definiert viele neue Kommandos im Zusammenhang mit der Steuerung des Mobiltelefons, wie beispielsweise Displayausgabe, Tastaturabfrage oder Versenden von Kurznachrichten. Das UMTS-Äquivalent zu dieser Norm ist die TS 31.111.

GSM 11.17, Version 7.0.2 : 1998

Digital cellular telecommunications system (Phase 2+) (GSM); Subscriber Identity Module (SIM) conformance test specification
Festlegung von Testumgebung, Testausrüstung, Testhierarchie und der einzelnen Testfälle für den Test von SIMs. Die beschriebenen Tests zielen ausnahmslos auf die elektrischen und informationstechnischen Aspekte. Dazu sind Tests von der elektrischen Versorgung über Datenübertragung, Dateiverwaltung, Kommandos bis hin zu typischen Abläufen in der GSM-Anwendung im Detail festgelegt. Diese Norm zeigt sehr gut und ausführlich, wie SIM Tests beschrieben, aufgebaut und durchgeführt werden können. Das UMTS-Äquivalent zu dieser Norm ist die TS 31.122.

GSM 11.18 Version 7.0.1 : 1998

Digital cellular telecommunications system (Phase 2 +); Specification of the 1.8 Volt Subscriber Identity Module – Mobile Equipment (SIM – ME) interface

GSM 11.19 Version 7.0.3 : 1998

Digital cellular telecommunications system (Phase 2+) (GSM) – Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile

IEEE 828 : 1990	Standard for Software Configuration Management Plans
IEEE 1363 : 2000	Standard Specifications for Public-Key Cryptography ☒ *Dies ist eine sehr ausführliche und umfassende Norm, welche beinahe alle Aspekte – von der Schlüsselgenerierung bis zur Verwendung bei digitaler Signatur, Schlüsselaustausch und Verschlüsselung bei asymmetrischen Kryptoalgorithmen – abdeckt.*
ISO 639 : 1988	Codes for the representation of names of languages
ISO 639	Codes for the representation of names of
– 1 : 2001	Part 1: Alpha-2 code
– 2 : 1998	Part 2: Alpha-3 code
ISO/IEC 646 : 1991	Information technology – ISO 7-bit coded character set for information interchange
ISO 3166	Codes for the representation of names of countries and their subdivisions
– 1 : 1997	Part 1: Country codes
– 2 : 1998	Part 2: Country subdivision code
– 3 : 1999	Part 3: Code for formerly used names of countries
ISO 4217 : 1995	Codes for the representation of currencies and funds
ISO 4909 : 2000	Bank cards – Magnetic stripe data contents for track 3
ISO/IEC 7501	Identification cards – Machine readable travel documents
– 1 : 1997	Part 1: Machine readable passport

– 2 : 1997	Part 2: Machine readable visa
– 3 : 1997	Part 3: Machine readable offcial travel documents
ISO 7810 : 1995	Identification cards – Physical characteristics *Beschreibung der wichtigsten physikalischen Eigenschaften einer Karte ohne Chip und Definition der Kartengrößen ID-1, ID-2 und ID-3.*
ISO 7811	Identification cards – Recording technique *Diese Normenreihe ist eine wichtige Referenz für die mechanischen Aspekte von Karten und legt für diesen Bereich die wesentlichen Kartenelemente in ihrer Ausführung fest.*
– 1 : 1995	Part 1: Embossing *Exakte Definition der zehn Ziffern sowie der grund-legenden Beschriftungsart für die Hochprägung von Karten.*
– 2 : 2001	Part 2: Magnetic stripe – low coercivity *Definition der Größe und Position des Magnetstreifens einer Karte. Außerdem sind in dieser Norm die physikalischen Eigenschaften des magnetisierbaren Materials und die Codierung der Zeichen auf dem Magnetstreifen festgelegt.*
– 3 : 1995	Part 3: Location of embossed characters on ID-1 cards *Definition von möglichen Positionen der Hochprägung auf ID-1 Karten.*
– 4 : 1995	Part 4: Location of read-only magnetic tracks – Tracks 1 and 2 *Definition der Position der nur lesbaren Spuren 1 und 2 auf einer ID-1 Karte.*
– 5 : 1995	Part 5: Location of read-write magnetic track – Track 3 *Definition der Position der schreib- und lesbaren Spur 3 auf ID-1 Karten.*
– 6 : 2001	Part 6: Magnetic stripe – High coercivity
– 7 WD : 2001	Part 7: Magnetic stripe – High coercivity high density
ISO 7812	Identification cards – Identification of issuers
– 1 : 2000	Part 1: Numbering system *Spezifikation eines Nummerierungsschemas für die Herausgeber von ID-Karten.*
– 2 : 2000	Part 2: Application and registration procedures *Festlegung der Registrierungsinstanz und eines Formulars für die Registrierung von Anwendungen. Enthält außerdem den Algorithmus für die Prüfsumme nach Luhn (Modulo 10 Prüfsumme).*
ISO 7813 : 2001	Identification cards – Financial transaction cards *Definition der grundlegenden physikalischen Eigenschaften, Größe und Hochprägung der ID-1 Karte nach ISO 7810 für Karten im Bereich des Zahlungsverkehrs. Auch sind hier die Dateninhalte von Spur 1 und 2 des Magnetstreifens definiert.*
ISO/IEC 7816	Identification cards – Integrated circuit(s) cards with contacts ☒ *Dies ist die wichtigste ISO-Normenreihe für Mikrocontroller-Chipkarten. Die ersten drei Teile fokussieren vor allem auf die Karten- und Chiphardware. Die nachfolgenden Teile legen alle Mechanismen und Eigenschaften von Anwendungen und Betriebssystemen für Chipkarten sowie der dazugehörigen Informationstechnik fest.*
– 1 : 1998	Part 1: Physical characteristics *Definition der physikalischen Eigenschaften einer Karte mit einem kontaktbehafteten Chip, sowie der dafür anzuwendenden Tests.*

