

Das Glossar aus dem „Handbuch der Chipkarten“

Version: September 2003



Dieses Glossar 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.

Diese Datei darf kopiert werden, solange ihr Inhalt nicht verändert wird. Sie ist in diesem Format problemlos ausdrückbar.

Die Autoren haben den Inhalt dieses Dokuments sorgfältig zusammengestellt, übernehmen jedoch keinerlei Haftung für die Korrektheit der Angaben.

Verbesserungs- und Ergänzungsvorschläge sind jederzeit herzlich willkommen. Diese können an die e-mail-Adresse Rankl@gmx.de mit dem Stichwort „Glossar“ 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

μ P-Karte	andere Bezeichnung für → <i>Mikroprozessorkarte</i>
0-PIN	Eine für alle neu ausgegebenen → <i>Chipkarten</i> einheitliche und bekannte → <i>PIN</i> , mit der jedoch kein Zugriff auf die eigentlichen Benutzerfunktionen möglich ist. Sie ist damit eine → <i>Trivial-PIN</i> . Die 0-PIN muss bei der erstmaligen Benutzung der Karte in die vom Benutzer gewünschte PIN mit den üblichen Mechanismen (i. d. R. CHANGE CHV) abgeändert werden, wobei die 0-PIN als neue gültige PIN nicht erlaubt ist. Zweck der 0-PIN ist, dass der Benutzer beim Erhalt der Karte zweifelsfrei feststellen kann, ob sich diese noch in ihrem ursprünglichen Ausgabezustand befindet oder unberechtigt auf dem Zustellungsweg bereits benutzt wurde. Der Name 0-PIN stammt daher, weil oft der Wert "0000" für diese Art von PIN verwendet wird.
1 μ m, 0,8 μ m, ...-Technologie	Bei der Herstellung von Halbleiterchips wird traditionell die Leistung der verwendeten Technologie durch die Längenangabe für die kleinste mögliche Transistorstruktur auf dem Halbleiter beschrieben. Dies ist meist die Breite des Gateoxids bei Transistoren. Die momentan minimal möglichen Strukturbreiten liegen in der Größenordnung von 0,25 μ m und 0,13 μ m. Größere Strukturen auf dem Chip sind selbstverständlich immer möglich.
1, 2, 4, 8, ..., x k-Chip	Die Bezeichnung x k-Chip (mit x als ganzzahliger positiver Zahl) ist die oftmals im Sprachgebrauch vereinfachende Typenbezeichnung für → <i>Mikrocontroller</i> mit einer bestimmten EEPROM-Größe (→ <i>EEPROM</i>) in kByte. Ein 32 k-Chip ist demnach ein Chipkarten-Mikrocontroller mit 32 kByte EEPROM. Für überschlagsmäßige Vergleiche von üblichen Chipkarten-Mikrocontrollern ist die Angabe der EEPROM-Größe durchaus ausreichend.
1G (erste Generation)	Bezeichnet die erste Generation von Mobilfunknetzen. Diese arbeiten analog und sind zellulär aufgebaut. Typische Beispiele für 1G-Systeme sind AMPS und das deutsche C-Netz.
2G (zweite Generation)	Bezeichnet die zweite Generation von Mobilfunknetzen. Diese arbeiten digital und sind zellulär aufgebaut. Typische Beispiele für 2G-Systeme sind → <i>GSM</i> und → <i>CDMA</i> .
3DES	→ <i>Triple-DES</i>
3G (dritte Generation)	Bezeichnet die dritte Generation von Mobilfunknetzen. Diese arbeiten digital und sind zellulär aufgebaut. Das typische Beispiel für ein 3G-System ist → <i>UMTS</i> . UMTS gehört wiederum zur Familie von → <i>IMT-2000</i> .
3GPP (<i>third generation partnership project</i>) [3GPP]	Das <i>third generation partnership project</i> , gegründet von den fünf Normungsinstituten ANSI T1 (USA), ARIB (Japan), ETSI (Europa), TTA (Korea) und TTC (Japan), hat zur Aufgabe, weltweit verwendbare technische Spezifikationen für ein Mobilfunksystem der dritten Generation (→ <i>3G</i>) auf der Grundlage eines weiterentwickelten GSM-Kernsystems (→ <i>GSM</i>) zu erstellen. Die betroffenen Normungsinstanzen setzen diese Spezifikationen anschließend in entsprechende Normen um. 3GPP wurde im Dezember 1998 in Kopenhagen von den wesentlichen internationalen Telekommunikations-Normungsinstanzen ins Leben gerufen. Ähnliche Aufgaben wie 3GPP hat 3GPP2 (<i>third generation partnership project 2</i>), hier ist jedoch der Fokus auf die Weiterentwicklung von Nicht-GSM-Systemen in Richtung dritter Generation wie beispielsweise CDMA-Systemen.
3GPP2	→ <i>3GPP</i>
4G (vierte Generation)	Bezeichnet die vierte Generation von Mobilfunknetzen. Diese stehen jedoch am Anfang der Konzeptionierung.
8, 16, 32 bit CPU (<i>central processing unit</i>)	Eine wichtige Kenngröße für die Leistungsfähigkeit eines → <i>Mikroprozessors</i> ist die Breite der Register für die zu verarbeitenden Daten im Rechenwerk. Sie wird in der Anzahl der Bits angegeben.
A2C (<i>administration to customer</i>)	Bezeichnet die Abwicklung von Geschäften des → <i>E-Commerce</i> zwischen öffentlicher Verwaltung und Endverbrauchern.
A3 (<i>algorithm 3</i>)	Bezeichnung für eine kryptografische Funktion bei → <i>GSM</i> für die Authentisierung des SIM durch das Hintergrundsystem mittels eines Challenge-Response-Verfahrens. A3 wird vom Netzbetreiber gewählt, ist also nicht einheitlich für das gesamte GSM-System.
A5 (<i>algorithm 5</i>)	Bezeichnung für eine kryptografische Funktion bei → <i>GSM</i> für die Verschlüsselung der Sprachdaten auf der Luftschnittstelle zwischen Mobile Station und Ba-

	se Station bzw. Hintergrundsystem. A5 ist einheitlich für das gesamte GSM-System.
A8 (<i>algorithm 8</i>)	Bezeichnung für eine kryptografische Funktion bei → <i>GSM</i> zur Erzeugung des Sitzungsschlüssels Kc für die Sprachdatenverschlüsselung auf der Luftschnittstelle. A8 wird vom Netzbetreiber gewählt, ist also nicht einheitlich für das gesamte GSM-System.
Ablaufsteuerung (<i>Sequence Control</i>)	Legt verbindlich eine bestimmte Reihenfolge von Aktivitäten fest. Beispielsweise wird bei der gegenseitigen Authentisierung von → <i>Chipkarte</i> und Hintergrundsystem die korrekte Reihenfolge der → <i>Kommandos</i> durch eine Ablaufsteuerung in der <i>Chipkarte</i> realisiert. Dazu besitzt das → <i>Chipkarten-Betriebssystem</i> einen Zustandsautomaten (<i>state machine</i>), mit dem durch festlegbare Zustände (<i>states</i>) und Zustandsübergänge (<i>state transition</i>) bestimmte einzuhaltende Kommandosequenzen definierbar sind. ¹
Abschaltsequenz	Legt für einen → <i>Chipkarten-Mikrocontroller</i> die Deaktivierungsreihenfolge der elektrischen Signale beim Ausschalten einer → <i>Chipkarte</i> fest. Sie sagt nichts über die Reihenfolge der mechanischen Dekontaktierung aus. Der Zweck der Abschaltsequenz ist, die gegenüber Ladungen und Spannungen an den Kontakten empfindlichen <i>Chipkarten-Mikrocontroller</i> zu schützen (→ <i>Anschaltsequenz</i>).
Acquirer (Sammelbeauftragter)	Instanz, welche die Errichtung und Verwaltung der datentechnischen Verbindungen und des Datenaustauschs zwischen dem Betreiber eines Zahlungssystems und den einzelnen Service-Anbietern betreibt. Der Acquirer kann die erhaltenen einzelnen Transaktionen zusammenfassen, so dass der Betreiber des Zahlungssystems nur mehr gesammelte Zertifikate erhält.
AES (<i>advanced encryption standard</i>)	Symmetrischer → <i>Kryptoalgorithmus</i> . Er wurde ursprünglich von Joan Daemen und Vincent Rijmen entwickelt und als Rijndael publiziert. Das → <i>NIST</i> hat ihn nach einer Ausschreibung und einem Bewertungsverfahren im Jahr 2000 als Nachfolger des DES ausgewählt und 2001 als US-Norm (FIPS 197) publiziert. ²
AFNOR (<i>Association Française de Normalisation</i>)	Französische Normungsorganisation mit Sitz in Paris.
AID (<i>application identifier</i>)	Kennzeichen für eine → <i>Anwendung</i> auf einer → <i>Chipkarte</i> ; in der ISO/IEC 7816-5 definiert. Ein Teil des AID kann national oder international registriert werden und ist dann für die registrierte Anwendung reserviert und weltweit eindeutig. Der AID besteht aus den beiden Datenelementen RID (<i>registered identifier</i>) und PIX (<i>proprietary identifier</i>). ³
AMPS (<i>advanced mobile phone system</i>)	Zellularer Mobiltelefonstandard, der vor allem in USA, Lateinamerika, Australien und in Teilen von Asien verbreitet ist. AMPS arbeitet analog im 800-MHz-Bereich. AMPS-Endgeräte besitzen keine → <i>Chipkarte</i> und wurden u. a. auch aus diesem Grund oft erfolgreich angegriffen. Die Weiterentwicklung vom AMPS ist D-AMPS, ein digitaler Standard, der ebenfalls den 800-MHz-Bereich benutzt.
analog	Mit diesem Begriff bezeichnet man Systeme, bei denen ein Signal eine unbegrenzte Anzahl von Werten annehmen kann.
Analyse (<i>analysis</i>)	Im Sinne der Softwareentwicklung die Ermittlung der Anforderungen des Auftragsgebers an ein informationstechnisches System sowie deren eindeutige und vollständige Beschreibung. Vereinfacht ausgedrückt, ist das Ergebnis der Analyse eine Beschreibung, „was“ gemacht werden soll. Der nächste Schritt bei einer sequentiellen Softwareentwicklung ist das → <i>Design</i> .
Anonymisierung	Veränderung von personenbezogenen Daten in einer Weise, dass es nicht mehr möglich ist, diese veränderten Daten der ursprünglichen Person zuzuordnen (→ <i>Pseudonymisierung</i>).
Anschaltsequenz	Legt für einen → <i>Chipkarten-Mikrocontroller</i> die Aktivierungsreihenfolge der elektrischen Signale beim Einschalten einer → <i>Chipkarte</i> fest. Sie sagt nichts über die Reihenfolge der mechanischen Kontaktierung aus. Zweck der Anschaltsequenz ist, die gegenüber Ladungen und Spannungen an den Kontakten empfindlichen <i>Chipkarten-Mikrocontroller</i> zu schützen (→ <i>Abschaltsequenz</i>).
ANSI (<i>American National Standards</i>)	US-amerikanische Normungsorganisation mit Sitz in New York.

¹ Siehe auch Abschnitt 5.8 „Ablaufsteuerung“.

² Siehe auch Abschnitt 4.7.1 „Symmetrische Kryptoalgorithmen“.

³ Siehe auch Abschnitt 5.6.1 „Dateitypen“.

<i>Institute</i>) [ANSI]	
Antikollisionsverfahren	Technisches Verfahren, das den störungsfreien Vielfachzugriff auf kontaktlose Karten ermöglicht.
Antwort (<i>response</i>)	→ <i>Kommando</i>
Antwort-APDU (<i>response-APDU</i>)	Antwort (→ <i>Kommando</i>) der → <i>Chipkarte</i> auf eine vom Terminal abgesendete → <i>Kommando-APDU</i> . Sie setzt sich aus den optionalen Antwortdaten und den je 1 Byte langen obligatorischen Statuswörtern SW1 und SW2 zusammen (→ <i>APDU</i>). ⁴
Anwendung (<i>application</i>)	Alle Daten, Dateien, → <i>Kommandos</i> , Abläufe, Zustände, Mechanismen, Algorithmen und Programme innerhalb einer → <i>Chipkarte</i> , um sie im Rahmen eines bestimmten Systems zu betreiben. Eine Anwendung mit den dazugehörigen Daten befindet sich in der Regel in einem eigenen DF direkt unterhalb des MFs. Dies wird oft auch als Oncard-Anwendung bezeichnet. Das Gegenstück ist die Offcard-Anwendung, die alle Programme und Daten einschließt, die sich nicht auf der Chipkarte befinden, jedoch für die Nutzung der Oncard-Anwendung auf der Chipkarte notwendig sind.
Anwendungsbetreiber	Eine Instanz, die eine → <i>Anwendung</i> auf → <i>Chipkarten</i> betreibt. Im Allgemeinen ist der Anwendungsbetreiber identisch mit dem Anwendungsanbieter.
APDU (<i>application protocol data unit</i>)	Softwaretechnischer Datencontainer, in den die Daten einer → <i>Anwendung</i> verpackt werden, um sie zwischen Terminal und → <i>Chipkarte</i> auszutauschen. Eine APDU wird vom Übertragungsprotokoll in eine TPDU (<i>transport protocol data unit</i>) umgewandelt und dann über die serielle Schnittstelle vom Terminal bzw. der Chipkarte verschickt. APDUs lassen sich in → <i>Kommando-APDU</i> und → <i>Antwort-APDU</i> einteilen. ⁵
API (<i>application programming interface</i>)	Detailliert spezifizierte Softwareschnittstelle für den Zugriff auf bestimmte Funktionen eines Programms.
Applet-Entwickler (<i>applet developer</i>)	Person oder Instanz, die ein → <i>Applet</i> entwickelt.
Applet	In der Programmiersprache Java erstelltes Programm, das von der virtuellen Maschine eines Rechners ausgeführt wird. Die Funktionalität eines Applets ist aus Sicherheitsgründen auf die vorher festgelegte Programmumgebung beschränkt. Ein Applet wird im Bereich von → <i>Chipkarten</i> manchmal auch Cardlet genannt und entspricht in der Regel einer Chipkarten-Anwendung (→ <i>Anwendung</i>).
ASK (<i>Amplitude Shift Keying</i> – Amplitudentastung)	Verfahren, bei dem die Amplitude der Trägerschwingung zwischen zwei Zuständen umgeschaltet wird.
ASN.1 (<i>abstract syntax notation one</i>)	Beschreibungssprache (Syntax und Grammatik) für Daten, mit der sich Daten und Datentypen unabhängig vom benutzenden Computersystem eindeutig definieren und darstellen lassen. Mit den → <i>BER</i> (<i>basic encoding rules</i>) und den → <i>DER</i> (<i>distinguished encoding rules</i>) werden die entsprechenden Daten dann konkret codiert. ASN.1 ist durch ISO/IEC 8824 und ISO/IEC 8825 definiert. ⁶
Assembler	Programm, das Assemblerprogramme in von einem Prozessor ausführbare Maschinensprache übersetzt. Nach dem Assembliervorgang muss das Programm üblicherweise noch mit einem Linker gebunden (<i>linking</i>) werden. Der Begriff Assembler wird jedoch oft auch als Kurzform von Assemblerprogrammcode benutzt.
asymmetrischer Kryptoalgorithmus	→ <i>Kryptoalgorithmus</i>
asynchrone Datenübertragung	Hier werden die Daten unabhängig von einem vorgegebenen Zeitraster übertragen (→ <i>synchrone Datenübertragung</i>).
atomarer Ablauf (<i>atomic operation</i>)	Eine oder mehrere Operationen in einem Programm, die entweder vollständig oder überhaupt nicht ausgeführt werden. Bei → <i>Chipkarten</i> werden atomare Abläufe oft im Zusammenhang mit EEPROM-Schreibroutinen eingesetzt. Damit

⁴ Siehe auch Abschnitt 6.5 „Struktur der Nachrichten – APDUs“.

⁵ Siehe auch Abschnitt 6.5 „Struktur der Nachrichten – APDUs“.

⁶ Siehe auch Abschnitt 4.1 „Strukturierung von Daten“.

	wird sichergestellt, dass Dateninhalte zu jedem Zeitpunkt konsistent sind. ⁷
ATR (<i>answer to reset</i>)	Sequenz von Bytes, welche eine → <i>Chipkarte</i> als Antwort auf den (Hardware-) Reset aussendet. Der ATR beinhaltet u.a. diverse Parameter für das Übertragungsprotokoll zur <i>Chipkarte</i> . ⁸
Attribut (<i>attribute</i>)	Im Sinne der → <i>objektorientierten</i> Programmierung die Datencontainer (im prozeduralen Sinne die Variablen), die ein → <i>Objekt</i> enthält. Die Attributwerte können durch → <i>Methoden</i> gelesen oder geändert werden.
Auswurfleser	Terminal, das eine gesteckte Karte durch ein elektrisches oder mechanisches Signal automatisch auswerfen kann.
Authentifizierung	anderer Ausdruck für → <i>Authentisierung</i>
Authentisierung	Vorgang des Nachweises der Echtheit einer Instanz (z. B. einer <i>Chipkarte</i>) durch kryptografische Verfahren. Vereinfacht ausgedrückt, stellt man bei der Authentisierung durch ein festgelegtes Verfahren fest, ob jemand wirklich derjenige ist, der er vorgibt zu sein.
Authentizität	Echtheit und Unverändertheit einer Instanz oder Nachricht.
Automat	In der Informationstechnik Teil eines Programms, das einen Ablauf auf der Grundlage eines vorher definierten Zustandsdiagramms (d. h. Zustände mit Zustandsübergängen) bestimmt.
Autorisierung	Prüfung, ob eine bestimmte Aktion ausgeführt werden darf, d. h. jemand wird zu etwas ermächtigt. Wird beispielsweise eine Kreditkartentransaktion durch den Kreditkarten-Herausgeber autorisiert, so sind die Kartendaten auf Korrektheit der Daten, Einhaltung der erlaubten Betragsgrenzen und ähnliche Kriterien geprüft worden und die beabsichtigte Zahlung wird daraufhin zugelassen. Eine Autorisierung kann durch die Authentisierung der betreffenden Instanz (z. B. einer <i>Chipkarte</i>) zustande kommen. Vereinfacht ausgedrückt, erteilt man bei der Autorisierung jemandem die Erlaubnis, etwas Bestimmtes zu tun.
B2A (<i>business to administration</i>)	Bezeichnet die Abwicklung von Geschäften des → <i>E-Commerce</i> zwischen Unternehmen und öffentlicher Verwaltung.
B2B (<i>business to business</i>)	Bezeichnet die Abwicklung von Geschäften des → <i>E-Commerce</i> zwischen Unternehmen.
B2C (<i>business to customer</i>)	Bezeichnet die Abwicklung von Geschäften des → <i>E-Commerce</i> zwischen Unternehmen und Endverbrauchern.
Bad Day Szenario	anderer Ausdruck für → <i>Schlechtfall</i>
baud	Benennt während einer Datenübertragung die Anzahl von Statusänderungen pro Sekunde. Je Statusänderung können jedoch abhängig vom Übertragungsverfahren ein oder mehrere Informationsbits übertragen werden. Aus diesem Grund kann Baud nur in dem Sonderfall, dass bei jeder Statusänderung lediglich ein Bit übertragen wird, mit der Übertragungsrateneinheit bit/s gleichgesetzt werden.
Bearer (Träger)	Bezeichnet den Trägerdienst, mit dessen Hilfe Daten an ein Endgerät übertragen werden. Ein möglicher Bearer für WAP ist beispielsweise SMS.
Bellcore-Angriff (<i>Bellcore-Attack</i>)	→ <i>differentielle Fehleranalyse</i>
Benutzer (<i>user</i>)	Person, die eine → <i>Chipkarte</i> verwendet. Sie muss nicht unbedingt der → <i>Karteninhaber</i> sein.
BER (<i>basic encoding rules</i>)	Die in → <i>ASN.1</i> festgelegten grundlegenden Codierungsregeln BER (<i>basic encoding rules</i>) dienen dazu, Daten als Datenobjekte zu codieren. BER-codierte Datenobjekte besitzen ein Kennzeichen (<i>tag</i>), eine Längenangabe (<i>length</i>), den eigentlichen Datenteil (<i>value</i>) und optional eine Endkennung. Aus diesem Grund werden sie auch als TLV-codierte Daten bezeichnet. Das BER-Format lässt auch verschachtelte Datenobjekte zu. Eine Untermenge der grundlegenden Codierungsregeln BER sind die DER (<i>distinguished encoding rules</i>). Diese geben unter anderem an, wie die Längenangabe der jeweiligen Datenobjekte zu codieren ist (1, 2 oder 3 Byte lang). ⁹
Betriebssystem	Umfasst alle Programme eines digitalen Rechnersystems, die zusammen mit den

⁷ Siehe auch Abschnitt 5.10 „Atomare Abläufe“.