– 2 : 1999	Part 2: Dimensions and location of the contacts *Definition der Größe und Position der Kontaktelemente einer Chipkarte sowie der möglichen Anordnung von Chip, Magnetstreifen und Hochprägung. Auch ist die Messmethode für die Position der Kontakte auf der Chipkarte beschrieben.*
– 3 : 1997	Part 3: Electronic signals and transmission protocols ☒ *Die wichtigste ISO-Norm für die elektrischen Rahmenparameter einer Mikrocontroller-Chipkarte. In dieser Norm sind alle grundlegenden elektrischen Eigenschaften wie Spannungsversorgung (5 Volt und 3 Volt), Anhalten der Taktfrequenz und Resetverhalten (Kalt- und Warmreset) festgelegt. Außerdem sind die Datenelemente, der Aufbau und die möglichen Abläufe von ATR und PTS definiert. Ein großer Teil dieser Norm befasst sich noch mit den Grundlagen der Datenübertragung auf physikalischer Ebene (z. B. Teiler) und die Definition der beiden Übertragungsprotokolle T = 0 und T = 1 mit ausführlichen Beispielen des Kommunikationsablaufs*.
– 4 : 1995	Part 4: Inter-industry commands for interchange ☒ *Die wichtigste ISO-Norm auf Anwendungsebene für Chipkarten. Definition der Dateiorganisation, Dateistrukturen, Sicherheitsarchitektur, TPDUs, APDUs, Secure Messaging, Returncodes und der logischen Kanäle. Den größten Teil nimmt eine ausführliche Beschreibung der Kommandos für Chipkarten ein. Außerdem werden die grundlegenden Mechanismen von Chipkarten für allgemeine Industrieanwendungen beschrieben.*
– 4 Amd. 1 : 1997	Part 4 – Amendment 1: Use of secure Messaging
– 5 : 1994	Part 5: Numbering system and registration procedure for application identifiers *Definition des Nummerierungsschemas für die eindeutige Identifizierung von nationalen und internationalen Anwendungen in Chipkarten. Außerdem werden die exakte Datenstruktur der AIDs definiert und die Registrierungsprozedur für Anwendungen erklärt*.
– 5 Amd. 1 : 1996	Part 5 – Amendment 1: Registration of identifiers
– 6 CD : 2001	Identification cards – Integrated circuit(s) cards with contacts – Part 6: Inter-industry data elements *Definition von Datenelementen (data objects – DO) und dazugehöriger TLV-Kennzeichnung für allgemeine Industrieanwendungen. Die dazugehörigen TLV-Strukturen sind ebenfalls erläutert sowie die Prozeduren für das Auslesen von Datenobjekten aus Chipkarten*.
– 7 : 1999	Part 7: Interindustry commands for Structured Card Query Language (SCQL) *Definition von zusätzlichen Kommandos für Chipkarten in Ergänzung zu ISO/IEC 7816-4. In dieser Norm sind die Prinzipien einer an SQL angelehnten Datenbank für Chipkarten definiert. Ebenso legt sie die Kommandos für die dazugehörigen SCQL-Zugriffe auf Chipkarten fest*.
– 8 : 1999	Part 8: Security related interindustry commands *Dieser Teil der Normenreihe ist zur Gänze dem Thema sicherheitsrelevante Funktionen und Kommandos gewidmet. Die Norm definiert ergänzend zu ISO/IEC 7816-4 zusätzliche Mechanismen für Secure Messaging. Des Weiteren sind umfangreiche Kommandos für krytografische Funktionen, wie beispielsweise digitale Signatur, Hash-Berechnung, MAC-Berechnung, Ver- und Entschlüsselung von Daten beschrieben.*
– 9 : 2000	Part 9: Enhanced interindustry commands *In dieser in drei Teile gegliederten Norm ist am Beginn der Lebenszyklus von Chipkarten-Anwendungen auf Dateiebene in Form von Zuständen*

	beschrieben. Der nächste große Abschnitt beschäftigt sich mit der Beschreibung von Zugriffskontrollobjekten (access control objects – ACO), die für die Reglementierung von Dateizugriffen verwendet werden können. Der dritte umfangreiche Teil der Norm definiert Suchkommandos für Dateiinhalte und die für die Verwaltung von Anwendungen notwendigen Administrationskommandos zum Erzeugen und Löschen von Dateien.
– 10 : 1999	Part 10: Electronic signals answer to reset for synchronous cards *Dieser Teil ist für Speicherkarten das Gegenstück zu Teil 3 dieser Normenreihe. Hier werden die wesentlichen elektrischen Rahmenparameter für Speicherkarten festgelegt. Auch sind die Datenelemente, der Aufbau und die mög-lichen Abläufe des ATR für synchrone Karten definiert.*
– 11 CD : 2000	Part 11: Personal verification through biometric methods *Dieser Normenteil definiert Kommandos zur biometrischen Benutzeridentifizierung sowie dazugehörige Datenelemente. Des Weiteren werden im Anhang überblickshaft der Ablauf für die Aufnahme der biometrischen Daten in die Chipkarte (enrollment) aufgezeigt und ein Szenario für die Überprüfung dieser biometrischen Daten beschrieben.*
– 15 CD : 2001	Part 15: Cryptographic Information Application *Dieser Teil der Normenreihe nutzt den PKCS #15 Standard als Grundlage und definiert darauf aufbauend alle notwendigen Datenelemente für eine interoperable Chipkarte für digitale Signatur. Die Norm enthält eine Beschreibung aller für eine Signaturkarte notwendigen Datenobjekte, Verzeichnisse und Dateien sowie eine ASN.1-Beschreibung aller in den Dateien gespeicherten Zertifikate, Schlüssel und sonstiger Verwaltungsinformationen.*
ISO 8372 : 1987	Information processing – Modes of Operation for a 64-Bit Block Cipher Algorithm ☒ *Definition der vier Modi für Verschlüsselungsalgorithmen mit 64 Bit Blockgröße (z. B.: DES): Electronic Codebook (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB) und Cipher Feedback (CFB). Die in ANSI X 3.106 und FIPS 81 beschriebenen Modi für Blockverschlüsselungsverfahren stellen eine Untermenge dieser Norm dar.*
ISO 8583 : 1993	Financial transaction card originated messages – Interchange message specifications *Norm für die Datenübertragung zwischen Terminal und Host. In einer angelehnten Form funktioniert auch in Deutschland die Kommunikation zwischen Terminals für Debitkarten und dem Hintergrundsystem.*
ISO 8583	Financial transaction card originated messages – Interchange message specifications
– 1 CD : 1998	Part 1: Messages, data elements and code values
– 2 : 1998	Part 2: Application and registration procedures for Institution Identification Codes (IIC)
– 3 : 1988	Part 3: Maintenance procedures for messages, data elements and code values
ISO 8730 : 1990	Banking – Requirements for message authentication *Grundlagen für die Sicherung von Daten bei der Übertragung d. h. Erzeugung und Prüfung von MACs. Im Anhang dazu befinden sich ausführliche Zahlenbeispiele, sowie die Beschreibung eines Pseudozufallszahlengenerators mit dem DES.*
ISO 8731	Banking – Approved algorithms for message authentication
– 1 : 1987	Part 1: DEA