⁸ Siehe auch Abschnitt 6.2 „Answer to Reset – ATR“.

⁹ Siehe auch Abschnitt 4.1 „Strukturierung von Daten“.

(OS – operating system)	Eigenschaften der Rechneranlage die Grundlage der möglichen Betriebsarten bilden und insbesondere die Abwicklung von Programmen steuern und überwachen. ¹⁰
Betriebssystemhersteller (operating system manufacturer)	Instanz, die die Programmierung und den Test eines → <i>Betriebssystems</i> durchführt.
big Endian	→ <i>Endianness</i>
binärkompatibler Programmcode	Programm, das direkt vom → <i>Mikroprozessor</i> ohne Übersetzung o. Ä. ausgeführt werden kann (→ <i>Programmcode</i>).
Blacklist	anderer Ausdruck für → <i>Sperrliste</i>
Blackbox-Test	Bei diesem Test geht man davon aus, dass die testende Instanz keine Kenntnisse von den internen Abläufen, Funktionen und Mechanismen der zu prüfenden Software hat.
Bluetooth [Bluetooth]	Eine für den Nahbereich (<100 m) konzipierte drahtlose Netzwerktechnologie im 2,4 GHz Frequenzbereich mit einer maximalen Bruttoübertragungsrate in der Größenordnung von 1 MBit/s. Die Firma Ericsson als Initiator dieser Technologie wollte mit der Namensgebung an den vor ca. 1000 Jahren lebenden dänischen König Harald II. erinnern, der den Beinamen Bluetooth trug. Sein Verdienst war die Zusammenfassung vieler einzelner Gebiete zu einem einheitlichen Königreich.
Bond-out-Chip	Ein in einem vielpoligen Keramikgehäuse untergebrachter Mikrocontroller, bei dem alle chipinternen Busse für Speicher frei zugänglich sind, sodass das üblicherweise maskenprogrammierte → <i>ROM</i> durch einen chipexternen Speicher ersetzt werden kann. Zweck eines Bond-out-Chips ist die Schaffung der Möglichkeit, ohne → <i>ROM-Maske</i> Tests von Software auf einer Zielhardware durchzuführen.
Bootloader (Urlader)	Einfaches kleines Programm, dessen einzige Funktion darin besteht, weitere und umfangreichere Programme beispielsweise über eine serielle Schnittstelle in einen Speicher nachzuladen und dort zu starten (→ <i>Loader</i>). Der Bootloader wird in der Regel dazu benutzt, den eigentlichen Programmcode in einen neuen Chip oder in ein neues elektronisches Gerät zu laden. Oft kann der Bootload-Vorgang nur ein einziges Mal ausgeführt werden.
Börsenanbieter (purse provider)	Die Organisation, die für die Gesamtfunktionalität und Sicherheit eines Börsensystems verantwortlich ist. Er ist im Regelfall auch der Herausgeber des elektronischen Kartengeldes und garantiert für die Einlösung.
Börseninhaber (purse holder)	Die Person, die die → <i>Chipkarte</i> mit der elektronischen Geldbörse besitzt.
BPSK (Binary Phase Shift Keying)	Phasenumtastung von 180°, wodurch sich zwei Phasenzustände ergeben.
Browser	Programm zur Betrachtung von Hypertextdokumenten, zur Navigation zwischen diesen Dokumenten und zur Ausführung von in die Hypertextdokumente eingebettetem → <i>Programmcode</i> . Einfach aufgebaute, wenig Speicher und Rechenleistung benötigende Browser werden oft auch als Microbrowser bezeichnet. Diese können beispielsweise als → <i>Anwendung</i> innerhalb eines → <i>Chipkarten-Betriebssystems</i> laufen (z. B.: SIM Alliance-Browser, auch S@T-Browser genannt) oder in die Software eines Mobiltelefons integriert sein (z. B. WAP-Browser). Browser können durch nachträglich ladbare Softwarekomponenten, so genannte Browser-Plug-Ins, in ihrem Funktionsumfang erweitert werden.
Brute-force-Angriff (brute force attack)	Angriff auf ein kryptografisches System durch die Berechnung aller Möglichkeiten eines Schlüssels.
BSI (Bundesamt für Sicherheit in der Informationstechnik) [BSI]	Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde 1991 gegründet und ist der Nachfolger der deutschen Zentralstelle für das Chiffrierwesen. Das BSI hat folgende Aufgaben: Untersuchung von Sicherheitsrisiken bei IT-Anwendungen, Prüfung und Bewertung der Sicherheit von IT-Systemen, Zulassung von IT-Systemen für Behörden und Unterstützung der Strafverfolgungs- und Verfassungsschutzbehörden. Außerdem bietet das BSI Beratung von Herstellern, Vertreibern und Anwendern in Fragen der IT-Sicherheit an und legt insofern oft auch die Rahmenbedingungen für Kryptografianwendungen in Deutschland fest.

¹⁰ Text in Anlehnung an die deutsche Norm DIN 44300.

buffern	Typischer Angriff bei Magnetstreifenkarten. Dazu wird der Magnetstreifen zunächst gelesen und gespeichert. Nachdem ein Terminal Daten (z. B. den Fehlbedienungs-zähler) auf dem Magnetstreifen verändert hat, werden die ursprünglichen Daten wieder auf den Magnetstreifen zurückgeschrieben.
bug fix	In der Softwareentwicklung die Ausbesserung eines bekannten Fehlers (<i>bug</i>) durch zusätzlichen → <i>Programmcode</i> . Der Fehler als solcher wird durch einen bug fix beseitigt, im Gegensatz zum → <i>work around</i> .
Burst	→ <i>Signalburst</i>
Bytecode (<i>bytecode</i>)	Dieser Begriff ist mehrfach besetzt und kann nur in seinem verwendeten Kontext korrekt interpretiert werden. Eine weit verbreitete Verwendung des Begriffs steht im Zusammenhang mit Java. Unter Bytecode wird dabei der von einem Java-Compiler aus dem Source-Code erzeugte (d.h. compilierte) Zwischencode für die Java Virtual Machine (JVM) bezeichnet. Der Bytecode ist von der Firma Sun standardisiert und wird vom Interpreter der Java Virtual Machine ausgeführt. Eine weitere Verwendung des Begriffs Bytecode gibt es im Umfeld von Mikrobrowsern (→ <i>Browser</i>). Unter „Bytecode“ wird hier das von einem so genannten Bytecode-Converter übersetzte Hypertextdokument verstanden. Das Ergebnis der Übersetzung ist der Bytecode, der dann im nächsten Schritt vom Mikrobrowser interpretiert wird.
CAD (<i>card acceptance device</i>)	Im Bereich des elektronischen Zahlungsverkehrs wird statt der ISO-Abkürzung → <i>IFD (interface device)</i> oft die Bezeichnung CAD für Chipkarten-Terminal benutzt.
CAMEL (<i>customized applications for mobile enhanced logic</i>)	Zusätzlich mögliches Charakteristikum von → <i>GSM</i> , um die Funktionalität von so genannten intelligenten Netzen (IN – <i>Intelligent Network</i>) zu unterstützen. Mit CAMEL können beispielsweise Rufnummern während des Rufaufbaus vom Netzwerk geändert werden. Damit lassen sich dann auf einfache Weise Anwendungen wie weltweites → <i>Roaming</i> mit vorbezahlten Karten oder weltweit verfügbare einheitliche Servicenummern realisieren.
CAP-Datei (<i>card application file – CAP-file</i>)	Datenaustauschformat zwischen der Java Offcard Virtual Machine und der Java Oncard Virtual Machine.
<i>Card Modelling Language</i> (CML)	Abstrakte und betriebssystemunabhängige Beschreibungssprache für die Definition von Chipkarten-Anwendungen (→ <i>Anwendung</i>).
<i>Cardholder Verification Method</i> (CVM)	Verfahren zur → <i>Identifizierung</i> von Personen. Üblicherweise ist dies die PIN-Prüfung, es kann jedoch auch bei höher entwickelten Systemen eine biometrische Benutzeridentifizierung sein.
Cardlet	→ <i>Applet</i>
CCITT (<i>Comité Consultatif International Télégraphique et Téléphonique</i>)	Einst ein internationaler Ausschuss für Telefon- und Telegraphendienste mit Sitz in Genf. Mittlerweile ist die CCITT unter Erweiterung der Aufgaben in → <i>ITU</i> umgetauft worden.
CCS (<i>cryptographic checksum</i>)	Kryptografische Prüfsumme über Daten, mit der Manipulationen dieser Daten während der Speicherung erkannt werden können. Werden Daten während ihrer Übertragung mit einer CCS geschützt, so spricht man von einem → <i>MAC (message authentication code)</i> .
CDMA (<i>code division multiple access – Codevielfachzugriff</i>)	Vielfachzugriffsverfahren zur parallelen Datenübertragung von mehreren Sendern zu einem Empfänger innerhalb eines Frequenzspektrums. Dazu wird im Sender das schmalbandige Funksignal durch eine für diesen Sender spezifische Abbildungsvorschrift auf ein breitbandiges Funksignal abgebildet, d. h. gespreizt. Bei bekannter senderindividueller Abbildungsvorschrift kann dann im Empfänger aus dem empfangenen breitbandigen Funksignal das schmalbandige Funksignal wiederhergestellt werden. CDMA wird bei UMTS auf der Luft-schnittstelle zwischen Mobiltelefon und Basisstation verwendet. ¹¹ Bei WCDMA (<i>wideband code division multiple access</i>) findet → <i>Uplink</i> und → <i>Downlink</i> in zwei getrennten Frequenzspektren statt, weshalb dieses CDMA-Verfahren oft auch als FD/CDMA (<i>frequency division/code division multiple access</i>) bezeichnet wird. Bei TD/CDMA (<i>time division/code division multiple access</i>) wird die Trennung zwischen Uplink und Downlink durch die Benutzung unterschiedlicher Zeitschlitze realisiert.

¹¹ Siehe auch Abschnitt 13.1.1 „Vielfachzugriffsverfahren“.

CEN (<i>Comité Européen de Normalisation</i>) [CEN]	Die europäische Normungsorganisation CEN in Brüssel (Belgien) setzt sich aus den nationalen Normungsorganisationen aller europäischen Länder zusammen und ist die offizielle Institution der EU für europäische Normung.
CEPS (<i>common electronic purse specifications</i>) [CEPSCO]	Eine Spezifikation für → <i>elektronische Geldbörsen</i> mit dem Fokus auf weltweite Interoperabilität (→ <i>interoperabel</i>) und Einbeziehung aller Komponenten, die für den Betrieb eines elektronischen Geldbörsensystems notwendig sind. CEPS wurde 1999 in ihrer ersten Version von CEPSCO veröffentlicht und baut auf vielen Prinzipien der europäischen Norm für elektronische Geldbörsen EN 1546 auf.
CEPT (<i>Conférence Européenne des Postes et Télécommunications</i>)	Europäische Normungsorganisation der nationalen Telekommunikationsgesellschaften.
Challenge-Response-Verfahren	Das im Chipkartenbereich übliche Authentisierungsverfahren. Ein geheimer Schlüssel eines Kryptoalgorithmus ist das gemeinsame Geheimnis der beiden Kommunikationspartner. Ein Kommunikationspartner sendet dem anderen eine Zufallszahl (<i>challenge</i>), dieser verschlüsselt diese mit einem Kryptoalgorithmus und sendet das Ergebnis an den Fragesteller zurück (<i>response</i>). Der Fragesteller wendet nun auf die erhaltene verschlüsselte Zufallszahl die Umkehrfunktion des Kryptoalgorithmus an und vergleicht das Ergebnis dieser Operation mit der ursprünglich gesendeten Zufallszahl. Stimmen beide überein, so weiß der Fragesteller, dass der andere Kommunikationsteilnehmer ebenfalls den geheimen Schlüssel kennt und schließt daraus, dass dieser authentisch ist. ¹²
Chinesischer Restklassensatz (<i>chinese remainder theorem</i>)	Verfahren, um den → <i>RSA</i> -Algorithmus zu beschleunigen. Dazu müssen jedoch die beiden geheimen Primzahlen p und q bekannt sein, weshalb das Verfahren nur zur Entschlüsselung bzw. zum Signieren benutzt werden kann.
Chipgröße (<i>chip size</i>)	Fläche eines Chips, üblicherweise in Quadratmillimeter gemessen. Sie ist weitgehend direkt proportional zum Chip-Preis. Die maximale Chipgröße bei Chipkarten-Mikrocontrollern liegt aufgrund der heute üblichen Module bei ca. 25 mm ² .
Chipkarte (<i>chip card</i>)	Der allgemeine Begriff für eine Karte, meist aus Kunststoff, die ein oder mehrere Halbleiterchips enthält. Eine Chipkarte kann entweder eine → <i>Speicherkarte</i> oder eine → <i>Mikroprozessorkarte</i> sein.
Chipkarten-Anwendung (<i>smart card application</i>)	→ <i>Anwendung</i>
Chipkarten-Betriebssystem (<i>smart card operating system</i>)	(Oft auch COS (<i>card operating system</i>) genannt) Eine auf die Belange von Chipkarten spezialisierte Form eines → <i>Betriebssystem</i> ; umschließt alle Programme auf einem → <i>Chipkarten-Mikrocontroller</i> , die den Betrieb und die Verwaltung von Chipkarten-Anwendungen (→ <i>Anwendung</i>) ermöglichen. Dazu müssen die für eine oder mehrere Chipkarten-Anwendungen benötigten Daten, Dateien, → <i>Kommandos</i> , Abläufe, Zustände, Mechanismen, Algorithmen und Programme in geeigneter Weise unterstützt werden. Bietet ein Chipkarten-Betriebssystem die Möglichkeit des Betriebs mehrerer parallel existierender Anwendungen, so spricht man von multiapplikationsfähig. Die Entwicklungstendenz von Chipkarten-Betriebssystemen geht in Richtung → <i>offener Chipkarten-Betriebssysteme</i> . Typische Chipkarten-Betriebssysteme sind → <i>Multos</i> , → <i>Java Card</i> , → <i>Windows for Smart Cards</i> und → <i>STARCOS</i> .
Chipkarten-Mikrocontroller (<i>smart card microcontroller</i>)	Speziell für die Anforderungen von Chipkarten optimierte → <i>Mikrocontroller</i> . Die Verbesserungen betreffen vor allem Aspekte der Chipsicherheit (z. B. Schutzschichten, Detektoren), Chipgröße und besondere Funktionseinheiten für chipkartenspezifische Anforderungen (z. B. UART für Kommunikation).
Chipmodul (<i>chip modul</i>)	Der Träger und die Halterung für ein Die mit darauf angeordneten Kontaktelementen. Die häufig gebrauchte Kurzform für Chipmodul ist Modul.
Chip-on-Tape (COT)	Beim Chip-on-Tape sind die → <i>Chipmodule</i> auf ein flexibles dünnes Band mit typischerweise 35 mm Breite paarig nebeneinander gesetzt.
CHV	→ <i>PIN</i>
CICC (<i>contactless integrated chip card</i>)	Nach ISO die normgerechte Bezeichnung für eine Karte mit Chip, bei der die Energie- und Datenübertragung berührungslos durch elektromagnetische Felder erfolgt. Es kann sich dabei sowohl um einen Speicherchip als auch einen Mikrocontrollerchip handeln.

¹² Siehe auch Abschnitt 4.11.2 „Gegenseitige symmetrische Authentisierung“.