	Sehr kurze Norm, in der der DEA für MAC-Berechnung als geeignet bezeichnet wird. Außerdem wird kurz die Paritätsberechnung für DES-Schlüssel beschrieben.
– 2 : 1992	Part 2: Message authenticator algorithm *Definition eines schnellen Algorithmus für die MAC-Berechnung im Bankenbereich. Im Anhang befinden sich Zahlenbeispiele sowie eine exakte Beschreibung des Algorithmus*.
ISO 8732 : 1988	Banking – Key management *Umfangreiche Norm über die Grundlagen und Verfahren des Schlüsselmanagements zwischen zwei oder mehreren beteiligten Instanzen mit Hilfe von symmetrischen Kryptoalgorithmen*.
ISO/IEC 8824	Information technology – Abstract Syntax Notation One (ASN.1) *Definition der grundlegenden Codierungsregeln von ASN.1*.
– 1 : 1998	Part 1: Specification of basic notation
– 1 : 1998 / Amd 1 : 2000	Part 1 – Amendment 1: Relative object identifiers
– 1 : 1998 / Amd 2 : 2000	Part 1 – Amendment 2: ASN.1 Semantic Model
– 1 : 1998 / Amd 3 : 2000	Part 1 – Amendment 3: XML value notation
– 1 : 1998 / Amd 4 : 2000	Part 1 – Amendment 4: Version number support
– 2 : 1998	Part 2: Information object specification
– 2 : 1998 / Amd 1 : 2000	Part 2 – Amendment 1: ASN.1 semantic model
– 2 : 1998 / Amd 2	Part 2 – Amendment 2: XML value notation
– 3 : 1998	Part 3: Constraint specification
– 4 : 1998	Part 4: Parameterization of ASN.1 specifications
– 4 : 1998 / Amd 1: 2000	Part 4 – Amendment 1: ASN.1 semantic model
ISO/IEC 8825	Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) *Definition der Datenbeschreibungssprache ASN.1*.
– 1:1998	Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
– 1:1998 / Amd 1:2000	Part 1 – Amendment 1: Relative object identifiers
– 2:1998	Part 2: Specification of Packed Encoding Rules (PER)
– 2:1998 / Amd 1:2000	Part 2 – Amendment 1: Relative object identifiers
– 3 FCD : 2001	Part 3: Specification of Encoding Control Notation (ECN)
– 3 : FCD / Amd 1 : 2001	Part 3 – Amendment 1: ASN.1 extensibility notation
– 4 : WD 2000	Part 4: XML Encoding Rules (XER)
ISO/IEC 8859 - 1 : 1998	Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1
ISO/IEC 9075	Information technology – Database languages – SQL *Definition der Datenbankabfragesprache Structured Query Language (SQL), welche eine Obermenge der chipkartenbasierten Datenbankabfragesprache SCQL ist*.
– 1 : 1999	Part 1: Framework (SQL/Framework)
– 1 : 1999 / Amd 1 : 2001	Part 1 – Amendment 1: On-Line Analytical Processing (SQL/OLAP)
– 2 : 1999	Part 2: Foundation (SQL/Foundation)
– 2 : 1999 / Amd 1 : 2001	On-Line Analytical Processing (SQL/OLAP)
– 3 : 1999	Part 3: Call-Level Interface (SQL/CLI)
– 4 : 1999	Part 4: Persistent Stored Modules (SQL/PSM)

– 5 : 1999	Part 5: Host Language Bindings (SQL/Bindings)
– 5 : 1999 / Amd 1 : 2001	On-Line Analytical Processing (SQL/OLAP)
– 9 : 2001	Part 9: Management of External Data (SQL/MED)
– 10 : 2000	Part 10: Object Language Bindings (SQL/OLB)
– 11 : CD 2001	Part 11: Information and definition schemas (SQL/schemata)
– 12 : AWI 2000	Part 12: Replication
– 13 : FCD 2001	Part 13: Java Routines and Types (SQL/JRT)
– 14 : WD 2001	Part 14: XML-Related Specifications (SQL/XML)
ISO/IEC 9126	Software engineering – Product quality
– 1 : 2001	Part 1: Quality model
– 2 : CD 2001	Part 2: External metrics
– 3 : CD 2001	Part 3: Internal metrics
– 4 : CD 2001	Part 4: Quality in use metrics
ISO 9564	Banking – Personal Identification Number management and security
– 1 : 1991	Part 1: PIN protection principles and techniques *Grundlagen der PIN-Auswahl, des PIN-Managements und des Schutzes der PIN für allgemeine Bankanwendungen. In den Anhängen sind unter anderem generelle Forderungen an Eingabegeräte für PINs definiert. Auch sind dort Vorschläge für das Layout der entsprechenden Tastaturen vorhanden. Des Weiteren befinden sich im Anhang Hinweise zum Löschen von sensitiven Daten auf verschiedenen Medien wie Magnetband, Papier oder Halbleiterspeicher.*
– 2 : 1991	Part 2: Approved algorithm(s) for PIN encipherment *Sehr kurze Norm, die den DES als Algorithmus zur PIN-Verschlüsselung definiert.*
– 3 : 2002	Part 3: PIN protection requirements for offline PIN handling in ATM and POS systems
ISO/IEC 9646-3 : 1998	Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 3: The Tree and Tabular Combined Notation (TTCN) *Umfangreiche Norm, welche eine allgemeine Hochsprache für die Festlegung von Tests beschreibt. TTCN wird vereinzelt im Umfeld von Chipkartentests eingesetzt.*
ISO/IEC 9796	Information technology – Security techniques – Digital signature scheme giving message recovery *Definition von Verfahren zur Erstellung und Überprüfung digitaler Signaturen mit Nachrichtenrückgewinnung. Im Anhang befinden sich mehrere Zahlenbeispiele zur Schlüsselerzeugung, Signaturerstellung und Prüfung der Signatur.*
– 1 : 1999	Part 1: Mechanisms using redundancy
– 2 : 1997	Part 2: Mechanisms using a hash-function
– 3 : 2000	Part 3: Discrete logarithm based mechanisms
ISO/IEC 9797	Information technology – Security techniques – Message Authentication Codes (MACs)
– 1 : 1999	Part 1: Mechanisms using a block cipher
– 2 : 1999	Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 9798	Information technology – Security techniques – Entity authentication ☒ *Normenreihe, die im Detail die unterschiedlichen kryptografischen Techniken für die Authentisierung von einer, zwei oder drei beteiligten*

	Instanzen beschreibt. Diese Normenreihe ist die wichtigste Referenz zum Thema Authentisierung.
– 1 : 1997	Part 1: General *Festlegung der Bezeichnungen und Notationen für die weiteren Teile der Normenreihe.*
– 2 : 1999	Part 2: Mechanisms using symmetric encipherment algorithms *Festlegung von Authentisierungsverfahren, die auf symmetrischen Kryptoalgorithmen basieren.*
– 3 : 1998	Part 3: Mechanisms using digital signature techniques *Festlegung von Authentisierungsverfahren, die auf digitalen Signaturen basieren.*
– 4 : 1999	Part 4: Mechanisms using a cryptographic check function *Festlegung von Authentisierungsverfahren, die auf kryptografischen Prüffunktionen basieren.*
– 5 : 1999	Part 5: Mechanisms using zero knowledge techniques *Festlegung von Authentisierungsverfahren, die auf Zero-Knowledge-Verfahren basieren.*
ISO 9807 : 1991	Banking and related financial services – Requirements for message authentication (retail)
ISO/IEC 9979 : 1999	Information technology – Security techniques – Procedures for the registration of cryptographic algorithms
ISO 9992	Financial Transaction Cards – Messages between the Integrated Circuit Card and the Card Accepting Device
– 1 : 1990	Part 1: Concepts and structures
– 2 : 1998	Part 2: Functions, messages (commands and responses), data elements and structures *Definition von Kommandos, Abläufen und Datenelementen für Chipkarten im Zahlungsverkehr. Enthält die Definition der Kennzeichen (tags) für Datenelemente im Zahlungsverkehr und viele Querverweise auf bestehende Normen der ISO/IEC 7816-Reihe.*
– 4 DIS : 1993	Part 4: Common data for interchange
– 5 CD : 1991	Part 5: Organization of data elements
ISO/IEC 10 116 : 1997	Information technology – Security techniques – Modes of operation for an n-bit block cipher algorithm *Beschreibung der vier üblichen Modi (ECB, CBC, CFB, OFD), mit denen ein Blockverschlüsselungsalgorithmus betrieben werden kann. Im Anhang befinden sich detaillierte Anmerkungen zur jeweiligen Anwendung der vier Verschlüsselungsmodi sowie in einem weiteren Anhang die entsprechenden Zahlenbeispiele dazu.*
ISO/IEC 10 118	Information technology – Security techniques – Hash functions *Allgemeine Grundlagen zu Hash-Funktionen, sowie dazugehörige Padding-Methoden.*
– 1 : 2000	Part 1: General
– 2 : 2000	Part 2: Hash functions using an n-bit block cipher algorithm *Definition von Hash-Funktionen, die einen Blockverschlüsselungsalgorithmus als Grundlage benutzen. Es ist ein Algorithmus mit einfacher und einer mit doppelter Schlüssellänge beschrieben. Im Anhang befindet sich jeweils ein dazu passendes Zahlenbeispiel auf der Basis des DES.*
– 3 : 1998	Part 3: Dedicated hash-functions
– 4 : 1998	Part 4: Hash-functions using modular arithmetic
ISO 10 202	Financial Transaction Cards – Security Architecture of Financial Transaction Systems using Integrated Circuit Cards
– 1 : 1991	Part 1: Card life cycle