Class-Datei (<i>classfile</i>)	Die kompilierten, d. h. in Bytecode übersetzten und mit zusätzlichen Informationen versehenen Java-Programme werden in einer so genannten Class-Datei abgespeichert. Nach dem Laden werden sie von der Java Virtual Machine ausgeführt.
Clearing	Funktion der Abrechnung im elektronischen Zahlungsverkehr zwischen dem Akzeptanten einer elektronischen Zahlung (in der Regel ein Händler) und seiner Bank.
Clearingsystem	Rechnergestütztes Hintergrundsystem, das die zentrale Abrechnung im Rahmen einer Anwendung für elektronischen Zahlungsverkehr übernimmt.
Clean Room VM	→ <i>Java Card Virtual Machine</i>
CLIP	Markenname von Europay für technologisch unterschiedliche elektronische Geldbörsensysteme mit Chipkarten.
CMDA 2000 (<i>code division multiple access 2000</i>)	Mobilfunksystem der dritten Generation (→ <i>3G</i>) im 2000 MHz-Frequenzbereich mit ähnlichen Leistungsmerkmalen wie → <i>UMTS</i> . Die vorgesehene Chipkarte für CDMA 2000 Endgeräte ist optional und hat den Namen → <i>R-UIM</i> .
CMM (<i>capability maturity model</i>)	International verwendetes Modell zur Bestimmung des Reifegrades einer Softwareentwicklung. Der Reifegrad wird mit einem standardisierten Fragenkatalog bestimmt und hat 5 Stufen. Reifegrad 1 kennzeichnet eine mehr oder minder nach chaotischen Prinzipien ablaufende Entwicklung, Reifegrad 5 kennzeichnet eine geordnete und sich kontinuierlich selbst verbessernde Entwicklung als höchsten möglichen Reifegrad. ¹³
CODEC (<i>compressor/decompressor</i> oder <i>coder/decoder</i>)	Hardwarechip oder Algorithmus, der entweder für die Kompression/Dekompression oder die Verschlüsselung/Entschlüsselung von Daten bestimmt ist.
Combikarte	Eingetragenes Warenzeichen der Firma ADE, das eine → <i>Dual-Interface-Karte</i> bezeichnet.
Common Criteria (CC) [CC]	Kriterienkatalog zur Entwicklung und → <i>Evaluierung</i> von informationstechnischen Systemen und soll zukünftig nationale und internationale Kriterienkataloge wie → <i>TCSEC</i> und → <i>ITSEC</i> ersetzen. Die Common Criteria wurden 1996 in der Version 1.0 von → <i>NIST</i> veröffentlicht und sind mittlerweile auch als ISO 15408 international genormt. Aktuell gültig ist die Version 2.0 von 1998.
Compiler	Programm, das eine Programmiersprache wie BASIC oder C in von einem Mikroprozessor direkt ausführbare Maschinensprache übersetzt. Nach dem Kompilationsvorgang muss das Programm üblicherweise noch mit einem Linker gebunden (<i>linking</i>) werden.
COS (<i>card operating system</i>)	Übliche Bezeichnung für → <i>Chipkarten-Betriebssysteme</i> . Sie ist auch oft ein Teil des Produktnamens des Betriebssystems (z. B. STARCOS).
CP8	Markenname eines → <i>Multiplication-Chipkarten-Betriebssystems</i> von Bull [Bull], das in verschiedenen Versionen erhältlich ist.
CPU (<i>central processing unit</i>)	→ <i>Mikroprozessor</i>
CRC (<i>cyclic redundancy check</i> – zyklische Redundanzprüfung)	Einfacher und weit verbreiteter Fehlererkennungscode (→ <i>EDC</i>) zur Sicherung von Daten. Vor seiner Anwendung muss der CRC durch einen Startwert und ein Teilerpolynom festgelegt werden.
CT-API (<i>chipcard terminal – application programming interface</i>)	Eine in Deutschland weit verbreitete anwendungsunabhängige Schnittstellen-Spezifikation für die Anbindung von → <i>MKT-Terminals</i> an PCs. Der Herausgeber der Spezifikation ist Teletrust Deutschland.
D-AMPS	→ <i>AMPS</i>
Dateibody (<i>file body</i>)	→ <i>Dateiheader</i>
Dateiheader (<i>file header</i>)	Dateien in Chipkarten sind üblicherweise immer in zwei getrennte Teile aufgespalten. Der Dateiheader genannte Teil enthält Informationen über die → <i>Dateistruktur</i> und die → <i>Zugriffsbedingungen</i> , während in dem mit einem Zeiger

¹³ Siehe auch Abschnitt 15.7 „Vorgehensmodelle“.

	verbundenen Dateibody die veränderbaren Nutzdaten gespeichert sind.
Dateistruktur (<i>file structure</i>)	Der von außerhalb der Chipkarte sichtbare Aufbau eines → <i>EFs</i> . Dateistrukturen dienen der logisch strukturierten und speicherplatzminimierten Ablage von Nutzdaten. Die üblichen Dateistrukturen nach ISO/IEC 7816-4 sind transparent, linear fixed, linear variable und cyclic. ¹⁴
Dateityp (<i>file type</i>)	Kennzeichnet bei Dateiverwaltungen in Chipkarten die Art einer Datei, d. h. ob es sich um eine Verzeichnisdatei (MF, DF) handelt oder um eine Datei für Nutzdaten (EF).
DEA (<i>data encryption algorithm</i>)	anderer Name für → <i>DES</i>
Debitkarte (<i>debit card</i>)	Karte mit oder ohne Chip, die einen Verfügungsrahmen aufweist und bei der die Bezahlung zeitgleich nach Erhalt des Gutes oder der Dienstleistung stattfindet. Dazu ist die Debitkarte mit einem Bankkonto verbunden, so dass unmittelbar bei der Bezahlung der entsprechende Betrag transferiert werden kann. Diese Bezahlung wird oft als „pay now“ bezeichnet. Das typische Beispiel für Debitkarten sind ec-Karten.
Debugging	Fehlersuche und -beseitigung mit dem Zweck, möglichst viele Fehler einer Software zu erkennen und zu korrigieren. Das Debugging wird in der Regel vom Softwareentwickler im Zuge der → <i>Implementierung</i> durchgeführt und ist nicht identisch mit dem Testing (→ <i>Test</i>).
DECT (<i>digital enhanced cordless telecommunications, früher: digital European cordless telecommunications</i>)	Ein von → <i>ETSI</i> herausgegebener Standard für schnurlose Telefone in → <i>Zellulartechnik</i> mit digitaler Datenübertragung im 1,9 GHz-Bereich. Chipkarten sind bei DECT im Mobilteil des Telefons vorgesehen, jedoch nach Spezifikation optional, was dazu führte, dass sie nicht verwendet werden.
Defragmentierung (<i>defragmentation</i>)	Eine Defragmentierung hat die Aufgabe, an unterschiedlicher physikalischer Position im Speicher abgelegte Daten so zu verschieben, dass diese Daten zusammenhängend abgelegt sind. Die wesentlichen Teile einer Defragmentierung müssen atomar ablaufen, da es sonst beim Abbruch des Vorgangs zu Speicherkonsistenzen kommen kann.
Delamination (<i>delamination</i>)	Unerwünschtes Auseinanderlösen von durch Druck und Hitze miteinander verbundenen (d. h. laminierten) Folien. Die Delamination einer Karte kann beispielsweise durch zu großflächige Aufdrucke mit nicht thermoplastischen Druckfarben (typische Farben für Offsetdruck) zwischen Kern- und Deckfolien verursacht werden.
Depersonalisierung (<i>depersonalisation</i>)	Rückgängigmachung der elektrischen → <i>Personalisierung</i> einer Chipkarte. Falls ein → <i>Chipkarten-Betriebssystem</i> eine Depersonalisierung zulässt, kann diese beispielsweise durch ein spezielles → <i>Kommando</i> nach vorheriger Authentisierung ausgeführt werden. Depersonalisierungen werden unter anderem bei falsch personalisierten Chipkarten ausgeführt, um diese wiederverwerten zu können.
DER (<i>distinguished encoding rules</i>)	→ <i>BER</i>
DES (<i>data encryption standard</i>)	Der bekannteste und verbreitetste symmetrische kryptografische Algorithmus (→ <i>Kryptoalgorithmus</i>). Er wurde von IBM zusammen mit dem → <i>NBS</i> entwickelt und 1977 als US-Norm (FIPS 46) als DEA (<i>data encryption algorithm</i>) publiziert. ¹⁵ Offizieller Nachfolger des DES ist der → <i>AES</i> .
Design (<i>design</i>)	Das Design, oft auch Entwurf genannt, im Sinne der Softwareentwicklung ist der Aufbau einer Softwarearchitektur anhand der bei der → <i>Analyse</i> ermittelten Anforderungen. Vereinfacht ausgedrückt, ist das Ergebnis des Designs eine Beschreibung, „wie“ die Anforderungen in der Software umgesetzt werden. Der nächste Schritt bei einer sequentiellen Softwareentwicklung ist die → <i>Implementierung</i> .
deterministisch	Bezeichnet ein Verfahren oder einen Algorithmus, das bzw. der bei identischen Ausgangsbedingungen immer zum gleichen Ergebnis kommt. Das Gegenteil ist → <i>probabilistisch</i> .

¹⁴ Siehe auch Abschnitt 5.6.4 „Dateistrukturen von Efs“.

¹⁵ Siehe auch Abschnitt 4.7.1 „Symmetrische Kryptoalgorithmen“.

DF (<i>dedicated file</i>)	Verzeichnis im Dateisystem einer Chipkarte. Ein Sonderfall eines DFs ist das Root-Verzeichnis MF.
DF Name	Neben dem FID (<i>file identifier</i>) ein weiteres Merkmal für ein DF, mit einer Länge zwischen 1 und 16 Byte. Er wird zur Selektion des DFs benutzt und kann einen registrierten 5 bis 16 Byte langen AID (<i>application identifier</i>) enthalten, der das DF weltweit eindeutig macht. ¹⁶
Die, Dice	Siliziumkristall in Form eines Plättchens, auf dem sich ein einzelner halbleitertechnisch aufgebaute elektronischer Schaltkreis (z. B. Mikrocontroller) befindet.
Diensteanbieter (<i>service provider</i>)	Instanz, welche gegen Bezahlung einen Dienst (z. B. Verkauf von Gütern oder Dienstleistungen) anbietet.
differentielle Fehleranalyse (DFA) (<i>differential fault analysis</i>)	Das Prinzip der differentiellen Fehleranalyse wurde 1996 von Dan Boneh, Richard A. DeMillo und Richard J. Lipton, die alle drei bei Bellcore angestellt waren, veröffentlicht [Boneh 96]. Das Verfahren basiert darauf, durch die bewusste Einstreuung von Fehlern während der kryptografischen Berechnung den geheimen Schlüssel zu ermitteln. Im ursprünglichem Verfahren wurden nur Public-Key-Algorithmen genannt. Diese Angriffsmethode wurde jedoch innerhalb einiger Monate sehr schnell weiterentwickelt [Anderson 96a], sodass mit der differentiellen Fehleranalyse prinzipiell alle Kryptoalgorithmen angegriffen werden können, sofern sie keine besonderen Schutzmaßnahmen aufweisen.
differentielle Kryptoanalyse (<i>differential crypto analysis</i>)	Hier werden Klartext-Paare mit bestimmten Unterschieden und gleichem Schlüssel benutzt, um durch die Analyse der Entwicklung dieser Unterschiede über die einzelnen DES-Runden hinweg den geheimen Schlüssel zu errechnen. Diese Analysemethode wurde von Eli Biham und Adi Shamir 1990 veröffentlicht.
digital	Bezeichnet Systeme, bei denen ein Signal nur eine begrenzte Anzahl von Werten annehmen kann.
digitale Signatur (<i>digital signature</i>)	Digitale Signaturen werden zur Feststellung der Authentizität von elektronischen Nachrichten oder Dokumenten verwendet. Digitale Signaturen beruhen in der Regel auf asymmetrischen Kryptoalgorithmen, wie beispielsweise dem RSA-Algorithmus. Die Rechtswirksamkeit einer digitalen Signatur wird in vielen Ländern durch Gesetz geregelt. In Deutschland beispielsweise durch das → <i>Signaturgesetz</i> . Digitale Signaturen werden manchmal auch elektronische Unterschriften genannt.
digitaler Fingerabdruck (<i>digital fingerprint</i>)	Häufige Bezeichnung für den Hash-Wert einer Nachricht (z. B. mit SHA-1 erstellt).
digitales Wasserzeichen (<i>digital watermark</i>)	Eine idealerweise unsichtbare bzw. unhörbare, nicht rückgängig zu machende Markierung in Bild- oder Tondateien zur Realisierung von Urheberschutz. Bei Bedarf können dann mit Analyseprogrammen entsprechende Bild- oder Tondateien auf ein digitales Wasserzeichen überprüft werden. Zur Erzeugung von digitalen Wasserzeichen werden oftmals Verfahren der → <i>Steganografie</i> benutzt.
Downlink	Verbindung von einem übergeordneten System (z. B. Basisstation) zu einem untergeordneten System (z. B. Mobiltelefon). Das Gegenteil ist der → <i>Uplink</i> .
Download	Übertragen von Daten von einem übergeordneten System (z. B. Hintergrundsystem, Host) an ein untergeordnetes System (z. B. Terminal). Das Gegenteil ist der → <i>Upload</i> .
DPA (<i>differential power analysis</i>)	Die differentielle Leistungsanalyse ist eine Angriffsmethode auf → <i>Chipkarten</i> und stellt eine Verbesserung der einfachen Leistungsanalyse (→ <i>SPA</i>) dar. Dabei wird wiederholt mit hoher zeitlicher Auflösung der Stromverbrauch eines Mikrocontrollers für eine bestimmte Operation mit bekannten Daten gemessen und durch Mittelwertbildung das Rauschen eliminiert. Dann wird der Stromverbrauch mit unbekanntem Daten gemessen und anschließend durch Differenzbildung der Messwerte der bekannten und der unbekanntem Daten auf die unbekanntem Daten geschlossen. Bekannt wurde die DPA durch eine Veröffentlichung von Paul Kocher, Joshua Jaffe und Benjamin Jun im Juni 1998 [Kocher 98]. ¹⁷
DRAM (<i>dynamic random access memory</i>)	RAM-Speicher in dynamischer Bauweise; benötigt zum Erhalt des Speicherinhalts eine konstante Stromversorgung sowie eine zyklische Wiederauffrischung des Inhalts. DRAM-Speicher sind aus Kondensatoren aufgebaut. Sie be-

¹⁶ Siehe auch Abschnitt 16.7 „Registrierungsstellen für RID“.

¹⁷ Siehe auch Abschnitt 8.2.4.1 „Angriffe auf der physikalischen Ebene“.

	nötigen weniger Platz auf dem Chip als SRAM-Speicher und sind deshalb billiger. Allerdings ist die Zugriffszeit auf SRAMs geringer.
Dual-Band-Mobiltelefon (<i>dual band mobile</i>)	Ein Dual-Band-Mobiltelefon kann in zwei Frequenzbändern (z. B. 900 MHz und 1800 MHz) arbeiten.
Dual-Interface-Karte (<i>dual interface card</i>)	Bezeichnung für eine → <i>Chipkarte</i> mit kontaktbehafteter und kontaktloser Schnittstelle für die Datenübertragung von und zur Chipkarte.
Dual-Mode-Mobiltelefon (<i>dual mode mobile</i>)	Mobiltelefon, das in zwei verschiedenen Mobilfunksystemen (z. B. GSM und AMPS) arbeiten kann.
Dual-Slot-Handy (<i>dual slot mobile</i>)	Bezeichnung für ein Mobiltelefon, das neben der Benutzerkarte (z. B. SIM) noch eine von außen zugängliche Kartenkontaktiereinheit für üblicherweise ID-1-Chipkarten (→ <i>Chipkarte</i>) besitzt. Mit Dual Slot Handys lassen sich beispielsweise Zahlungen über das Mobilfunknetz mit bestehenden elektronischen Geldbörsen auf Chipkarten abwickeln.
Dual-Slot-Lösung (<i>dual slot solution</i>)	Chipkarten-Anwendung, die auf der Nutzung der zweiten Kartenkontaktiereinheit eines Dual-Slot-Handies beruht.
duplizieren	Das Übertragen von echten Daten auf eine zweite Karte zum Zwecke der Herstellung einer oder mehrerer identischer (d. h. geklonter) Karten. Der Begriff ist in der Regel identisch mit → „klonen“.
Dynamic STK (<i>dynamic SIM application toolkit</i>)	Veralteter Ausdruck für Microbrowser-Lösungen (→ <i>Browser</i>) nach der → <i>SIM Alliance</i> Spezifikation.
ECBS (European Committee for Banking Standards) [ECBS]	Eine im Jahr 1992 gegründete europäische Organisation zur Entwicklung technischer Lösungen und Standards für eine europaweite → <i>interoperable</i> Infrastruktur für Zahlungsverkehrssysteme.
ECC (<i>elliptic curve cryptosystem</i>)	Die Bezeichnung für Kryptosysteme (d. h. in der Regel Kryptoalgorithmen) auf der Grundlage von elliptischen Kurven.
ECC (<i>error correction code</i>)	Prüfsumme über Daten. Mit einem ECC können Fehler in den Daten mit einer bestimmten Wahrscheinlichkeit erkannt und ggf. auch fehlerfrei korrigiert werden.
E-Commerce (<i>Electronic Commerce</i> , elektronischer Geschäftsverkehr)	Unter diesem Begriff versteht man alle Formen von Dienstleistung, Handel und dazugehörigem Zahlungsverkehr in offenen Netzen, d. h. vor allem im Internet. Werden bei E-Commerce mobile Endgeräte verwendet so spricht man von → <i>M-Commerce</i> .
EDC (<i>error detection code</i>)	Prüfsumme über Daten. Mit einem EDC können Fehler in den Daten mit einer bestimmten Wahrscheinlichkeit erkannt werden. Ein typisches Beispiel für einen EDC ist die XOR- oder CRC-Prüfsumme bei verschiedenen Datenübertragungsprotokollen.
EDGE (<i>enhanced data rates for GSM and TDMA evolution</i>)	EDGE ist als letzte Evolutionsstufe für GSM-Netzwerke vorgesehen. Unter Beibehaltung der existierenden Netzinfrastruktur können durch ein anderes Modulationsverfahren auf der Luftschnittstelle GSM-Mobiltelefone nach EDGE-Standard mit einer Datenübertragungsrate von bis zu 384 kBit/s an Basisstationen angebunden werden.
EEPROM (<i>electrical erasable read only memory</i>)	Eine nichtflüchtige Speicherart, die in → <i>Chipkarten</i> Verwendung findet. EEPROMs sind in Speicherseiten, Pages genannt, aufgeteilt. Die Seitengröße wird auch als → <i>Granularität</i> bezeichnet. Der Inhalt der Speicherseiten kann verändert und als Ganzes gelöscht werden, wobei es aber eine physikalisch bedingte Obergrenze der Anzahl der schreibenden bzw. löschenden Zugriffe gibt. ¹⁸ Der Schreibvorgang bei EEPROM-Zellen findet durch den Fowler-Nordheim-Effekt statt und nicht durch Hot-Electron-Injection wie bei → <i>Flash-EEPROM</i> . EEPROM-Zellen haben eine typische Schreibzeit von 3 ms pro Speicherseite.
EF (<i>elementary file</i>)	Die eigentlichen Datenspeicher im Dateibaum einer Chipkarte. Sie können entweder die Eigenschaft „working“ (d. h. für den Gebrauch durch das Terminal) oder „internal“ (d. h. für den Gebrauch durch das Betriebssystem der Chipkarte) haben und besitzen eine interne Struktur (transparent, linear fixed, linear variable, cyclic, ...). ¹⁹

¹⁸ Siehe auch Abschnitt 3.4.2 „Speicherarten“.