– 2 : 1996	Part 2: Transaction process
– 3 : 1998	Part 3: Cryptographic key relationship
– 4 : 1996	Part 4: Secure application modules
– 5 : 1998	Part 5: Use of algorithms
– 6 : 1994	Part 6: Card holder verification
– 7 : 1998	Part 7: Key Management *Definition von allgemeinen Mechanismen für Schlüsselmanagement und zur Schlüsselableitung. Es werden sowohl symmetrische als auch asymmetrische Verfahren beschrieben.*
– 8 : 1998	Part 8: General principles and overview
ISO/IEC 10 373	Identification cards – Test methods ☒ *Grundlegende Norm zum Test von Karten. Genaue Beschreibung von Testmethoden für Kartenkörper und Kartenkörper in Verbindung mit dem implantierten Chip. Die einzelnen Tests werden mit vielen erklärenden Zeichnungen detailliert beschrieben.*
– 1 : 1998	Part 1: General characteristics tests
– 2 : 1998	Part 2: Cards with magnetic stripes
– 3 : 2001	Part 3: Integrated circuit(s) cards with contacts and related interface devices *Festlegung von Testumgebung, Testmethoden und Testabläufen für elektrische Tests von kontaktbehafteten Chipkarten. Dazu sind Abläufe für die Prüfung der Kontaktpositionen, der elektrischen Versorgung und der Datenübertragung bei ATR, PTS und den Übertragungsprotokollen im Detail festgelegt.*
– 4 CD : 1998	Part 4: Contactless integrated circuit cards
– 5 : 1998	Part 5: Optical memory cards
– 6 : 2001	Part 6: Proximity cards
– 7 : 2001	Part 7: Vicinity cards
ISO/IEC 10 536	☒ Identification cards – Contactless integrated circuit(s) cards – Close-coupled cards *In dieser Norm werden kontaktlose Chipkarten beschrieben, deren Einsatzgebiet sich auf den direkten Kontakt mit dem Terminal beschränkt.*
– 1 : 2000	Part 1: Physical characteristics *Definition der physikalischen Eigenschaften von kontaktlosen Chipkarten sowie der dazugehörigen Testmethoden.*
– 2 : 1995	Part 2: Dimension and location of coupling areas *Spezifikation der Abmessungen und Lage der Koppelflächen für kontaktlose Karten und den Betrieb in Kartenterminals mit Kartenschlitz oder an der Oberfläche.*
– 3 : 1996	Part 3: Electronic signals and reset procedures *Definition der elektrischen Signale der induktiven und kapazitiven Koppelelemente zwischen Terminal und Chipkarte.*
– 4 CD : 1997	Part 4: Answer to reset and transmission protocols *Festlegungen der Datenübertragung auf physikalischer Ebene, des Aufbaus und der Datenelemente von ATR und PTS für kontaktlose Chipkarten. Definition des Übertragungsprotokolls T = 2 mit vielen Beispielszenarien für den Protokollablauf.*
ISO/IEC 10646	Information technology – Universal Multiple-Octet Coded Character Set (UCS)
– 1 : 2000	Part 1: Architecture and Basic Multilingual Plane
– 2 : 2001	Part 2: Supplementary Planes
ISO 11 568	Banking – Key management

– 1 : 1994	Part 1: Introduction to Key Management
– 2 : 1994	Part 2: Key management techniques for symmetric ciphers
– 3 : 1994	Part 3: Key life cycle for symmetric ciphers
– 4 : 1998	Part 4: Key management techniques for public key cryptosystems
– 5 : 1998	Part 5: Key life for public key cryptosystems
– 6 : 1998	Part 6: Key management schemes
ISO/IEC 11 693 : 2000	Identification cards – Optical memory cards
ISO/IEC 11 694	Identification cards – Optical memory cards and devices – Linear recording method
– 1 : 2000	Part 1: Physical characteristics
– 2 : 2000	Part 2: Dimensions and location of the accessible optical area
– 3 : 2001	Part 3: Optical properties and characteristics
– 4 : 1996	Part 4: Logical data structures
ISO/IEC 11 770	Information technology – Security techniques – Key management
– 1 : 1996	Part 1: Framework
– 2 : 1996	Part 2: Mechanisms using symmetric techniques
– 3 : 1999	Part 3: Mechanisms using asymmetric techniques
ISO/IEC 12 207 : 1995	Information technology – Software life cycle processes
ISO/IEC 13 239 : 2000	Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures
ISO 13 491	Banking – Secure cryptographic devices
– 1 : 1998	Part 1: Concepts, requirements and evaluation methods
– 2 : 2000	Part 2: Security compliance checklists for devices used in magnetic stripe card systems
ISO/IEC 13 888	Information technology – Security techniques – Non-repudiation
– 1 : 1997	Part 1: General
– 2 : 1998	Part 2: Mechanisms using symmetric techniques
– 3 : 1997	Part 3: Mechanisms using asymmetric techniques
ISO/IEC 14 443	☒ Identification cards – Contactless integrated circuit(s) cards – Proximity cards *In dieser Norm werden kontaktlose Chipkarten beschrieben, die bis zu einigen 10 cm Abstand zu Terminals verwendet werden können.*
– 1 : 2000	Part 1: Physical characteristics
– 2 : 2001	Part 2: Radio frequency power and signal interface
– 3 : 2001	Part 3: Initialization and anticollision
– 4 : 2001	Part 4: Transmission protocol
ISO/IEC 14 888	Information technology – Security techniques – Digital signature with appendix *Diese Norm spezifiziert grundlegende Mechanismen und Vorgehensweisen für digitale Signaturen mit Anhang. Die Norm ist unabhängig von einem bestimmten asymmetrischen Kryptoalgorithmus.*
– 1: 1998	Part 1: General
– 2 : 1999	Part 2: Identity-based mechanisms
– 3 : 1998	Part 3: Certificate-based mechanisms
ISO/IEC 15 292 : 2001	Information technology – Security techniques – Protection Profile registration procedures
ISO/IEC 15 408	Information technology – Security techniques – Evaluation criteria for IT security