¹⁹ Siehe auch Abschnitt 5.6.4 „Dateistrukturen von Efs“.

Einlagenkarte (<i>mono layer card</i>)	Karte, die sich aus einer einzigen Schicht Kunststoffolie zusammensetzt (→ <i>Mehrlagenkarte</i>).
Einwegfunktion (<i>one-way function</i>)	Mathematische Funktion, die sich einfach berechnen lässt, deren Umkehrfunktion aber einen sehr großen Rechenaufwand erfordert.
elektronische Geldbörse (<i>electronic purse, e-purse</i>)	Karte mit Chip, die vor der Bezahlung mit einem Geldbetrag aufgeladen werden muss. Diese Bezahlung wird oft als „pay before“ bezeichnet. Die typischen Beispiele für elektronische Geldbörsen sind die deutsche Geldkarte, die österreichische Quick Börse, Visa Cash, Proton oder Mondex. Elektronische Geldbörsen können die Eigenschaft von Purse-to-Purse-Transaktionen (siehe auch Purse-to-Purse-Transaktion) haben. ²⁰
elektronischer Scheck (<i>electronic cheque</i>)	Variante einer → <i>elektronischen Geldbörse</i> , die mit festen und nicht stückelbaren Beträgen arbeitet. Diese Bezahlung wird oft als „pay before“ bezeichnet. ²¹
Embossing (<i>embossing</i>)	→ <i>Hochprägung</i>
Emulator (<i>emulator</i>)	Gerät (d. h. eine Hardware), das die Funktionsweise eines anderen Gerätes (des Zielsystems) nachahmt. Die Nachahmung mittels Software bezeichnet man hingegen als → <i>Simulator</i> . Emulatoren werden oft zur Entwicklung von Software für noch nicht existierende Zielsysteme eingesetzt. Ein Chipkarten-Emulator ist somit eine Hardwareschaltung, die eine echte Chipkarte auf elektrischer und logischer Ebene vollständig nachbildet. Aufgrund der Realisierung eines Großteils der Funktionalität in Hardware sind Emulatoren in der Regel schneller, d. h. echtzeitnäher, als Simulatoren.
EMV (Europay, Mastercard, Visa) [EMV]	Eine gemeinsame Spezifikation für Zahlungsverkehrskarten mit Chip sowie dazugehörige Terminals der Firmen Europay, Master Card, Visa und American Express. Diese Spezifikationen sind zum weltweiten Industriestandard für Kredit, Debit- und Börsenkarten avanciert und somit das Pendant des Zahlungsverkehrs zur Telekommunikationsnorm GSM 11.11.
EMV-Spezifikation	→ <i>EMV</i>
Ende-zu-Ende-Verbindung (<i>end-to-end-connection</i>)	Die direkte Kommunikation zweier Instanzen unter Zuhilfenahme von Kommunikationspfaden einer oder mehrerer weiterer Instanzen, die jedoch den Informationsgehalt des eigentlichen Datenaustausches nicht verändern. Ist die Kommunikation der zwei Ursprungsinstanzen kryptografisch gesichert, so spricht man von → <i>tunneling</i> . Ein typisches Beispiel für eine Ende-zu-Ende-Verbindung ist die direkte Kommunikation eines Anwendungsanbieters mit einer SIM nach GSM 03.48.
Endianness	Gibt die Reihenfolge der Bytes innerhalb eines Bytestrings an. Big Endian besagt, dass sich das höherwertigste Byte am Anfang und folglich das niederwertigste am Schluss der Kette von Bytes befindet. Bei little Endian ist die Reihenfolge umgedreht, d. h. das niedrigstwertige Byte ist am Anfang und das höchstwertige am Schluss.
enrollment	Prozess der ursprünglichen Aufnahme der biometrischen Daten eines → <i>Chipkartenbenutzers</i> und die Einbringung in die entsprechende Chipkarte. Die beim enrollment in der Chipkarte gespeicherten Daten sind dann im Folgenden die Basis für die weiteren biometrischen Benutzeridentifizierungen.
EP SCP	→ <i>SMG9</i>
EPROM (<i>erasable read only memory</i>)	Nichtflüchtige Speicherart, die früher in Chipkarten Verwendung fand und vollständig durch die → <i>EEPROM</i> -Technologie abgelöst ist. Ein EPROM kann nur durch UV-Licht gelöscht werden, weshalb es im Chipkartenbereich nur als WORM-Speicher (<i>write once, read multiple</i>) verwendet werden kann. ²²
ETS (<i>European telecommunication standard</i>)	Bezeichnung der von → <i>ETSI</i> herausgegebenen Normen, die sich in erster Linie mit europäischer Telekommunikation beschäftigen.
ETSI (<i>European telecommunications standards institute</i>) [ETSI]	Normungsinstitut der europäischen Telekommunikationsgesellschaften mit Sitz in Sophia Antipolis, Frankreich; es beschäftigt sich mit der Normung im Bereich der europäischen Telekommunikation. Die im Chipkartenbereich wichtigsten ETSI-Normen sind die Normenreihe für GSM (z. B. GSM 11.11 für die SIM) und für UMTS (z. B. TS 31.102 für die USIM-Anwendung). Die Expertentref-

²⁰ Siehe auch Abschnitt 12.1.2 „Elektronisches Geld“.

²¹ Siehe auch Abschnitt 12.1.2 „Elektronisches Geld“.

²² Siehe auch Abschnitt 3.4.2 „Speicherarten“.

	fen der ETSI-Normungsgruppen finden in der Regel an den unterschiedlichsten (sehenswerten) Orten in Europa oder, je nach Gastgeber, weltweit statt, weshalb manche Menschen der festen Überzeugung sind, dass die Abkürzung ETSI eigentlich für <i>European travel and sightseeing institute</i> steht.
etu (<i>elementary time unit</i>)	Die Dauer eines Bits bei der Datenübertragung zu Chipkarten. Die absolute Zeitdauer für ein etu ist nicht festgelegt, sondern in Abhängigkeit vom an die Chipkarte angelegten Takt und des Clock Rate Conversion Factors definiert.
Eurosmart [Eurosmart]	Die 1994 gegründete Interessenvertretung der europäischen Chipkartenhersteller mit Sitz in Brüssel. Die Aufgaben von Eurosmart sind die Förderung und Standardisierung (→ <i>Standard</i>) von → <i>Chipkarten</i> und Chipkarten-Systemen, die Bildung eines Forums für den Austausch von Marktdaten und technischen Daten sowie die Etablierung von Verbindungen zu nationalen und internationalen Standardisierungsgremien.
Evaluierung (<i>evaluation</i>)	Die unparteiliche, objektive, wiederholbare und reproduzierbare Bewertung von informationstechnischen Systemen (d.h. Hardware und/oder Software) durch eine vertrauenswürdige Instanz gemäß den Vorgaben eines Kriterienkatalogs. Das zu evaluierende informationstechnische System wird → <i>Target of Evaluation</i> genannt. International gebräuchliche Kriterienkataloge zur Evaluierung von → <i>Chipkarten</i> und Chipkartensystemen sind → <i>ITSEC</i> und <i>Common Criteria</i> (→ <i>CC</i>).
f1, f2, f3, f4, f5 (<i>function 1 ... 5</i>)	Bezeichnungen für kryptografische Funktionen bei → <i>UMTS</i> zur Authentisierung von Netzwerk und → <i>USIM</i> als auch zum Aufbau einer kryptografisch gesicherten Datenübertragung auf der Luftschnittstelle. Der Kern dieser <i>Security Functions</i> ist ein symmetrischer → <i>Kryptoalgorithmus</i> , der mit zusätzlich verknüpften Eingangswerten parametrisiert werden kann. Als Beispielalgorithmus ist seitens der USIM-Spezifikation für f1 bis f5 der MILENAGE-Algorithmus vorgeschlagen, der in seinem Kern auf dem → <i>AES</i> basiert.
Fab (<i>fab</i>)	Halbleiterproduktionsstätte.
face	Das <i>face</i> eines Halbleiters ist diejenige Seite des Chips, auf der sich die halbleitertechnisch erzeugten Funktionsstrukturen befinden. So bedeutet beispielsweise eine Face-to-face-Kontaktierung, dass zwei Chips in ihren Funktionsstrukturen so zusammengelegt werden, dass die Chips elektrisch miteinander verbunden sind.
Falltür (<i>trap door</i>)	Ein vorsätzlich angelegter Mechanismus in einer Software oder in einem Algorithmus, mit dem Sicherheitsfunktionen oder Schutzmechanismen umgangen werden können.
FAT (<i>file allocation table</i>)	Dateizuordnungstabelle, die eine spezielle Methode zur Dateiverwaltung bezeichnet. Dabei wird der zu verwaltende Speicher in Speicherabschnitte (so genannte Cluster) aufgeteilt und Informationen über die Belegung und die Adressen dieser Speicherabschnitte in der FAT verwaltet.
fault tree analysis	Beim Testen jene Methode, bei der zur Fehlersuche jeder mögliche Programmablauf im Programmcode durchlaufen wird.
FD/CDMA (<i>frequency division/code division multiple access</i>)	→ <i>CDMA</i>
FDMA (<i>frequency division multiple access</i> – Frequenzvielfachzugriff)	Ein → <i>Vielfachzugriffsverfahren</i> zur parallelen Datenübertragung von mehreren Sendern zu einem Empfänger auf verschiedenen Frequenzbändern. Dazu erhält jeder Sender aus dem ganzen zur Verfügung stehenden Frequenzbereich ein Frequenzband, auf dem er exklusiv senden darf. FDMA wird bei vielen Mobiltelefonanwendungen auf der Luftschnittstelle zwischen Mobiltelefon und Basisstation benutzt, wie beispielsweise im deutschen C-Netz. ²³
Fehlbedienungszähler (<i>error counter</i>)	Zähler, der Schlechtfälle erfasst und von dem es abhängt, ob ein bestimmtes Geheimnis (PIN oder Schlüssel) weiterhin benutzt werden kann. Erreicht der Fehlbedienungszähler den Maximalwert, so ist das Geheimnis gesperrt und kann nicht mehr verwendet werden. Der Fehlbedienungszähler wird üblicherweise auf null zurückgesetzt, wenn die Aktion erfolgreich verlaufen ist (d. h. im Gutfall).
FIB (<i>focused ion beam</i>)	Gerät zur Erzeugung eines gebündelten Ionenstrahls zum Abtragen oder Aufbauen von Material auf Halbleitern.

²³ Siehe auch Abschnitt 13.1.1 „Vielfachzugriffsverfahren“.

FID (<i>file identifier</i>)	Ein zwei Byte großes Merkmal für eine Datei, das zur Selektion dieser Datei benutzt werden kann. Sowohl MF als auch DF und EF besitzen einen FID. Der FID des MFs ist immer '3F00'. ²⁴
FIPS (<i>Federal Information Processing Standard</i>)	Die von → NIST herausgegebenen US-amerikanischen Normen.
Firewall	Instanz (Hardware und/oder Software), die eine sicherheitstechnische Trennung zwischen bestimmten → <i>Anwendungen</i> oder Instanzen realisiert. Eine Firewall kann beispielsweise zwei Anwendungen auf einer Chipkarte in einer Art und Weise separieren, dass diese nicht über die Firewall hinweg unberechtigterweise auf Daten zugreifen können. Die deutsche Übersetzung Brandschutzmauer, welche sich zwischen zusammenhängenden Gebäuden befindet, beschreibt plastisch den Zweck und die Funktionsweise einer Firewall.
Flash	Gebräuchliche Kurzform für einen → <i>Flash-EEPROM</i> -Speicher.
Flash-EEPROM (<i>flash electrical erasable read only memory</i>)	Nichtflüchtige Speicherart, die in Chipkarten in Zukunft Verwendung finden wird. Ein Flash-EEPROM ähnelt in Funktionalität und halbleitertechnischem Aufbau dem → <i>EEPROM</i> , doch findet bei Flash-EEPROM-Zellen der Schreibvorgang durch eine so genannte Hot-Electron-Injection statt und nicht durch den Fowler-Nordheim-Effekt wie beim EEPROM. Bei der Hot-Electron-Injection werden durch eine hohe Potenzialdifferenz zwischen Source und Drain schnelle Elektronen erzeugt, von denen ein Teil die Tunnel-Oxidschicht durchdringt und im Floating Gate gespeichert wird. Dieser Effekt reduziert die Schreibzeit auf ca. 10 µs. Flash-EEPROMs eignen sich aufgrund ihrer großen Speicherseiten (z. Zt. typisch 128 Byte) sehr gut als Ersatz für maskenprogrammiertes → <i>ROM</i> . ²⁵
Floorlimit	Das Floorlimit gibt an, ob eine Zahlung von einer dritten Instanz autorisiert (→ <i>Autorisierung</i>) werden muss. Unterhalb dieser Grenze ist eine Autorisierung nicht notwendig, oberhalb dieser Grenze muss eine Autorisierung vorgenommen werden, da sonst die Zahlung nicht möglich oder garantiert ist.
flüchtiger Speicher (<i>volatile memory</i>)	Speicherart (z. B. RAM), die ihren Inhalt nur bei dauernder Stromzufuhr behält.
Footprint	exakter: Memory Footprint, bezeichnet die Aufteilung eines Speichers für bestimmte Zwecke.
Foundry	Halbleiterproduktionsstätte, die auf Vertragsbasis von Dritten entwickelte Halbleiter herstellt.
FPLMTS (<i>future public land mobile telecommunication service</i>)	→ <i>IMT-2000</i>
FRAM (<i>ferroelectric read access memory</i>)	Nichtflüchtige Speicherart, die in → <i>Chipkarten</i> sehr selten Verwendung findet. FRAMs sind in Speicherseiten, so genannte Pages, aufgeteilt. Die Seitengröße wird auch als → <i>Granularität</i> bezeichnet. Für diese Speicherart benutzt man zur Speicherung von Informationen die Eigenschaften von ferroelektrischen Substanzen, die zwischen Control Gate und Floating Gate eingebracht werden. FRAM-Zellen haben eine typische Schreibzeit von 100 ns pro Speicherseite und benötigen keine spezielle Löschspannung. Allerdings ist bei FRAM-Speicher die Anzahl der Lesezyklen limitiert, und die Herstellung beinhaltet schwer beherrschbare Prozessschritte, weshalb diese Speichertechnologie bei Chipkarten-Mikrocontrollern bisher wenig Anwendung findet.
Frame	Folge von Datenbits und optional Fehlererkennungsbits mit Rahmenbegrenzungen am Anfang und Ende. Frames für die kontaktlose Datenübertragung bei Chipkarten sind in ISO/IEC 14443 definiert.
Garbage Collection	Sammelt den von einer → <i>Anwendung</i> nicht mehr benutzten Speicher und stellt ihn wieder als Freispeicher zur Verfügung. Die Garbage Collection wurde früher mittels Interrupt zum normalen Programmablauf realisiert. In modernen Computersystemen ist die Garbage Collection ein Thread niedriger Priorität, welcher ständig den Speicher auf nicht mehr benötigte Bereiche durchsucht und ihn dann wieder freigibt.
Geldkarte	Markenname der seit 1996 in Deutschland eingeführten elektronischen Geldbörse. Die Geldkarte ist sowohl die Bezeichnung für die Anwendung auf einer → <i>Multiapplication-Chipkarte</i> als auch für Chipkarte an sich. Das Chipkarten-

²⁴ Siehe auch Abschnitt 5.6 „Dateien in der Chipkarte“.

²⁵ Siehe auch Abschnitt 3.4.2 „Speicherarten“.

	Betriebssystem für die Geldkarte bzw. für die Debit-Funktionalität ist → <i>SEC-COS (security card operating system)</i> .
geschlossene Anwendung (<i>closed application</i>)	Eine → <i>Anwendung</i> auf einer Chipkarte, die nur dem Anwendungsbetreiber zur Verfügung steht und nicht allgemein verwendet werden kann.
geschlossene Börse (<i>closed purse</i>)	Realisation einer geschlossenen → <i>Anwendung</i> für eine elektronische Geldbörse. Sie kann nur in dem vom Anwendungsbetreiber freigegebenen Rahmen und nicht für allgemeine Zahlungstransaktionen verwendet werden.
Glitch	Sehr kurzer Spannungseinbruch oder eine sehr kurze Spannungserhöhung.
Global Platform [Global Platform]	Ein im Jahr 1999 gegründetes, international agierendes Gremium verschiedener Chipkartenfirmen zur Standardisierung von Technologien für → <i>Multiapplication-Chipkarten</i> . Die wichtigste von Global Platform herausgegebene Spezifikation ist die Open Platform (→ <i>OP</i>)-Spezifikation.
GPRS (<i>general packet radio system</i>)	Eine von → <i>ETSI</i> standardisierte Erweiterung von → <i>GSM</i> , um höhere Übertragungsraten für Daten bei mobilen Endgeräten zu realisieren. GPRS bietet eine → <i>paketorientierte</i> Verbindung mit einer Datenübertragungsrate bis zu 115,2 kBit/s durch Bündelung der 8 vorhandenen Zeitschlitze zu je 14400 Bit/s. Ein Mobiltelefon mit GPRS-Technologie ist hinsichtlich der Datenübertragung ständig im Netz eingebucht und damit zu jedem Zeitpunkt für Datenübertragungen verfügbar. Die Datenübertragungsrate wird dem aktuell notwendigen Kapazitätsbedarf dynamisch angepasst, so dass immer nur die aktuell benötigte Kapazität belegt wird. Aus diesem Grund eignet sich GPRS auch sehr gut für diskontinuierliche Datenübertragungen.
Granularität (<i>granularity</i>)	Bei → <i>EEPROM</i> -Speichern ein häufig benutzter alternativer Ausdruck für die Pagegröße. Beispielsweise hat ein EEPROM mit der Granularität 32 die Pagegröße von 32 Byte.
Greylist (<i>greylist</i>)	Liste in einer Datenbank, auf der alle → <i>Chipkarten</i> oder Geräte vermerkt sind, die unter Beobachtung stehen (→ <i>Sperrliste, Hotlist, Whitelist</i>).
Greybox Test (<i>greybox test</i>)	Mischform zwischen Whitebox Test und Blackbox Test. Die testende Instanz kennt dabei teilweise die internen Abläufe, Funktionen und Mechanismen der zu prüfenden Software.
GSM (<i>global system for mobile communications</i>)	Digitales, zellulares, betreiberübergreifendes, länderübergreifendes und bodengebundenes Mobilfunksystem der zweiten Generation (→ <i>2G</i>). Die für dieses Mobilfunksystem zugewiesenen Frequenzbereiche sind bei 900 MHz (GSM 900), 1800 MHz (GSM 1800) und 1900 MHz (GSM 1900). Das GSM-System ist durch eine Reihe von Spezifikationen definiert, deren Herausgeber → <i>ETSI</i> ist. Der Zusammenschluss der wesentlichen Netzbetreiber und Hersteller bei GSM ist die → <i>GSM Association</i> . Ursprünglich war GSM nur für einige Länder in Zentraleuropa als Nachfolger der länderspezifischen analogen Mobilfunksysteme geplant. GSM hat sich jedoch zu dem Weltstandard für Mobilfunk entwickelt. Die niedrigen Datenübertragungsraten im GSM-System von 9600 Bit/s bzw. 14400 Bit/s haben die Notwendigkeit der Verbesserung des Systems zu Tage gefördert. Der Evolutionspfad des GSM-Systems hinsichtlich Übertragungskapazität sieht deshalb als nächste Entwicklungsstufen das verbindungsorientierte → <i>HSCSD</i> und das paketorientierte → <i>GPRS</i> vor. Anschließend kann die Datenübertragungsrate bei GSM mit → <i>EDGE</i> nochmals erhöht werden. Der designierte Nachfolger von GSM wird → <i>UMTS</i> sein. ²⁶
GSM Association [GSM Association]	Weltweit agierendes Gremium mit Sitz in Dublin und London zur Abstimmung von Mobilfunksystemen. Es wurde 1987 in Kopenhagen gegründet und ist verantwortlich für die Entwicklung und den Einsatz der → <i>GSM-Normen</i> . Die GSM Association repräsentiert über 500 Netzbetreiber, Hersteller und Zulieferer der GSM-Industrie.
Guillochen	Die meist runden oder ovalen geschlossenen und miteinander verwobenen Linienfelder, die sich auch auf vielen verschiedenen Geldscheinen oder Aktien befinden. Diese Muster lassen sich aufgrund ihrer feinen Struktur hochqualitativ nur auf drucktechnischem Wege erzeugen und sind deshalb nur schwer kopierbar.
Gutfall (<i>good case</i>)	Bei einer logischen Entscheidung der Fall, der zum günstigeren oder beabsichtigten Ergebnis führt.
HAL (<i>hardware abstraction layer</i>)	Zwischenschicht in einem Betriebssystem zur Verbergung aller Hardware-spezifika der Zielplattform vor dem Rest des Betriebssystems. Ziel ist es, eine Portierung des Betriebssystems stark zu vereinfachen, indem beim Wechsel der Hardwareplattform lediglich Anpassungen innerhalb des HAL notwendig sind. ²⁷

²⁶ Siehe auch Abschnitt 13.3 „Das UMTS-System“.