– 1 : 1999	Part 1: Introduction and general model
– 2 : 1999	Part 2: Security functional requirements
– 3 : 1999	Part 3: Security assurance requirements
ISO/IEC 15 693	Identification cards – Contactless integrated circuit(s) cards – Vicinity cards *In dieser Norm werden kontaktlose Chipkarten beschrieben, die in bis zu einem Meter Abstand zu Terminals verwendet werden können.*
– 1 CD : 2000	Part 1: Physical characteristics
– 2 WD : 2000	Part 2: Air interface and initialization
– 3 WD : 2001	Part 3: Anticollision and transmission protocol
– 4 WD : 1996	Part 4: Extended command set and security features
ISO 15 782	Banking – Certificate management for financial services
– 1 DIS : 2000	Part 1: Public Key Certificates
– 2 : 2001	Part 2: Certificate extensions
ISO/IEC 15 946	Information technology – Security techniques – Cryptographic techniques based on elliptic curves
– 1 FDIS : 2001	Part 1: General
– 2 FDIS : 2001	Part 2: Digital signatures
– 3 FDIS : 2001	Part 3: Key establishment
– 4 CD : 2000	Part 4: Digital signatures giving message recovery
ISO 17 090	Public key infrastructure
– 1 CD : 2001	Part 1: Framework and overview
– 2 CD : 2001	Part 2: Certificate profile
– 3 CD : 2001	Part 3: Policy management of certification authority
ITU X.509 : 2000	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework ☒ *Diese Norm legt Aufbau und Codierung von Zertifikaten fest. Sie stellt weltweit die meistbenutzte Grundlage für Zertifikatsstrukturen dar und ist identisch mit der ISO/IEC 9594-8.*
Java Card 2.1.1 : 2000	☒ *Dieser Industriestandard ist die Grundlage der Java Card; er wird vom Java Card Forum erstellt und von der Firma Sun veröffentlicht. Alle drei Standards ergänzen sich und decken die verschiedenen Implementierungs-Aspekte einer Java Card ab.*
Application Programming Interface	*Dieser Standard spezifiziert die gesamte Schnittstelle, das API, die einem Applet auf einer Java Card zur Verfügung steht. Das Dokument umfasst im Wesentlichen eine umfangreiche Aufstellung aller Klassen und Interfaces des Java Card API.*
Runtime Environment (JCRE) Specification	*Dieser Standard spezifiziert die Java Card Laufzeitumgebung, die im Wesentlichen aus der Virtuellen Maschine und dem Java Card API besteht. Das Dokument beschreibt im Detail die Themen Lebensdauer der Virtuellen Maschine und Lebensdauer von Applets, Selektion von Applets, transiente Objekte, Sharing von Objekten, Transaktionen und Atomität von Transaktionen sowie Installation von Applets.*
Virtual Machine Specification	*Dieser Standard spezifiziert die Virtuelle Maschine der Java Card. Er umfasst den detaillierten Aufbau der Virtuellen Maschine, den Befehlssatz der Virtuellen Maschine und das Format der CAP-Dateien.*

Multifunktionale Karten Terminals MKT Spezifikation, Version 1.0 : 1999

	Die von Teletrust Deutschland herausgegebene MKT Spezifikation ist in Deutschland der Quasi-Standard für die Anbindung von Terminals an PCs.
Teil 1	MKT-Basiskonzept
Part 2	CT-ICC-Interface – MKT-Schnittstelle für kontaktorientierte Chipkarten mit synchroner und asynchroner Übertragung
Part 3	CT-API 1.1 – Anwendungsunabhängiges Card Terminal Applikation Programming Interface
Part 4	CT-BCS – Anwendungsunabhängiges Card Terminal Basic Command Set
Part 5	Chipkarten mit synchroner Übertragung – ATR und Datenbereiche
Part 6	Chipkarten mit synchroner Übertragung – Übertragungsprotokolle
Part 7	Chipkarten mit synchroner Übertragung – Anwendung von Interindustry Commands
PKCS	*Die Public Key Cryptography Standards sind von der Firma RSA Inc. veröffentlichte Industriestandards mit Fokus auf den Einsatz von asymmetrischen Kryptoalgorithmen.*
PKCS #1 V 2.1 : 2001	RSA Encryption Standard ☒ *Dieser PKCS-Standard beschreibt die Funktionsweise der Ver- und Entschlüsselung mit dem RSA-Algorithmus*.
PKCS #3 V 1.4 : 1993	Diffie-Hellman Key-Agreement Standard *Dieser PKCS-Standard beschreibt die Funktionsweise eines Schlüssel-austauschverfahrens zwischen zwei Instanzen nach dem Verfahren von Diffie-Hellman.*
PKCS #5 V 2.0 : 1999	Password-Based Cryptography Standard *Dieser PKCS-Standard enthält Empfehlungen zur Realisierung von Verschlüsselung, Schlüsselableitung und MAC-Bildung auf der Grundlage von Schlüsseln, die aus Passwörtern gebildet werden.*
PKCS #11 V 2.11 : 2001	Cryptographic Token Interface Standard ☒ *Dies ist die weltweite De-facto-Norm für eine API zum Aufruf von kryptografischen Funktionen. Die API hat den Namen „Cryptoki" (cryptographic token interface) und beinhaltet Funktionen wie RC2, RC4, RC5, MD5, SHA-1, DES, Triple-DES, IDEA, RSA, DSA, MAC-Berechnung und Schlüsselerzeugung für die unterschiedlichen Kryptoalgorithmen*.
PKCS #13 V 1.0 : 1998	Elliptic Curve Cryptography Standard
PKCS #14 V 1.0 Proposal : 1998	Pseudorandom Number Generation Standard *Dieser nicht fertig gestellte und nicht sehr umfangreiche PKCS-Standard enthält Vorschläge zur Konzeption von Pseudozufallsgeneratoren.*
PKCS #15 V 1.1 : 2000	Cryptographic Token Information Format Standard ☒ *Dies ist die weltweite De-facto-Norm der notwendigen Datenelemente einer interoperablen Chipkarte für digitale Signatur. Der Standard enthält eine Beschreibung aller für eine Signaturkarte notwendigen Verzeichnisse und Dateien sowie eine ASN.1-Beschreibung aller in den Dateien gespeicherten Zertifikate, Schlüssel und sonstiger Verwaltungsinformationen*.

OCF - Programmer's Guide V 1.2 : 2001

Open Platform Card Specification 2.1 : 2001

☒ *Dies ist die wichtigste Spezifikation zum Thema Verwaltung von Applikationen auf Multiapplikations-Chipkarten. Die sehr umfangreiche Spezifikation enthält eine detaillierte Darstellung der Software- und Sicherheits-Architektur von Multiapplikations-Chipkarten sowie eine ausführliche Beschreibung von dazu notwendigen Kommandos. Der Anhang enthält unter anderem die Spezifizierung einer API für das Applikationsmanagement auf Java Cards, was zum De facto-Standard bei diesem Typ von Chipkarten avanciert ist.*[2]