²⁷ Siehe auch Abschnitt 5.2 „Grundlagen“.

Halbbyte (<i>half byte</i>)	→ <i>Nibble</i>
halbduplex (<i>half duplex</i>)	Datenübertragung, bei der miteinander kommunizierende Geräte zu einem Zeitpunkt entweder senden oder empfangen können. Das gleichzeitige Senden und Empfangen von Daten ist mit einer Halbduplex-Verbindung nicht möglich, dazu wird eine Vollduplex-Verbindung benötigt (→ <i>vollduplex</i>).
Händlerkarte (<i>merchant card</i>)	→ <i>Chipkarte</i> , die sich bei einem elektronischen Zahlungsverkehrssystem im Terminal des Händlers als Sicherheitsmodul befindet.
handover	Bezeichnet bei Mobilfunknetzen die unterbrechungsfreie Weitergabe eines Mobiltelefons von einer Zelle zur nächsten. Bei GSM wird ein handover immer vom Netz initiiert.
Happy-Day-Szenario (<i>happy day szenario</i>)	anderer Ausdruck für → <i>Gutfall</i>
Hardmaske (<i>hard mask</i>)	Dieser Begriff bedeutet, dass sich der gesamte → <i>Programcode</i> weitgehend im ROM befindet (→ <i>ROM-Maske</i>). Dies spart gegenüber einer Softmaske Platz, da ROM-Zellen wesentlich kleiner als EEPROM-Zellen sind. Dies hat aber den Nachteil, dass die volle Zeitspanne einer kundenindividuellen Halbleiterproduktion anfällt. Die Durchlaufzeit bei einer Hardmaske ist aus diesem Grund erheblich größer als bei einer Softmaske. Hardmasken werden üblicherweise für große Stückzahlen bei weitgehend einheitlicher Funktionalität der Chipkarten verwendet. Das Gegenteil einer Hardmaske ist die → <i>Softmaske</i> , bei der wesentliche Funktionen im EEPROM sind.
Hash-Funktion	Verfahren zur Komprimierung von Daten mittels einer Einwegfunktion, sodass die ursprünglichen Daten nicht rückrechenbar sind. Die Hash-Funktion liefert für einen Eingabewert beliebiger Länge einen Ausgabewert fester Länge und ist so beschaffen, dass eine Änderung der Eingangsdaten mit sehr hoher Wahrscheinlichkeit Auswirkungen auf den berechneten Hash-Wert (d. h. den Ausgabewert) hat. Ein typischer Vertreter der Hash-Algorithmen ist der SHA-1. Das Ergebnis einer Hash-Funktion ist der Hash-Wert, der oft auch als digitaler Fingerabdruck bezeichnet wird. ²⁸
HBCI (<i>home banking computer interface</i>)	Ein von der deutschen Kreditwirtschaft festgelegter Standard zur Realisierung von Homebanking in Deutschland unter optionaler Zuhilfenahme von Chipkarten.
Heimatnetz (<i>home net</i>)	Im Mobilfunkbereich jenes Mobilfunknetz, bei dessen Betreiber der Teilnehmer Kunde ist.
Hintergrundsystem (<i>background system</i>)	Hintergrundsysteme sind alle Computersysteme, die die Verarbeitung und Verwaltung von Daten ab der Hierarchie der Terminals übernehmen.
Hochprägung (<i>embossing</i>)	Teil der physikalischen Personalisierung, bei der Zeichen in einen Kartenkörper aus Kunststoff in einer solchen Weise geprägt werden, dass sie erhaben sind. Die Hochprägung wird in der Fachsprache auch Embossing genannt.
Hologramm	Fotografische Aufnahme bei der Holographie. Sie ist ein dreidimensionales Bild des fotografierten Objekts. Je nach Betrachtungswinkel des Beobachters wird das Objekt auf dem Hologramm auch unter verschiedenen Winkeln gesehen. Die bei Karten üblicherweise verwendeten Hologramme sind Prägehologramme, bei denen auch bei alltäglichen Lichtverhältnissen ein halbwegs passables dreidimensionales Bild sichtbar ist.
Homezone	Bei Mobilfunknetzen die Bezeichnung für einen standortbezogenen Dienst (→ <i>Location Based Service</i>), bei dem in einem bestimmten Gebiet (üblicherweise der Nahbereich um die eigene Wohnung) die Gesprächsgebühren zu einem deutlich niedrigeren Tarif (i. d. R. Festnetztarif) abgerechnet werden. Ein Festnetzanschluss für Sprachverbindungen kann dadurch überflüssig werden.
horizontaler Prototyp	→ <i>Prototyp</i>
Hotlist	Liste in einer Datenbank, auf der alle → <i>Chipkarten</i> oder Geräte vermerkt sind, die wahrscheinlich manipuliert sind und keinesfalls akzeptiert werden dürfen (→ <i>Sperrliste, Redlist, Greylist, Whitelist</i>).
HSCSD (<i>high speed circuit switched data</i>)	Die verbindungsorientierte HSCSD-Technologie ist eine Ergänzung zum GSM-Standard, um durch zusätzliche Nutzung vorhandener Zeitslots auf der Luftschnittstelle durch Kanalbündelung eine theoretische Erhöhung der Datenübertragungsrate von bis zu $8 \cdot 9600 \text{ bit/s}$ (76800 bit/s) (Uplink und Downlink) zu erreichen. Bestehende GSM-Netze lassen sich mit relativ geringem Aufwand durch Erweiterungen in den Basisstationen sowie spezielle Mobiltelefone auf HSCSD erweitern. Der Nachteil ist jedoch, dass der Bedarf an Übertragungskanälen maximal bis auf das 8-fache steigt.

²⁸ Siehe auch Abschnitt 4.9 „Hash-Funktionen“.

HSM (<i>hardware security module</i> oder <i>host security module</i>)	→ <i>Sicherheitsmodul</i>
HTML (<i>hypertext markup language</i>)	Auf XML aufbauende logische Auszeichnungssprache für Hypertext-Dokumente im WWW (→ <i>WML</i> , <i>WWW</i> , <i>XML</i> , <i>Hypertext</i>).
Hybridkarte	Karte mit zwei unterschiedlichen Kartentechnologien. Typische Beispiele sind eine Karte mit Magnetstreifen und zusätzlichem Chip oder eine → <i>Chipkarte</i> mit optischem Speicher an der Kartenoberfläche.
Hypertext (<i>hypertext</i>)	Hypertext besitzt gegenüber normalem Text zusätzliche Querverweise (Hyperlinks) zu weiteren Stellen im Text oder anderen Dokumenten. Diese können durch eine entsprechende Benutzeraktion (i. d. R. durch Anklicken) aufgerufen werden. Gegenüber dem üblichen linear aufgebauten Fließtext wie beispielsweise in Büchern bietet Hypertext somit eine beliebige Vernetzung von Texten durch Querverweise. → <i>HTML</i> und → <i>WML</i> sind zwei typische Vertreter von Auszeichnungssprachen für Hypertext-Dokumente.
ICC (<i>integrated chip card</i>)	Nach ISO die normgerechte Bezeichnung für eine Karte mit Chip. Es kann sich dabei sowohl um einen Speicherchip als auch einen Mikrocontrollerchip handeln.
ID-1 Karte (<i>ID-1 card</i>)	Nach ISO 7810 das Standardformat für → <i>Chipkarten</i> . Sie hat eine Breite von ≈ 85,6 mm, eine Höhe von ≈ 54 mm und eine Dicke ≈ 0,76 mm. ²⁹ Im Mobilfunkbereich wird mittlerweile jedoch vor allem das ID-000 Format (→ <i>Plug-In</i>) eingesetzt.
Identifizierung (<i>identification</i>)	Vorgang des Nachweises der Echtheit eines Gerätes oder einer Person durch Vergleich eines übergebenen Passwortes mit einem gespeicherten Referenzpasswort. Identifizierung kann als ein Spezialfall der → <i>Authentisierung</i> angesehen werden, wobei bei der Identifizierung eine Person authentisiert wird. Das zur Identifizierung verwendete Verfahren wird manchmal auch als → <i>cardholder verification method</i> bezeichnet.
IEC (<i>International Electrotechnical Commission</i>) [IEC]	Die IEC wurde 1906 gegründet und hat ihren Sitz in Genf, Schweiz. Die Aufgabe der IEC ist die weltweite Normung im Bereich der Elektrotechnik.
IFD (<i>interface device</i>)	Nach ISO die normgerechte Bezeichnung für ein Chipkarten-Terminal.
Implanter	Fertigungsmaschine für Chipkarten, deren Aufgabe es ist, Module in die Kavität von Kartenkörpern einzufügen, in der Fachsprache Implantieren genannt.
Implementierung (<i>implementation</i>)	Im Sinne der Softwareentwicklung die Erstellung eines Programms anhand der beim → <i>Design</i> festgelegten Software-Architektur. Zur Implementierung gehört das → <i>Debugging</i> , jedoch nicht der → <i>Test</i> , der bei einer sequentiellen Softwareentwicklung der nächste und abschließende Schritt ist.
IMSI-Catcher	Gerät zum Abhören von GSM-Gesprächen durch Aufbau einer eigenen Zelle. Das Funktionsprinzip beruht darauf, dass sich der IMSI-Catcher zwischen Mobiltelefon und Basisstation dazwischenschaltet, er sich also gegenüber dem Mobiltelefon als Basisstation ausgibt und gegenüber der echten Basisstation als Mobiltelefon.
IMT-2000 (<i>international mobile telecommunication 2000</i>)	Konzept der → <i>ITU</i> für Mobilfunk-Lösungen der dritten Generation (→ <i>3G</i>) im 2000 MHz Frequenzbereich. IMT-2000 entstand 1995 als Nachfolger von FPLMTS (<i>future public land mobile telecommunication service</i>), ein 1985 begonnenes Konzept der ITU für Mobilfunk, das sich jedoch nicht in der ursprünglichen Form als weltweit einheitliches System durchsetzen ließ. Eine mögliche Realisierung von IMT-2000 ist → <i>UMTS</i> .
Individualisierung (<i>individualisation</i>)	→ <i>Personalisierung</i>
Initialisierer (<i>initializer</i>)	Instanz, die die → <i>Initialisierung</i> durchführt.
Initialisierung (<i>initialisation</i>)	Das Laden der festen und personenunabhängigen Daten einer → <i>Anwendung</i> in das EEPROM. Ein Synonym für Initialisierung ist die Vorphersonalisierung.
Inlettfolie	Folie, die sich nach dem Zusammenlaminierten aller Folien im Innern des Kartenkörpers befindet. Ein Synonym für Inlettfolie ist Kernfolie. In der Regel wird die Inlettfolie zwischen zwei Deckfolien einlaminiert und bildet so mit den beiden äußeren Folien die Karte. Die Inlettfolie ist oft Träger von Sicherheitsmerkmalen oder elektrischen Bauteilen, wie beispielsweise der Spule für kontaktlose Chipkarten.

²⁹ Siehe auch Abschnitt 3.1.1 „Formate“.

Instrumentierung	Einfügen von speziellem → <i>Programmcode</i> in ein zu analysierendes Programm, um Abläufe und Aufrufe in diesem Programm für Testing analysieren zu können. ³⁰
Intelligente Speicherkarte	Speicherkarte mit erweiterter Logikschaltung für zusätzliche Sicherheitsfunktionen, die den Speicherzugriff überwachen.
interoperabel (<i>interoperability</i>)	Dieses Adjektiv wird in der Chipkartenwelt für Lösungen benutzt, die nicht auf eine spezifische Chipkarten-Anwendung (siehe auch Anwendung) oder Geräte eines bestimmten Herstellers zugeschnitten sind. → <i>Offene Chipkarten-Betriebssysteme</i> sind in der Regel interoperabel. Das Gegenteil von interoperablen Lösungen sind → <i>proprietäre</i> Lösungen. Ein Beispiel für eine → <i>interoperable</i> Chipkarte ist die → <i>SIM</i> , die in allen → <i>GSM</i> -Mobiltelefonen gleichermaßen ohne Kompatibilitätsprobleme eingesetzt werden kann.
Interpreter (<i>interpreter</i>)	Programm, das eine Programmiersprache wie BASIC oder Java zur Laufzeit in eine von einem Mikroprozessor ausführbare Maschinsprache übersetzt und auch sofort ausführt. Aufgrund des zur Laufzeit stattfindenden Übersetzungsvorgangs sind interpretierte Programme immer langsamer als kompilierter → <i>Programmcode</i> . Interpreter lassen jedoch wesentlich hardwareunabhängigere Programme als Compiler zu.
ISDN (<i>integrated services digital network</i>)	Bezeichnung für ein international standardisiertes digitales Fernsprechnetz, das gleichermaßen Telefongespräche wie Datenübertragung unterstützt. Ein ISDN-Anschluss besteht aus zwei Basiskanälen mit jeweils 64 kBit/s Übertragungsrate und einem Steuerkanal mit 16 kBit/s Übertragungsrate.
ISO (<i>International Standardisation Organization</i>) [ISO]	Die ISO wurde 1947 gegründet und hat ihren Sitz in Genf, Schweiz. Die Aufgabe von ISO ist, die weltweite Normung zu unterstützen, um einen ungehinderten Austausch von Gütern und Dienstleistungen zu ermöglichen. Die erste ISO-Norm wurde 1951 veröffentlicht und beschäftigt sich mit Temperaturen bei Längenmessungen.
ITSEC (<i>Information Technique System Evaluation Criteria</i>)	Kriterienkatalog zur Entwicklung und → <i>Evaluierung</i> der Sicherheit von informationstechnischen Systemen im europäischen Bereich und wurden 1991 veröffentlicht. Die Weiterentwicklung der ITSEC und Vereinheitlichung mit diversen nationalen Kriterienkatalogen sind die → <i>Common Criteria</i> .
ITU (<i>International Telecommunications Union</i>) [ITU]	Internationale Organisation zur Koordinierung, Normung und Entwicklung von globalen Telekommunikationsdiensten mit Sitz in Genf. Die Vorgängerorganisation war die CCITT.
Java Card Runtime Environment (JCRE) (Java Card Laufzeitumgebung)	Java Card Laufzeitumgebung besteht im Wesentlichen aus der → <i>Java Card Virtual Machine</i> (JVM) und dem Java Card API.
Java Card Virtual Machine (JCVM)	(→ <i>Virtual Machine</i>) Ein – üblicherweise in Software – simulierter → <i>Mikroprozessor</i> , der die Aufgabe hat, den Java Bytecode auszuführen und die Klassen und Objekte zu verwalten. Zusätzlich stellt die Java Card Virtual Machine die Trennung der → <i>Anwendungen</i> durch Firewalls sicher und ermöglicht die gemeinsame Nutzung von Daten. Im Prinzip kann sie auch als eine Art → <i>Interpreter</i> gesehen werden. Eine Clean Room VM ist die Implementation einer Java VM auf der Grundlage von öffentlich zugänglichen Informationen, d. h. ohne zusätzliche lizenzbedingte Informationen von Sun. Clean Room Implementierungen der Java VM gelten im allgemeinen als befreit von anfallenden Lizenzzahlungen an Sun.
Java Card	→ <i>Chipkarte</i> mit → <i>Mikrocontroller</i> , die unter anderem eine → <i>Java Card Virtual Machine</i> und ein → <i>Java Card Runtime Environment</i> besitzt. Java Cards sind → <i>Multiapplication-Chipkarten</i> mit der Eigenschaft, dass sie Programme in Java verwalten und ausführen können. Streng genommen ist eine Java Card kein → <i>Chipkarten-Betriebssystem</i> , da u. a. beispielsweise in den Ursprungsspezifikationen keine Dateiverwaltung festgelegt ist. In der Praxis gilt jedoch die Java Card als Urtyp eines → <i>offenen Chipkarten-Betriebssystems</i> .
Java Development Kit (JDK)	Sammlung von Softwarewerkzeugen, die die Softwareentwicklung in Java ermöglichen.
Java	Eine von der Firma Sun entwickelte hardwareunabhängige und objektorientierte Programmiersprache (→ <i>objektorientierte Programmierung</i>), die im Bereich des Internets stark verbreitet ist. Java Source Code wird mit einem Compiler in einen standardisierten Bytecode übersetzt, der dann üblicherweise mit einer so genannten