RFC 1319 : 1992	The MD2 Message-Digest Algorithm
RFC 1320 : 1992	The MD4 Message-Digest Algorithm
RFC 1321 : 1992	The MD5 Message-Digest Algorithm
RFC 1750 : 1994	Randomness Recommendations for Security *Darstellung der Funktionsprinzipien von unterschiedlichen Zufallszahlengeneratoren. Aufbauend darauf werden Empfehlungen für Verfahren zur Konzeption einer hochwertigen Pseudozufallszahlen-generierung für PCs gegeben.*
RFC 2706 : 1999	ECML V1: Field Names for E-Commerce
SET Book 1, Version 1.0 : 1997	Secure Electronic Transaction Specification, Book 1: Business Description
SET Book 2, Version 1.0 : 1997	Secure Electronic Transaction Specification, Book 2: Programmer's Guide
SET Book 3, Version 1.0 : 1997	Secure Electronic Transaction Specification, Book 3: Formal Protocol Definition
TIA/EIA/IS-820 : 2000	Removable User Identity Module (R-UIM) for TIA/EIA Spread Spectrum Standards
TIA/EIA/IS-820-1 : 2001	Removable User Identity Module (R-UIM) for TIA/EIA Spread Spectrum Standards, Addendum 1
TIA/EIA/IS-839 : 2000	R-UIM Overview, Operation, and File Structure Support in TIA/EIA-136
TR 33.900, V 1.2.0 : 2000	3rd Generation Partnership Project; Technical Specification Group SA WG3; A Guide to 3rd Generation Security Architecture *Überblick zu Sicherheitsarchitektur, vorhandenen Sicherheitsfunktionen und möglichen Angriffsszenarien bei 3G-Mobilfunknetzen. Die sicherheitstechnischen Details sind in den entsprechenden Normen TS 33.102, TS 33.120 und TS 21.133 beschrieben.*
TS 21.111, Version 4.0.0 : 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; USIM and IC card requirements *Kurze Norm mit den Festlegungen der grundsätzlich notwendigen Funktionalitäten eines Sicherheitsmoduls, d. h. einer USIM, für ein UMTS-Mobilfunknetzwerk. Diese Norm ist das UMTS-Äquivalent zur GSM-Norm GSM 02.17.*
TS 21.133, Version 4.0.0 : 2001	

[2] Siehe auch Abschnitt 5.11 „Open Platform".

	Universal Mobile Telecommunications System (UMTS); 3G Security; Security Threats and Requirements
TS 22.038, Version 4.1.0 : 2001	
	3rd Generation Partnership Project; Technical Specification Group Terminals; USIM/SIM Application Toolkit (USAT, SAT); Service description; Stage 1
TS 22.112, Version 5.0.0 : 2001	
	Technical Specification; 3rd Generation Partnership Project; Technical Specification Group Terminals; USAT Interpreter – Stage 1
TS 23.038, V 4.3.0 : 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; Alphabets and language-specific information *Festlegung der Zeichen-Codierung bei SMS, USSD und der bei UMTS benutzten Zeichensätze.*
TS 23.040, V 4.3.0 : 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; Technical realization of the Short Message Service (SMS)
TS 23.048, Version 5.1.0 : 2001	
	3rd Generation Partnership Project; Technical Specification Group Terminals; Security Mechanisms for the (U)SIM application toolkit; Stage 2
TS 31.102, Version 4.2.0 : 2001	
	3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM Application ☒ *Spezifikation der logischen Eigenschaften der Chipkarten-Anwendung USIM, wobei diese durch eine Beschreibung der Schnittsstelle zwischen USIM und dem UMTS-Mobiltelefon realisiert ist. Die TS 31.102 beinhaltet eine detaillierte Beschreibung aller Dateien mit ihren Datenelementen, die Definition einiger weniger USIM-spezifischen Kommandos und eine Aufstellung von Kommandosequenzen für typische Abläufe. Zusammen mit der TS 31.101 ist diese Norm das UMTS-Äquivalent zur GSM-Norm GSM 11.11.*
TS 31.110, Version 4.0.0 : 2001	
	3rd Generation Partnership Project; Technical Specification Group Terminals; Numbering system for telecommunication IC card applications *Diese Norm wird in Zukunft als TS 101.220 veröffentlicht.*
TS 31.111, Version 4.4.0 : 2001	
	3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT) *Definition und ausführliche Beschreibung des USIM Application Toolkits für USIMs. USAT beschreibt eine Schnittstelle zwischen Mobiltelefon und USIM zur teilweisen Steuerung des Mobiltelefons von Zusatzanwendungen der USIM aus. Die Norm führt proaktive Kommandos für die USIM ein und definiert viele neue Kommandos im Zusammenhang mit der Steuerung des Mobiltelefons, wie beispielsweise Displayausgabe, Tastaturabfrage oder Versenden von Kurznachrichten. Das GSM-Äquivalent zu dieser Norm ist die GSM 11.14.*
TS 31.112, Version 5.0.0 : 2001	
	3rd Generation Partnership Project; Technical Specification Group Terminals; USAT Interpreter Architecture Description; Stage 2
TS 31.113, Version 5.0.0 : 2001	
	3rd Generation Partnership Project; Technical Specification Group Terminals; USAT Interpreter Byte Codes
TS 31.114, Version 1.1.0 : 2002	

3rd Generation Partnership Project; Technical Specification Group Terminals; USAT Interpreter Protocol and Administration

TS 31.121, Version 4.0.0 : 2001

3rd Generation Partnership Project; Technical Specification Group Terminals; UICC-Terminal Interface; USIM Application Test Specification

TS 31.122, Version 3.0.0 : 2000

3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Conformance Test Specification
Festlegung von Testumgebung, Testausrüstung, Testhierarchie und der einzelnen Testfälle für das Testing von USIMs. Die beschriebenen Tests zielen ausnahmslos auf die elektrischen und informationstechnischen Aspekte. Dazu sind Tests von der elektrischen Versorgung über Datenübertragung, Dateiverwaltung, Kommandos bis hin zu typischen Abläufen in der UMTS-Anwendung im Detail festgelegt. Diese Norm zeigt sehr gut und ausführlich, wie USIM Tests beschrieben, aufgebaut und durchgeführt werden können. Diese Norm ist das USIM-Äquivalent zur SIM-Testnorm GSM 11.17.