³⁰ Siehe auch Abschnitt 9.3.3 „Dynamische Tests von Betriebssystemen und Anwendungen“.

	virtuellen Maschine auf der jeweiligen Zielhardware (Intel, Motorola, ...) und Betriebssystemplattform (Windows, MacOS, Unix, ...) interpretiert wird. Es gibt Mikroprozessoren (Pico Java), die den Bytecode von Java direkt ausführen können.
Java Card Forum [JCF]	Ein im Jahr 1997 gegründetes und international agierendes Gremium verschiedener Chipkartenfirmen zur Förderung der Java Card Technologie und zur Entwicklung der dazugehörigen Spezifikationen (→ <i>Javacard</i>).
Kaltreset (<i>cold reset</i>)	→ <i>Reset</i>
Karte (<i>card</i>)	Allgemeiner Begriff für ein in seinen physischen Abmessungen genormtes rechteckiges Stück Material mit abgerundeten Ecken. Eine Karte kann mit verschiedenen → <i>Kartenelementen</i> ausgestattet sein und damit auch einen Halbleiterchip (→ <i>Chipkarte</i>) besitzen. Der englische Begriff <i>card</i> hat im WML-Umfeld eine völlig andere Bedeutung (→ <i>Card</i>).
Kartenakzeptant (<i>card acceptor</i>)	Eine Instanz, bei der Karten für eine bestimmte Form von Interaktion (z. B. Bezahlung) verwendet werden können. Typisches Beispiel ist ein Händler, der Kreditkarten zur Bezahlung akzeptiert.
Kartenbenutzer (<i>card holder</i>)	Person, die eine Karte benutzt. Sie ist deshalb der Kartenbesitzer, aber nicht unbedingt der Karteneigentümer.
Kartenbesitzer	Person, die die tatsächliche Verfügungsgewalt über eine Karte hat. Der Kartenbesitzer muss nicht zwangsläufig der Karteneigentümer sein.
Karteneigentümer	Natürliche oder juristische Person, die die rechtliche Herrschaft über die Karte hat und mit dieser nach Belieben verfahren kann. Bei Kredit- und Debitkarten sind die kartenherausgebenden Banken oft die Eigentümer der Karten, die kartenbenutzenden Kunden sind dann lediglich die Kartenbesitzer.
Kartenelement (<i>card component</i>)	Zusätzliche Funktionseinheiten auf einer → <i>Karte</i> , wie beispielsweise Unterschriftsstreifen, → <i>Hochprägung</i> , → <i>Magnetstreifen</i> , Chip (→ <i>Speicherkarte</i> , <i>Mikroprozessorkarte</i>) und Tastatur (→ <i>System-on-Card</i>).
Kartenemittent	andere Bezeichnung für den → <i>Kartenherausgeber</i>
Kartenherausgeber (<i>card issuer</i>)	Auch Kartenemittent; Instanz, die für die Ausgabe von Karten verantwortlich ist. Bei Monoapplikationskarten ist der Kartenherausgeber in der Regel zugleich Anwendungsanbieter, muss es aber nicht zwangsläufig sein.
Kartenhersteller (<i>card manufacturer</i>)	Instanz, die Kartenkörper herstellt, in die er Module einbettet.
Karteninhaber	Besitzer einer Karte, meistens auch der Benutzer.
Kartenkörper	Kunststoffkarte, die als Halbfertigprodukt in nachfolgenden Produktionsschritten weiterverarbeitet wird und u. U. weitere Funktionselemente enthält (z. B. implantierter Chip).
Kartenleser (<i>card reader</i>)	Mechanisch und elektrisch einfach aufgebautes Gerät, das zur Aufnahme und galvanischen Kontaktierung einer → <i>Chipkarte</i> dient. Im Gegensatz zu Terminals haben Kartenleser kein Display und keine Tastatur. Unabhängig vom Term „Kartenleser“ können Kartenleser in der Regel auch zum Schreiben von Daten in Karten verwendet werden.
Kavität (<i>cavity</i>)	Die üblicherweise gefräste Aussparung im Kartenkörper für das zu implantierende Modul.
Kennzeichen (<i>tag</i>)	→ <i>Tag</i>
Kerckhoff-Prinzip	Das nach Auguste Kerckhoff (1835–1903) benannte Prinzip besagt, dass die gesamte Sicherheit eines Kryptoalgorithmus ausschließlich auf der Geheimhaltung des Schlüssels beruhen soll und nicht auf der Geheimhaltung des Kryptoalgorithmus.
Kernel (Kern)	Zentraler Teil eines → <i>Betriebssystems</i> , der grundlegende Betriebssystemfunktionen den darüberliegenden Schichten des Betriebssystems bereitstellt.
Kernfolie (<i>core foil</i>)	anderer Ausdruck für → <i>Inletfolie</i>
Kernspannung (<i>core voltage</i>)	Die direkt auf dem Chip verwendete Betriebsspannung des Prozessors oder Mikrocontrollers. Ist die Kernspannung geringer als die an den Chip angelegte Spannung, so muss sie von einem auf dem Chip befindlichen Spannungswandler entsprechend reduziert werden. Niedrige Kernspannungen sind wegen der notwendigen Spannungsfestigkeit bei zunehmend geringeren Strukturbreiten und zur Reduktion der chipinternen Kapazitäten bei den immer höher werdenden Taktfrequenzen notwendig. Die typische Kernspannung von Mikrocontrollern in

	0,13 µm-Technologie ist beispielsweise 1,8 V.
Kineogramm	Ein Kineogramm zeigt unter verschiedenen Blickwinkeln unterschiedliche Darstellungen. Das Kineogramm kann einen scheinbaren und ruckartigen Bewegungsablauf zeigen, oder es zeigt unterschiedliche Motive in Abhängigkeit vom Betrachtungswinkel. Kineogramme sind ähnlich, aber nicht identisch den Hologrammen, die ein 3-dimensionales Bild zeigen.
Kippbild, Kineogramm	Vom Aufbau her ein Hologramm, dessen Abbildung sich sprunghaft mit dem Betrachtungswinkel ändert.
Klasse (<i>class</i>)	Im Sinne der → <i>objektorientierten Programmierung</i> eine Art von abstrakter Bauanleitung für ein → <i>Objekt</i> , d. h. für dessen → <i>Attribute</i> , → <i>Methoden</i> und Beziehungen zu anderen Objekten.
Klon	→ <i>klonen</i>
klonen	Das vollständige Kopieren von ROM und EEPROM eines Mikrocontrollers. Klonen ist ein typischer Angriff auf ein Chipkartensystem. Das Ergebnis ist ein Mikrocontroller mit vollends identischem Speicherinhalten und wird Klon genannt.
Kollision	Eine Kollision entsteht, wenn zwei oder mehr kontaktlose Karten, die sich im Aktionsbereich eines Terminals befinden, gleichzeitig Daten an das Terminal senden, so dass dieses die empfangenen Daten nicht decodieren oder eindeutig zuordnen kann.
Kommando (<i>command</i>)	Im Bereich von → <i>Chipkarten-Betriebssystemen</i> eine Anweisung an die Chipkarte, eine bestimmte Aktion auszuführen. Das Ergebnis eines Kommandos ist eine Antwort (<i>response</i>) der Chipkarte, die mindestens den Status, optional aber auch dazugehörige Daten des ausgeführten Kommandos rückmeldet. Kommandos werden durch → <i>Kommando-APDUs</i> an die Chipkarte übermittelt und Antworten durch → <i>Antwort-APDUs</i> .
Kommando-APDU (<i>command-APDU</i>)	→ <i>Kommando</i> vom Terminal an die Chipkarte; besteht aus dem Kommando-Header und optional aus dem Kommando-Body. Der Kommando-Header setzt sich wiederum aus Class-, Instruction-, P1- und P2-Byte zusammen (→ <i>APDU</i>). ³¹
kompletieren (<i>completion</i>)	Das Vervollständigen des Betriebssystems durch Laden der EEPROM-Teile. Dies ermöglicht nachträgliche Änderungen und Anpassungen, ohne dass eine neue ROM-Maske erstellt werden muss. Beim Kompletieren werden in jede Chipkarte identische Daten geschrieben, es ist also dem Prinzip nach eine Art Initialisierung.
Kontaktfläche	Die an der Vorderseite einer → <i>Chipkarte</i> befindlichen sechs oder acht Kontaktflächen sind die elektrische Schnittstelle zwischen dem Terminal und dem Mikrocontroller in der Chipkarte. Alle elektrischen Signale werden über diese Kontakte geführt.
kontaktlose Karte (<i>contactless card</i>)	Kurzbezeichnung für eine → <i>Chipkarte</i> , bei der die Energie- und Datenübertragung berührungslos durch elektromagnetische Felder erfolgt (→ <i>CICC</i>).
Kreditkarte (<i>credit card</i>)	Karte mit oder ohne Chip, die einen Verfügungsrahmen aufweist und bei der die Bezahlung zeitlich nach Erhalt des Gutes oder der Dienstleistung stattfindet. Diese Bezahlung wird oft als „buy now – pay later“ bezeichnet. Das typische Beispiel für die Kartenart sind hochgeprägte Kreditkarten.
Kryptoalgorithmus (<i>cryptoalgorithm</i>)	Rechenvorschrift mit mindestens einem geheimen Parameter, dem → <i>Schlüssel</i> , um Daten zu ver- oder entschlüsseln. Es gibt symmetrische Kryptoalgorithmen (z. B. DES-Algorithmus), die zur Ver- und Entschlüsselung den gleichen Schlüssel benutzen und asymmetrische Kryptoalgorithmen (z. B. RSA-Algorithmus), die zur Verschlüsselung einen öffentlichen Schlüssel und zur Entschlüsselung einen geheimen Schlüssel verwenden.
Kryptokoprozessor	Bezeichnet im Chipkartenbereich eine zusätzliche numerische Recheneinheit auf einem Mikrocontroller. Die Funktionalität dieses Koprozessors ist optimiert zur schnellen Berechnung von Secret-Key-Algorithmen (z. B. DES) und/oder Public-Key-Algorithmen (RSA, DSA, ECC).
kryptografischer Algorithmus (<i>crypto-</i>	Die mittlerweile selten verwendete Langform von → <i>Kryptoalgorithmus</i> .

³¹ Eine detaillierte Darstellung findet sich im Abschnitt 6.5.1 „Struktur der Kommando-APDUs“.

<i>graphic algorithm</i>)	
Kryptokarte	→ <i>Mikroprozessorkarte</i>
Kundenkarte (<i>customer card</i>)	→ <i>Chipkarte</i> , die von Kunden in einem elektronischen Zahlungsverkehrssystem an den Terminals der Händler zum Bezahlen benutzt wird.
kuvertieren	Automatisches Falten und Einstecken eines Briefes in einen Briefumschlag.
Ladebeauftragter (<i>load agent</i>)	Instanz, welche das Laden von elektronischen Geldeinheiten auf eine elektronische Geldbörse vornimmt. Er ist sozusagen das Gegenstück zum Leistungsanbieter.
Laminieren (<i>laminate</i>)	Das Verkleben von dünnen Materialschichten unter Druck und Hitze. Karten werden in der Regel aus mehreren Kunststofffolien laminiert.
Lasercutter	Gerät zum Bohren und Schneiden mit einem energiereichen Laserstrahl in einer Genauigkeit von Teilen eines Mikrometers vorzugsweise auf Halbleitern.
Lasergravur (<i>laser engraving</i>)	Verfahren zur Schwärzung von speziellen Kunststoffschichten durch Verbrennen mit einem Laser. Dieses Verfahren wird umgangssprachlich oft auch „lasern“ genannt.
Lead-Frame Modul	Kostengünstige Module, bei denen die aus einer Kupferlegierung mit galvanisierter Goldoberfläche gestanzten Kontaktflächen durch einen Moldkörper aus Kunststoff zusammengehalten werden. Auf diesem wird dann mit Pick-and-Place der Chip aufgesetzt und im Wire-Bond-Verfahren mit den Rückseiten der Kontaktflächen verbunden. Anschließend schützt man den Chip noch mit einem Überzug aus lichtundurchlässigem Epoxidharz.
Lead-Frame-Verfahren	Eines der zurzeit kostengünstigsten Verfahren zur Modulherstellung, ohne Nachteile bei der mechanischen Stabilität dafür in Kauf nehmen zu müssen.
Leadtime	Die Zeit in der Halbleiterfertigung von der Maskenabgabe (→ <i>ROM-Maske</i>) bis zu den ersten Mustern.
Lebenszyklus (<i>life cycle</i>)	Die Summe der Lebensphasen einer → <i>Chipkarte</i> , beginnend von der Chip- und Kartenherstellung über die → <i>Personalisierung</i> bis zur Benutzung und dem logischen oder physischen Lebensende der Karte. Im Lebenszyklus einer Karte werden dann die einzelnen Phasen zur Festlegung von bestimmten Sicherheitsmechanismen und Funktionalitäten verwendet. Ein Beispiel für die diesbezügliche Einteilung des Lebenszyklus einer Karte ist die → <i>Open Platform-Spezifikation</i> .
Leistungsanbieter (<i>service provider</i>)	In einem Chipkartensystem derjenige, der Leistungen anbietet, die ein Benutzer in Anspruch nimmt und bezahlt. Beim Beispiel eines Zahlungsverkehrssystems mit elektronischen Geldbörsen ist er derjenige, der vom Börseninhaber für seine Ware oder Dienstleistung Geld von einer elektronischen Geldbörse erhält.
leitungsorientiert	→ <i>verbindungsorientiert</i>
Linker	Ein Linker hat die Aufgabe, die symbolischen Speicheradressen eines kompilierten oder assemblierten → <i>Programmcodes</i> in absolute oder relative Speicheradressen umzusetzen.
little Endian	→ <i>Endianness</i>
Loader (<i>loader</i>)	Programm, mit dessen Hilfe weitere Programme, beispielsweise über eine serielle Schnittstelle, nachgeladen werden können (→ <i>Bootloader</i>).
Location based Service (standortbezogener Dienst)	Mehrwertdienste für Mobiltelefonteilnehmer, die auf dem Wissen über die aktuelle geografische Position beruhen. Beispiele dazu sind lokale Wettervorhersagen, dynamisch an den aktuellen Standort angepasste Stadtpläne und integrierte Standortangaben bei Notrufen.
logische Kanäle (<i>logical channels</i>)	Logische Kanäle dienen dazu, mit mehreren → <i>Anwendungen</i> auf einer Chipkarte parallel und unabhängig voneinander Daten auszutauschen. Die Kommunikation findet jedoch nach wie vor über die nur einmal vorhandene serielle Schnittstelle mit Chipkarte statt, durch die logischen Kanäle können jedoch die Empfängeranwendungen für die → <i>APDUs</i> auf der Chipkarte eindeutig adressiert werden. ³²
M/Chip	Name einer → <i>EMV</i> -konformen Implementierung einer chipgestützten Debit-/Kreditkarte von Europay und Mastercard. Die Variante M/Chip Select verwendet neben symmetrischen Kryptoalgorithmen auch asymmetrische und stellt eine

³² Siehe auch Abschnitt 6.7 „Logische Kanäle“.

	Obermenge von M/Chip light dar, welche eine vereinfachte Variante ist und nur symmetrische Kryptoalgorithmen benutzt.
MAC (<i>message authentication code</i> – Datensicherungscode)	Kryptografische Prüfsumme über Daten, mit der Manipulationen dieser Daten während der Übertragung erkannt werden können. Werden Daten während ihrer Ablage in einem Speicher mit einem MAC geschützt, so spricht man von einer CCS (→ <i>cryptographic checksum</i>).
Magnetkarte	Oft verwendete und sachlich nicht korrekte Kurzform des Begriffs → <i>Magnetstreifenkarte</i> .
Magnetstreifenkarte	Karte mit einem Magnetstreifen, auf dem Daten geschrieben und wieder gelesen werden können. Der Magnetstreifen enthält in der Regel drei Datenspuren mit unterschiedlicher Datenaufzeichnungsdichte. Spur 1 und 2 werden nach der Ausgabe an den Kartenbenutzer nur mehr gelesen, und Spur 3 darf auch im Feld noch geschrieben werden. Die magnetische Eigenschaft des magnetisierbaren Materials kann entweder hoch- oder niederkoerzitiv sein.
Maosco	→ <i>Multos</i>
Maske	Kurzform von → <i>ROM-Maske</i> .
M-Commerce (<i>mobile Commerce</i> , mobiler Geschäftsverkehr)	Alle Formen von Dienstleistung, Handel und dazugehörigem Zahlungsverkehr mit mobilen Endgeräten (z. B. Mobiltelefon, PDA). Werden stationäre Endgeräte verwendet, spricht man von → <i>E-Commerce</i> .
Mehrlagenkarte (<i>multi layer card</i>)	Karte, die sich aus mehreren Schichten Kunststoffolie zusammensetzt. Diese werden in die äußeren Deckfolien (<i>overlay foil</i>) und die Kernfolien (<i>core foils</i>) unterteilt (→ <i>Einlagenkarte</i>).
Memory Footprint	Die Aufteilung der Speicherbelegung bei einem Rechnersystem.
Methode (<i>method</i>)	Eine Methode im Sinne der → <i>objektorientierten Programmierung</i> ist eine Funktion für die Manipulation von Attributwerten (→ <i>Attribut</i>) eines → <i>Objekts</i> , die von der → <i>Klasse</i> des Objektes zur Verfügung gestellt wird.
MExE (<i>mobile station execution environment</i>)	Framework zur Integration einer Java Virtual Machine (JVM) in Mobiltelefone. Es können dann Java-Programme in Mobiltelefone geladen und ausgeführt werden. Damit besteht die Möglichkeit, Zusatzanwendungen direkt im Mobiltelefon und nicht (wie zur Zeit üblich) auf der SIM zu realisieren.
MF	Das Master File im Dateisystem einer Chipkarte ist ein besonderes DF. Es ist das Wurzelverzeichnis des Dateibaums und wird automatisch nach einem Reset der Chipkarte selektiert.
Microbrowser	→ <i>Browser</i>
Mikrocontroller (<i>microcontroller</i>)	Ein Mikrocontroller besitzt auf einem Chip einen → <i>Mikroprozessor</i> , flüchtigen Speicher (→ <i>RAM</i>), nichtflüchtigen Speicher (→ <i>ROM</i> , <i>EEPROM</i> , <i>Flash-EEPROM</i>) und entsprechende Schnittstellen für die Kommunikation nach chip-extern. Er ist damit ein selbstständig arbeitsfähiger Computer auf einem einzelnen Chip. Mikrocontroller werden neben Chipkarten vor allem in der Steuerungstechnik eingesetzt.
Mikroprozessor	Wichtigste Funktionseinheit eines → <i>Mikrocontrollers</i> . Er löst die im Programm festgelegten Maschinenbefehle in die elementaren Mikrobefehle auf und führt diese aus. Ein Mikroprozessor enthält alle für die Befehlsabarbeitung notwendigen Register, ein Steuerwerk und das Rechenwerk. Das eigentliche Rechenwerk eines Mikroprozessors wird manchmal auch Prozessor genannt. Der Begriff CPU (<i>central processing unit</i>) wird oft als Synonym zu Mikroprozessor gebraucht.
Mikroprozessorkarte	Karte mit Chip, welcher einen → <i>Mikrocontroller</i> mit CPU, flüchtigem (→ <i>RAM</i>) und nichtflüchtigem (→ <i>ROM</i> , <i>EEPROM</i> , ...) Speicher besitzt. Mikroprozessorkarten können noch einen numerischen Koprozessor (→ <i>Kryptokoprozessor</i>) haben, um Public-Key-Kryptoalgorithmen schnell ausführen zu können. Diese Art von Karten werden manchmal auch Kryptokarten oder Kryptocontrollerkarten genannt.
MILENAGE-Algorithmus	Der symmetrische Beispiyalgorithmus für die kryptografischen Funktionen f1 bis f5 (→ <i>f1</i>) der → <i>USIM</i> . Der MILENAGE-Algorithmus basiert in seinem Kern auf dem → <i>AES</i> .
MKT (Multifunktionales Kartenterminal)	Eine in Deutschland weit verbreitete Spezifikation für multifunktionale Chipkartenterminals (→ <i>Terminal</i>) und deren Anbindung an PCs mittels der → <i>CT-API-Schnittstellenspezifikation</i> . Es werden sowohl → <i>Speicherkarten</i> als auch

	→ <i>Mikroprozessorkarten</i> unterstützt. Der Herausgeber der Spezifikation ist Teletrust Deutschland.
Modul	→ <i>Chipmodul</i>
Modulhersteller	Instanz, die Dice in Module einbaut und eine elektrische Verbindung durch Bonden mit den Kontaktelementen herstellt.
Mondex [Mondex]	→ <i>Elektronische Geldbörse</i> auf Chipkarten mit der Möglichkeit von → <i>Purse-to-Purse-Transaktionen</i> .
Monoapplication-Chipkarte	Dieser Begriff sagt aus, dass sich auf einer Chipkarte nur eine → <i>Anwendung</i> befindet.
monofunktionale Chipkarte	Prozessorchipkarten, deren Betriebssystem nur eine einzige → <i>Anwendung</i> unterstützt und unter Umständen sogar auf diese Anwendung hin optimiert wurde. Verwaltungsfunktionen (z. B. Generieren und Löschen von Dateien) werden von monofunktionalen Chipkarten entweder überhaupt nicht oder nur in sehr eingeschränkter Form unterstützt.
MoU (<i>memorandum of understanding</i>)	Gemeinsame rechtliche Grundlage aller GSM-Netzbetreiber. Das Gremium hinter dem MoU ist die → <i>GSM Association</i> .
Multiapplication-Chipkarte (<i>multi application smart card</i>)	Dieser Begriff sagt aus, dass sich auf einer Prozessorchipkarte mehrere → <i>Anwendungen</i> befinden, z. B. eine Bankkarte mit Telefonfunktion.
multifunktionale Chipkarte (MFC, <i>multi functional card</i>)	(Üblicherweise) Prozessorchipkarten, die mehrere → <i>Anwendungen</i> unterstützen und die entsprechende Verwaltungsfunktionen für die Anlage und das Löschen von Anwendungen und Dateien haben.
Multitasking	Computersysteme, die Multitasking unterstützen, ermöglichen es, mehrere Programme quasi gleichzeitig auszuführen. Die parallel ausgeführten Programme befinden sich üblicherweise in einem von den anderen Programmen abgegrenzten und geschützten Adressraum und können nur über spezielle Mechanismen Daten miteinander austauschen. Multitasking ist nicht dem Multithreading gleichzusetzen, da dort ein einzelnes Programm quasi gleichzeitig mehrere Aufgaben ausführt. Ein Computersystem kann sowohl Multitasking als auch Multithreading unterstützen.
Multithreading	Computersysteme, die Multithreading unterstützen, ermöglichen es einem Programm, quasi gleichzeitig mehrere Aufgaben auszuführen. Die einzelnen Threads eines Programms benutzen dabei üblicherweise einen gemeinsamen Adressraum. Multithreading ist nicht dem Multitasking gleichzusetzen, da sich dort mehrere individuelle Programme in separierten Adressräumen parallel in der Ausführung befinden. Ein Computersystem kann sowohl Multithreading als auch Multitasking unterstützen.
Multos (<i>multiapplication operating system</i>)	Markenname eines offenen Multiapplication-Chipkarten-Betriebssystems (→ <i>Chipkarten-Betriebssystem, offenes Chipkarten-Betriebssystem</i>). ³³ Der Herausgeber der Spezifikationen, der Lizenzgeber und Betreiber der für Multos notwendigen Zertifizierungsdienste ist das Maosco Consortium [Maosco].
Namensraum (<i>namespace</i>)	Eine Menge von Namen, in der alle Namen eindeutig sind.
Nativecode (<i>native code</i>)	Programm in dem spezifischen Maschinencode für den Mikroprozessor, auf dem er ausgeführt wird.
NBS (<i>National Bureau of Standards</i>)	Die vor 1988 gültige Bezeichnung des → <i>NIST</i> .
NCSC (<i>National Computer Security Center</i>) [NCSC]	Das US-amerikanische NCSC ist eine Unterorganisation des NSA, zuständig für die Prüfung von Sicherheitsprodukten und Herausgeber von Kriterien für sichere Computersysteme, u. a. der TCSEC.
negative file	→ <i>Blacklist</i>
Nibble	Die vier höherwertigen oder niederwertigen Bits eines Bytes. Ein anderer Ausdruck für Nibble ist Halbbyte.
Nichtabstreitbarkeit	(I. d. R. kryptografische) Verfahren, die sicherstellen, dass der Empfänger den

³³ Siehe auch Abschnitt 5.14.2 „Multos“.

<i>(non-repudiation)</i>	Erhalt einer Nachricht nicht leugnen kann. Der Sender der Nachricht kann damit beweisen, dass sie der Empfänger bekommen hat. Nichtabstreitbarkeit ist also das Analogon zum „Einschreiben mit Rückantwort“ bei der konventionellen Briefpost.
nichtflüchtiger Speicher <i>(non-volatile memory)</i>	Speicherart (z. B. ROM, EPROM, EEPROM), die ihren Inhalt auch ohne Stromzufuhr behält.
NIST (<i>National Institute of Standards and Technology</i>) [NIST]	Das US-amerikanische NIST ist eine Abteilung des amerikanischen Wirtschaftsministeriums und zuständig für die US-nationale Normung von Informationstechnik. Bis 1988 trug es die Bezeichnung NBS. Das NIST ist der Herausgeber der FIPS-Normen.
Norm (<i>standard</i>)	Dokument, das technische Beschreibungen und/oder genaue Kriterien enthält, die als Regeln und/oder Definition von Eigenschaften verwendet werden, um dadurch sicherzustellen, dass Materialien, Produkte, Prozesse oder Leistungen für ihren Zweck verwendet werden können. In diesem Buch wird der Ausdruck „Norm“ durchgehend im Zusammenhang mit einem nationalen oder internationalen Normungsgremium (z. B. ISO, CEN, ANSI, ETSI) benutzt. Der deutsche Begriff Norm ist nicht mit dem deutschen Begriff → <i>Standard</i> gleichzusetzen.
NPU (<i>numeric processing unit</i>)	→ <i>Kryptokoprozessor</i>
NSA (<i>National Security Agency</i>) [NSA]	Die US-amerikanische NSA ist die offizielle Institution für Kommunikationssicherheit der amerikanischen Regierung. Sie ist direkt dem Verteidigungsministerium untergeordnet und hat u.a. die Aufgabe, ausländische Kommunikation abzuhören und zu decodieren. Die Entwicklung neuer Kryptoalgorithmen und die Beschränkung des Einsatzes von bestehenden fällt ebenfalls in das Aufgabengebiet dieser Behörde.
Null-PIN	→ <i>0-PIN</i>
Nutzdaten	Jene Daten, die direkt für eine → <i>Anwendung</i> notwendig sind.
Nutzen	Beim Druck die Zusammenfassung von kleinen zu bedruckenden Teilen (z. B. eine Karte) auf einem großen Bogen, der nach dem Bedrucken in einzelne Teile getrennt wird. Dadurch kann der Druckvorgang fertigungstechnisch optimiert werden, da die großen Bögen in einem Arbeitsschritt gefertigt werden können, anstatt in vielen einzelnen. Ein typischer Nutzen beim Druck von Karten besteht beispielsweise aus 42 Karten auf einer großen Kunststoffolie.
Objekt (<i>object</i>)	Im Sinne der → <i>objektorientierten</i> Programmierung ist ein softwaretechnisches Konstrukt, dessen Bauanleitung eine → <i>Klasse</i> ist, die Daten enthält, d. h. → <i>Attribute</i> hat, die mit in der Klasse definierten → <i>Methoden</i> gelesen und geändert werden können.
objektorientierte Programmierung (<i>object oriented programming</i>)	Die objektorientierte Programmierung basiert darauf, dass alle Daten einer Software in → <i>Objekten</i> abgelegt sind, die auch → <i>Methoden</i> bereitstellen, um diese Daten zu lesen oder zu ändern. Die Objekte werden durch → <i>Klassen</i> definiert. Ein zentraler Aspekt der objektorientierten Programmierung ist, dass die zu verarbeitenden Daten und nicht der Programmablauf wie bei der → <i>prozeduralen Programmierung</i> im Mittelpunkt steht. Typische objektorientierte Programmiersprachen sind C++ und → <i>Java</i> .
OCF (<i>open card framework</i>) [OCF]	Die OCF-Spezifikation beschreibt eine plattformunabhängige Java-basierte Schnittstelle zur Einbindung von Chipkarten in beliebige Anwendungen auf PCs. Die Voraussetzung ist, dass für das jeweils am PC benutzte Terminal ein passender Treiber vorhanden ist und die verwendete Chipkarte OCF-kompatibel ist.
Offcard-Anwendung (<i>offcard application</i>)	→ <i>Anwendung</i>
offene Anwendung	→ <i>Anwendung</i> auf einer Chipkarte, die unterschiedlichen Leistungsanbietern (z. B. Händlern, Dienstleistern) ohne notwendige Rechtsbeziehung untereinander zur Verfügung steht.
offene Börse	Realisation einer offenen → <i>Anwendung</i> für eine elektronische Geldbörse. Mit ihr können allgemeine Zahlungstransaktionen für unterschiedliche Leistungsanbieter getätigt werden.
offene Plattform (<i>open platform</i>)	→ <i>offenes Chipkarten-Betriebssystem</i> oder → <i>OP</i>
offenes Chipkarten-Betriebssystem (<i>open smart card operations</i>)	Ein → <i>Chipkarten-Betriebssystem</i> wird als offen bezeichnet, wenn es die Möglichkeit bietet, unabhängig vom → <i>Betriebssystemhersteller</i> dritte → <i>Anwendungen</i> und Programme auf die Chipkarte zu laden und diese dort in sicherer

<i>ting system)</i>	Umgebung auszuführen. Die drei bekanntesten offenen Chipkarten-Betriebssysteme sind → <i>Multos</i> , → <i>Java Card</i> und → <i>Windows for Smart Cards</i> . Offene Chipkarten-Betriebssysteme sind in der Regel → <i>interoperabel</i> und nicht → <i>proprietär</i> . Ein anderer Ausdruck für offenes Chipkarten-Betriebssystem ist auch offene Plattform (<i>open platform</i>), welche aber nicht mit der Schnittstelle zur Verwaltung von Applikationen auf einer Chipkarte (→ <i>OP</i>) verwechselt werden darf.
Oncard-Anwendung (<i>oncard application</i>)	→ <i>Anwendung</i>
oncard Matching	Fähigkeit einer → <i>Chipkarte</i> , <i>oncard</i> oder <i>offcard</i> gemessene biometrische Daten mit in der Chipkarte gespeicherten Referenzdaten zwecks Benutzeridentifizierung (→ <i>Identifizierung</i>) zu vergleichen.
OP (<i>Open Platform</i>)	früher Visa Open Platform (VOP); eine ursprünglich von Visa International spezifizierte Schnittstelle im → <i>Chipkarten-Betriebssystem</i> mit der Aufgabe der Verwaltung von Chipkarten-Applikationen. Die Spezifikation umfasst unter anderem das Nachladen von Chipkarten-Applikationen, die Sicherstellung der Applikationslebenszyklen (→ <i>Lebenszyklus</i>) und die Verbindung einer Chipkarten-Applikation mit dem Chipkarten-Betriebssystem. Die OP-Spezifikation ist der internationale <i>de facto</i> Standard bei → <i>Multiapplication-Chipkarten</i> und zum Applikationsmanagement. Der Herausgeber von OP ist mittlerweile das → <i>Global Platform Gremium</i> .
Optische Speicherkarte (<i>optical memory card</i>)	Karte, bei der Informationen in einer reflektierenden Schicht auf der Kartenoberfläche eingebrannt sind (analog einer CD).
OTA (<i>over the air</i>)	Bezeichnung für die Möglichkeit im → <i>GSM</i> - und → <i>UMTS</i> -System, zwischen Hintergrundsystem und → <i>SIM</i> über die Luftschnittstelle von Feststation und Mobilstation eine Ende-zu-Ende-Verbindung (→ <i>End-to-End-Verbindung</i>) aufzubauen. Damit können dann beispielsweise direkt vom Hintergrundsystem aus Kommandos transparent an die <i>SIM</i> gesendet werden. OTA ist auch eine der Grundlagen für alle → <i>Zusatzanwendungen</i> auf der <i>SIM</i> , da diese über die Luftschnittstelle auch direkt und transparent Daten mit übergeordneten Systemen austauschen können. Als Übertragungsdienst (→ <i>Bearer</i>) für OTA wird oft der Kurzmitteilungsdienst → <i>SMS</i> benutzt.
Package	Bei der <i>Javacard</i> ein → <i>Namensraum</i> und die kleinste Einheit innerhalb der Sprache <i>Java</i> . Ein <i>Package</i> kann über Klassen und Interfaces verfügen. ³⁴
Padding	Erweiterung eines Datenstrings durch Fülldaten mit dem Zweck, diesen Datenstring auf eine bestimmte Länge zu bringen. Meist muss die neue Länge des Datenstrings ein Vielfaches einer bestimmten Blocklänge (z. B. 8 Byte) sein, um dann den Datenstring beispielsweise durch einen Kryptoalgorithmus weiterverarbeiten zu können.
paketorientiert (<i>packet-switched</i>)	Bei paketorientierten Verbindungen werden die auszutauschenden Daten beim Sender in Pakete aufgeteilt, einzeln und u. U. auch über unterschiedliche Wege übertragen und beim Empfänger wieder zu den ursprünglichen Daten zusammengesetzt. Bei paketorientierten Verbindungen wird in der Regel die übertragene Datenmenge abgerechnet und nicht die Zeitdauer der Verbindung (→ <i>verbindungsorientiert</i>). Typische Beispiele für paketorientierte Verbindungen sind <i>X.25</i> und <i>GPRS</i> .
parallele Datenübertragung	Hier werden mehrere (z. B. 8/16/32) Datenbits gleichzeitig auf eben so vielen Datenleitungen übertragen (→ <i>serielle Datenübertragung</i>).
Paritätsbit (<i>parity bit</i>)	Der wohl bekannteste Fehlererkennungscode (→ <i>EDC</i>) ist die Verwendung eines Paritätsbits, das an das zu schützende Byte angehängt wird. Vor der Berechnung der Parität muss festgelegt werden, ob mit gerader (<i>even</i>) oder ungerader (<i>odd</i>) Parität gearbeitet wird. Bei der geraden Parität wird das Paritätsbit so gewählt, dass die Gesamtzahl der Einsen im Datenbyte und im Paritätsbit eine gerade Zahl ergibt. Bei ungerader Parität muss die Zahl der Einsen in Datenbyte und Paritätsbit ungerade sein. Mit einem Paritätsbit ist die sichere Erkennung von einem falschen Bit pro Byte möglich. Die Korrektur eines Bitfehlers hingegen ist nicht möglich, da das Paritätsbit keine Aussage über die Position des veränderten Bits erlaubt.
Passivierung	Schutzschicht auf einem Halbleiter, um ihn vor Oxidation und anderen chemischen Vorgängen zu schützen. Vor einer physischen Manipulation des Halbleiters muss sie teilweise oder vollständig entfernt werden.
Patch	In der Softwareentwicklung ein kleines Programm, manchmal auch in Maschinencode geschrieben, das die Funktionalität eines vorgegebenen Programms er-

³⁴ Siehe auch Abschnitt 5.14.1 „Java Card“.