TS 31.900, Version 3.1.0 : 2001

3rd Generation Partnership Project; Technical Specification Group Terminals; SIM/USIM Internal and External Interworking Aspects

TS 33.102, Version 4.1.0 : 2001

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture
Zentrale Norm für die gesamte Sicherheitsarchitektur eines UMTS-Mobilfunknetzwerks bezüglich Netzwerkzugriff, Authentisierung, Vertraulichkeit und Datenintegrität. Diese Norm enthält unabhängig von einem bestimmten Kryptoalgorithmus eine vollständige Beschreibung der Netzwerksicherheitsfunktionen, Authentisierungsprotokolle, Verschlüsselungsverfahren sowie der Erzeugung der Authentisierungsvektoren und der verwendeten Schlüsselableitungen.

TS 33.103, Version 4.1.0 : 2001

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Integration guidelines

TS 33.105, Version 4.1.0 : 2001

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements

TS 33.120, Version 4.0.0 : 2001

Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives

TS 35.205, Version 4.0.0 : 2001

Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General

TS 35.206, Version 4.0.0 : 2001

Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification

TS 35.207, Version 4.0.0 : 2001

	Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' Test Data
TS 35.208, Version 4.0.0 : 2001	
	Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design Conformance
TS 35.909, Version 4.0.0 : 2001	
	Universal Mobile Telecommunications System (UMTS); 3G security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP Authentication and Key Generation functions
TS 42.009, V4.0.0 : 2001	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); Security aspects *Grundlagendokument mit einem Überblick über die wichtigen Sicherheitsaspekte eines PLMN.*
TS 51.011, Version 4.2.0 : 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface *Diese Norm ist nach dem neuen ETSI-Nummern-schema die GSM 11.1.*
TS 101.220, V 4.0.0 : 2001	Integrated Circuits Cards (ICC); ETSI numbering system for telecommunication application providers *Festlegung der AIDs, PIX und TAR für SIM, TETRA-SIM und USIM. Außerdem ist der Codierungsraum der PIX für die unterschiedlichen Arten von Zusatzanwendungen dieser Telekommunikations-Chipkarten definiert.*
TS 102.221, Version 4.4.0 : 2001	Smart cards; UICC-Terminal interface; Physical and logical characteristics ☒ *Spezifikation der physikalischen und logischen Eigenschaften einer USIM, wobei diese durch eine Beschreibung der Schnittstelle zwischen USIM und dem UMTS-Mobiltelefon realisiert ist. Die Spezifikation beinhaltet die Definition der Kartengrößen ID-1 und Plug-In, der mechanischen Rahmenparameter für die Karte und die Kontakte. Weiterhin ist in dieser Spezifikation die Festlegung aller elektrischen Rahmenwerte sowie Struktur und Dateninhalt von ATR und PPS enthalten, sowie die Definition der Übertragungsprotokolle, der Dateistrukturen, Sicherheitsmechanismen, Kommandos und Returncodes. Zusätzlich sind alle von einer bestimmten Telekommunikationsanwendung unabhängigen Dateien mit ihren Datenelementen sowie Kommandosequenzen aufgeführt. Diese Norm ist die Grundlage für ein Chipkarten-Betriebssystem für eine USIM und wird von der TS 31.102 mit allen anwendungsspezifischen Teilen für eine USIM ergänzt. Diese beiden Normen sind das UMTS-Äquivalent zur GSM-Norm GSM 11.11*
TS 102.222, Version 3.3.0 : 2001	Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications *In dieser Spezifikation sind die administrativen Kommandos zur Verwaltung von Dateien sowie die dazugehörigen Sicherheitsbedingungen für Telekommunikations-Chipkarten festgelegt.*
TS 102.223, Version 4.1.0 : 2001	

Smart cards; Card Application Toolkit (CAT)

Definition und ausführliche Beschreibung eines generischen Application Toolkits für Telekommunikations-Chipkarten. CAT beschreibt eine Schnittstelle zwischen Mobiltelefon und Chipkarte zur teilweisen Steuerung des Mobiltelefons von Zusatzanwendungen der Chipkarte aus. Die Norm definiert die Kommandos im Zusammenhang mit der Steuerung des Mobiltelefons, wie beispielsweise Displayausgabe, Tastaturabfrage oder Versenden von Kurznachrichten. Auf dieser Grundlagennorm baut beispielsweise GSM 11.14 und TS 31.111 auf.

TS 102.224, Version 1.0.0 : 2001

Smart cards; Security mechanisms for the Card Application Toolkit; Functional requirements

TS 102.225, Version 1.0.0 : 2001

Smart cards; Secured packet structure for UICC applications

TS 102.226, Version 1.0.0 : 2001

Smart cards; Remote APDU Structure for UICC based Applications

TS 102.230, Version 4.0.0 : 2001

Smart cards; UICC-Terminal Interface; Physical, Electrical and Logical Test Specification

Festlegung der physikalischen und elektrischen Tests für UICCs. Weiterhin sind grundlegende Tests für die Kommunikationsverbindung zur

UICC und Tests zu den beiden Übertragungsprotokollen T = 0 und T = 1 beschrieben.

TS 102.240, Version 1.0.0 : 2001

Smart Cards; UICC Application Programming Interface (UICC API); Service description

TS 102.241, Version 1.0.0 : 2001

UICC Application Programming Interface (UICC API); UICC API for Java Card

TS 102.241, Version 4.4.0 : 2002

Universal Mobile Telecommunications System (UMTS); Network architecture

Unicode Standard, Version 3.1.1 : 2001

Universal Serial Bus Specification, Revision 2.0, 2000

Diese sehr umfangreiche Spezifikation ist die Grundlage für die USB-Schnittstelle.

Wireless Application Protocol Identity Module Specification, Version 260 : Juli 2001

Spezifikation der physikalischen und logischen Eigenschaften einer WIM, der digitalen Signaturanwendung für Telekommunikations-Chipkarten. Es sind alle für eine WIM-Anwendung notwendigen Mechanismen, Kommandos, Datenelemente und Dateien aufgeführt.