	gänzt oder abändert. Patches werden in der Regel zur schnellen und unkomplizierten Korrektur von Programmfehlern benutzt. Sie werden entweder als → <i>work around</i> oder als → <i>bug fix</i> realisiert.
Patent	Dokument, das einem Erfinder das Recht zur alleinigen Verwertung der Erfindung für einen beschränkten Zeitraum und für ein oder mehrere bestimmte Länder einräumt. Die maximale Laufzeit eines Patents beträgt üblicherweise 20 Jahre.
Pay before	Dieser Ausdruck bezieht sich auf den Geldfluss bei Karten im Zahlungsverkehr. Vor dem Erhalt der gewünschten Ware oder Dienstleistung fließt das „echte“ Geld des Karteninhabers. Typische Vertreter von Pay before sind die → <i>elektronischen Geldbörsen</i> , die vor dem Einkauf mit elektronischem Geld geladen werden müssen. Im Telekommunikationsbereich wird diese Art der Bezahlung als → <i>prepaid</i> bezeichnet.
Pay later	Dieser Ausdruck bezieht sich auf den Geldfluss bei Karten im Zahlungsverkehr. Erst nach dem Erhalt der gewünschten Ware oder Dienstleistung fließt das „echte“ Geld des Karteninhabers. Typische Vertreter von Pay later sind die Kreditkarten, bei denen zum Teil erst Wochen nach dem Kauf das Geld vom Konto des bezahlenden auf das Konto des Händlers transferiert wird. Im Telekommunikationsbereich wird diese Art der Bezahlung als → <i>postpaid</i> bezeichnet.
Pay now	Dieser Ausdruck bezieht sich auf den Geldfluss bei Karten im Zahlungsverkehr. Beim Erhalt der gewünschten Ware oder Dienstleistung fließt das „echte“ Geld des Karteninhabers. Typische Vertreter dafür sind alle Debitkarten, wie beispielsweise die ec-Karte, die es ermöglicht, unmittelbar beim Kauf Geld vom Konto des Bezahlers auf das Konto des Händlers zu transferieren.
PC/SC (<i>personal computer/smart card</i>) [PC/SC]	Die PC/SC-Spezifikation beschreibt eine plattform- und programmiersprachenunabhängige Schnittstelle zur Einbindung von Chipkarten in beliebige Anwendungen. Die Voraussetzung ist, dass für das jeweils am PC benutzte Terminal ein passender Treiber vorhanden ist und die verwendete Chipkarte PC/SC-kompatibel ist. Im Dezember 1997 wurde die Version 1.0 der aus acht Teilen bestehenden „Interoperability Specification for ICCs and Personal Computer Systems“ veröffentlicht. ³⁵
PCD (<i>Proximity Coupling Device</i>)	Ein PCD ist ein Kartenterminal welches die Kommunikation mit einer kontaktlosen Karte (→ <i>PICC</i>) ermöglicht.
Persistenz (<i>persistent</i>)	Persistenz ist die Fähigkeit eines Objekts, über die Ausführungszeit eines Prozesses hinaus zu existieren, das Gegenteil ist die Transistenz. Persistente Objekte überdauern deshalb sowohl eine Sitzung als auch plötzliche Spannungsausfälle, ohne dass Daten verloren gehen oder inkonsistent werden.
Personalisierer (<i>personaliser</i>)	Instanz, die die Personalisierung durchführt.
Personalisierung (<i>personalisation</i>)	Die Personalisierung ist der Vorgang der Zuordnung einer Karte zu einer Person. Dies kann einerseits durch die physikalische Personalisierung (z. B. Hochprägung, Lasergravur) oder auch durch die elektrische Personalisierung (d. h. Laden der personenbezogenen Daten in den Speicher der Chipkarte) geschehen. Das Wort Individualisierung für diesen Vorgang wäre der exaktere Begriff, da bei der elektrischen Personalisierung nicht zwangsläufig personenbezogene Daten in den Chip geschrieben werden, wie beispielsweise bei anonymen → <i>vorbezahlten SIMs</i> .
Phase 1, Phase 2, Phase 2+	Diese Phasen kennzeichnen einzelne aufeinander aufbauende Entwicklungsschritte im → <i>GSM</i> -System. In Phase 1 wurden u. a. die Basisdienste Sprachübertragung, Rufweiterleitung, → <i>Roaming</i> und → <i>SMS</i> realisiert. In Phase 2 kamen ab 1996 zu den Diensten der Phase 1 u. a. die Dienste Konferenzschaltung, Gesprächsweitergabe, Rufnummernübermittlung und GSM im 1 800 MHz Frequenzband hinzu. Anschließend wurden diese Dienste in Phase 2+ u. a. mit der Funktionalität des → <i>SIM Application Toolkit</i> , HSCSD (<i>high speed circuit switched data</i>) und → <i>GPRS</i> ergänzt.
PICC (<i>Proximity Integrated Circuit Card</i>)	Kontaktlose Chipkarte mit einer Reichweite von ungefähr 10 cm.
PIN (<i>personal identification number</i>)	Eine üblicherweise 4-stellige numerische geheime Zahl zur → <i>Identifizierung</i> einer Person. In der Telekommunikationswelt wird für die PIN meist die Bezeichnung CHV (<i>card holder value</i>) benutzt.
PIN-Pad	Im ursprünglichen Sinn die mechanisch und kryptografisch besonders geschützte Eingabetastatur bei Terminals. Im allgemeinen Sprachgebrauch wird oft auch das ganze Terminal als PIN-Pad bezeichnet.

³⁵ Siehe auch Abschnitt 11.4.1 „PC/SC“.

PKCS #1 ... 15 (<i>public key cryptography standard number 1 ... 15</i>) [RSA]	Die Public Key Cryptography Standards sind von der Firma RSA Inc. veröffentlichte Regelwerke mit Fokus auf die Anwendung von asymmetrischen Kryptgorithmen, wie z. B. RSA. ³⁶
PKI (<i>public key infrastructure</i>)	Alle Einrichtungen, die zum Betrieb und zur Verwaltung einer auf asymmetrischer Kryptografie aufbauenden Datenspeicherung und Datenaustausch notwendig sind. Dies ist unter anderem eine → <i>Zertifizierungsinstanz</i> , eine → <i>Registrierungsinstanz</i> , ein → <i>Verzeichnisdienst</i> für Sperrlisten (→ <i>Zertifikatswiderrufsliste</i>), ein Zeitstempeldienst (→ <i>Zeitstempel</i>) und → <i>Signaturkarten</i> .
PLMN (<i>public land mobile network</i>)	<i>terminus technicus</i> für terrestrische Mobilfunknetze.
Plug-In (Einschubkarte)	Chipkarte in kleinem Format nach GSM 11.11 und TS 102.221, die vor allem im Mobilfunkbereich und als Sicherheitsmodul bei Terminals Verwendung findet. Die offizielle Formatbezeichnung für ein Plug-In nach ISO lautet ID-000 Format im Gegensatz zum größeren ID-1 Format (→ <i>ID-1 Karte</i>) der üblichen Chipkarten. Sie hat eine Breite von ≈ 25 mm, eine Höhe von ≈ 15 mm und eine Dicke $\approx 0,76$ mm. ³⁷
polling	Das laufende programmgesteuerte Abfragen eines Eingabekanals zur Detektion einer eingehenden Nachricht. Polling benötigt je nach Wiederholrate der stattfindenden Abfragen unter Umständen große Rechenleistung, weshalb man versucht, polling zu vermeiden und stattdessen eine von der Rechnerhardware unterstützte Abfrage mittels Interrupt bevorzugt.
POS (<i>point of sale</i>)	Die Örtlichkeit, bei der ein bestimmtes Gut oder eine bestimmte Dienstleistung verkauft wird.
postpaid	Bezieht sich auf den Geldfluss bei Karten im Telekommunikationsbereich. Erst nach dem Erhalt der Dienstleistung (i. d. R. Telefonat oder Datenübertragung) fließt das echte Geld des Karteninhabers. Postpaid-Karten sind seitens der Zahlfunktion mit Kreditkarten vergleichbar. Im Zahlungsverkehr wird diese Art der Bezahlung als → <i>pay later</i> bezeichnet.
Power-On-Reset	→ <i>Reset</i>
prepaid (vorbezahlt)	Bezieht sich auf den Geldfluss bei Karten im Telekommunikationsbereich. Bereits vor dem Erhalt der Dienstleistung (i. d. R. Telefonat oder Datenübertragung) fließt das echte Geld des Karteninhabers. Prepaid-Karten sind seitens der Zahlfunktion mit elektronischen Geldbörsen vergleichbar. Im Zahlungsverkehr wird diese Art der Bezahlung als → <i>pay before</i> bezeichnet.
prepaid SIM (vorbezahlte SIM)	Vorbezahlte und in der Regel wiederaufladbare SIM. Die gesamte Funktionalität der Abrechnung und Wiederaufladung wird im Regelfall durch das Hintergrundsystem abgedeckt, hat also keine Auswirkungen auf Datenelemente oder Funktionen in der SIM. Das Gegenteil ist eine → <i>postpaid SIM</i> .
Proaktivität	Transaktions-Mechanismus für Chipkarten, der es der Chipkarte ermöglicht, selbstständig Aktionen im Terminal zu starten. Damit wird das starre Master-Slave-Prinzip bei der Chipkarten-Kommunikation umgangen. Realisiert wird die Proaktivität durch zyklisch stattfindende Anfragen des Terminals (d. h. <i>polling</i>) an die Chipkarte. Die Zykluszeit der Anfragen kann dabei vorab durch die Chipkarte eingestellt werden. Entstanden und hauptsächlich eingesetzt wird die Proaktivität vor allem bei SIMs, um nach GSM 11.14 einen Teil der Steuerung des Mobiltelefons zu übernehmen.
probabilistisch (<i>probabilistic</i>)	Bezeichnet ein Verfahren oder Algorithmus, der bei identischen Ausgangsbedingungen zu unterschiedlichen Ergebnissen kommt. Das Gegenteil ist → <i>deterministisch</i> .
Programmcode	Bezeichnung für ein von einem → <i>Interpreter</i> oder direkt vom → <i>Mikroprozessor</i> ausführbares Programm (→ <i>Nativecode</i>).
proprietär (<i>proprietary</i>)	Dieses Adjektiv wird in der Chipkartenwelt in häufig abwertender Form für firmenspezifische Lösungen benutzt, deren Spezifikationen nicht vollständig veröffentlicht oder die Eigentum einer einzelnen Firma sind. Das Gegenteil zu proprietär sind so genannte offene Lösungen, die auch von Dritten benutzt werden können. Sowohl die Verwendung des Begriffs proprietär als auch des Begriffs der offenen Lösung ist aber keinesfalls eindeutig. Objektiv gesehen ist

³⁶ Siehe auch Abschnitt 4.7.2 „Asymmetrische Kryptoalgorithmen“.

³⁷ Siehe auch Abschnitt 3.1.1 „Formate“.

	manches so genannte offene Chipkarten-Betriebssystem auch beachtlich proprietär und abhängig von einer bestimmten Firma. Eine proprietäre Chipkarten-Anwendung (→ <i>Anwendung</i>) wäre beispielsweise ein elektronisches Geldbörsensystem für ein abgegrenztes Gebiet, das sich nicht an die einschlägigen Spezifikationen hält und von einer bestimmten Firma als Speziallösung entwickelt wurde.
Protection Profil (PP)	Im Rahmen einer → <i>Evaluierung</i> eine implementierungsunabhängige Menge von Sicherheitsvorgaben (→ <i>Security Target</i>), angepasst an spezifische Anwendungsgebiete für bestimmte → <i>Targets of Evaluation</i> .
Proton [Proton]	Markenname eines weltweit verbreiteten elektronischen Geldbörsensystems mit ca. 50 Millionen ausgegebenen Karten (Stand Frühjahr 2002). Die Spezifikationen von Proton definieren u. a. auch ein Multiapplication-Chipkarten-Betriebssystem (→ <i>Chipkarten-Betriebssystem</i>).
Prototyp	Ein (Software-)Prototyp ist ein ablauffähiges Modell des späteren Produkts mit eingeschränkter Funktionalität. Er wird zur Erprobung von bestimmten Eigenschaften des späteren Produkts benutzt. Beim horizontalen Prototyp werden nur bestimmte Ebenen der Software realisiert, wogegen beim vertikalen Prototyp bestimmte Teile durch alle Ebenen der Software hindurch realisiert werden.
prozedurale Programmierung	Die prozedurale Programmierung basiert darauf, dass Programme als Folgen von Anweisungen an einen → <i>Mikroprozessor</i> formuliert werden. Der Programmablauf kann zur Vereinfachung in Funktionen zerlegt werden und die notwendigen Daten werden in Variablen gehalten. Ein zentraler Aspekt der prozeduralen Programmierung ist, dass der Programmablauf und nicht wie bei der → <i>objektorientierten Programmierung</i> die zu verarbeitenden Daten im Mittelpunkt stehen. Typische prozedurale Programmiersprachen sind Basic und C.
Prozessmodell	anderer Begriff für → <i>Vorgehensmodell</i>
Prozessor	→ <i>Mikroprozessor</i>
Prozessorkarte	Kurzform von → <i>Mikroprozessorkarte</i> .
Pseudonymisierung	Veränderung von personenbezogenen Daten mittels einer Zuordnungsvorschrift in einer Weise, dass es nicht mehr möglich ist, diese veränderten Daten ohne Kenntnis der Zuordnungsvorschrift der ursprünglichen Person zuzuordnen. Der Begriff rührt daher, dass im einfachsten Fall der ursprüngliche Name durch ein einzigartiges Pseudonym ersetzt wird. In einer separaten Zuordnungstabelle (der Zuordnungsvorschrift) wird dann die Verbindung zwischen Pseudonym und ursprünglichem Namen hergestellt (→ <i>Anonymisierung</i>).
PSTN (<i>public switched mobile network</i>)	Bezeichnung für das reguläre öffentliche leitungsgebundene Telefonnetz.
Public-Key-Algorithmus	→ <i>Kryptoalgorithmus</i>
PUK (<i>personal unblocking key</i>)	Spezielle → <i>PIN</i> zum Rücksetzen des auf dem Maximalwert stehenden Fehlbedienungs Zählers der <i>PIN</i> . Eine PUK hat üblicherweise eine größere Länge (z. B. 8stellig) als die <i>PIN</i> , da Benutzer die PUK nur im Fall einer vergessenen <i>PIN</i> kennen müssen und dann in ihren Unterlagen nachsehen können. Mit der erfolgreichen Benutzung einer PUK wird gleichzeitig eine neue <i>PIN</i> festgelegt, da die alte <i>PIN</i> dem Benutzer offensichtlich nicht mehr bekannt war.
Pull-Technologie	Informationsweitergabe durch das Abholen von Information von einem übergeordneten System (z. B. Server) durch ein untergeordnetes System (z. B. Mobiltelefon). Der Gegensatz zur Pull-Technologie ist die → <i>Push-Technologie</i> .
Purse-to-Purse-Transaktion (<i>purse to purse transaction</i>)	Transaktion von elektronischen Geldeinheiten von einer elektronischen Geldbörse direkt zu einer anderen, ohne den Umweg über ein drittes, übergeordnetes System. Im Regelfall bedeutet diese Funktionalität, dass das Börsensystem anonym arbeiten muss und die elektronischen Geldbörsen für diese Funktion einen gemeinsamen Schlüssel benutzen müssen.
Push-Technologie	Informationsweitergabe durch das Versenden von Information von einem übergeordneten System (z. B. Server) an ein untergeordnetes System (z. B. Mobiltelefon). Der Gegensatz zur Push-Technologie ist die → <i>Pull-Technologie</i> .
Quick	Markenname der 1995 in Österreich landesweit eingeführten elektronischen Geldbörse. Diese basiert in ihren wesentlichen Teilen auf der europäischen Norm für branchenübergreifende elektronische Geldbörsen EN 1546. ³⁸
Radicchio [Radicchio]	Weltweite Initiative von Firmen und Organisationen zur Entwicklung von sicheren mobilen → <i>E-Commerce</i> -Lösungen mit → <i>PKI</i> .

³⁸ Siehe auch Abschnitt 12.3.1 „CEN-Norm EN 1546“.

RAM (<i>random access memory</i>)	Flüchtige Speicherart, die in Chipkarten als Arbeitsspeicher Verwendung findet. Das RAM verliert seinen Inhalt bei Stromausfall. SRAM und DRAM sind RAM-Speicher mit besonderen technischen Eigenschaften. ³⁹
Rauschfreiheit	Eine Eigenschaft von → <i>Kryptoalgorithmen</i> . Diese benötigen bei Rauschfreiheit unabhängig von → <i>Schlüssel</i> , Klar- und Schlüsseltext für die Ver- und Entschlüsselung immer die gleiche Zeit. Ist ein Kryptoalgorithmus nicht rauschfrei, kann durch eine Analyse der Berechnungszeit der Schlüsselraum sehr stark eingeschränkt werden. Auf diese Weise kann der Schlüssel wesentlich schneller als bei einer erschöpfenden Schlüsselsuche gefunden werden.
Record	Auch Datensatz; eine bestimmte Anzahl von Daten ähnlich einem String.
Redlist	→ <i>Hotlist</i>
regelbasierte Programmierung	Diese Programmierung basiert darauf, dass allgemeine Regeln formuliert werden, die dann auf die zu lösenden Probleme angewandt werden. Anhand dieser Regeln kann dann das Problem vom Computer selbstständig gelöst werden. Ein zentraler Aspekt der regelbasierten Programmierung besteht darin, dass keine Programmabläufe wie bei der → <i>prozeduralen Programmierung</i> oder die zu verarbeitenden Daten wie bei der → <i>objektorientierten Programmierung</i> im Mittelpunkt stehen, sondern allgemeine Regeln. Typische regelbasierte Programmiersprachen sind Lisp und Prolog.
Registrierungsinstanz (<i>registration authority – RA</i>)	Nimmt bei einer → <i>PKI</i> die Zertifizierungsanträge von Antragstellern entgegen und leitet diese nach Prüfung der Echtheit der Antragsteller an die → <i>Zertifizierungsinstanz</i> weiter. Die Registrierungsinstanz ist somit die Instanz, die die eindeutige Zuordnung von Zertifikaten zu Personen herbeiführt.
Remote Applet Management	Die Verwaltung (Erzeugen, Löschen, ...) von → <i>Applets</i> in einer Chipkarte von einem Hintergrundsystem aus. Beispielsweise ist es in verschiedenen → <i>GSM-Systemen</i> über die Luftschnittstelle möglich, Applets in eine SIM zu laden bzw. zu löschen.
Remote File Management	Die Verwaltung (Erzeugen, Löschen, Schreiben, Lesen, Änderung der Zugriffsbedingungen, ...) von Dateien in einer Chipkarte von einem Hintergrundsystem aus. Beispielsweise ist es in verschiedenen → <i>GSM-Systemen</i> möglich, über die Luftschnittstelle neue Dateien in einer SIM zu erzeugen und in diese Daten zu schreiben.
Reset	Zurücksetzen eines Computers (hier: einer Chipkarte) auf einen klar definierten Ausgangszustand. Man spricht von einem Kaltreset oder Power-On-Reset, wenn zur Ausführung des Resets die Versorgungsspannung ab- und wieder angeschaltet wird. Ein Warmreset wird durch ein Signal auf der Resetleitung zur Chipkarte ausgeführt, die Versorgungsspannung bleibt davon unberührt.
Retikel	→ <i>ROM-Maske</i>
roaming	Die Erreichbarkeit eines Mobiltelefons in einem anderem Netz als dem → <i>Heimatnetz</i> .
roll back	Funktionalität von Betriebssystemen, Daten im Fehler- oder Abbruchfall konsistent zu halten. Bei der roll back-Funktionalität werden die bei einer fehlerhaften oder abgebrochenen Operation verwendeten Daten durch die ursprünglichen Daten wieder ersetzt. Dieser Prozess kann automatisch oder nach Anforderung angestoßen werden und ist bei Chipkarten-Betriebssystemen oft durch → <i>atomare Abläufe</i> realisiert. Eine andere Strategie der Konsistenzhaltung von Daten im Fehler- oder Abbruchfall ist die → <i>roll forward</i> -Funktionalität.
roll forward	Funktionalität von Betriebssystemen, Daten im Fehler- oder Abbruchfall konsistent zu halten. Bei der roll forward-Funktionalität wird bei einer fehlerhaften oder abgebrochenen Operation mit den vorhandenen inkonsistenten Daten die Operation in einer Art wieder aufgenommen, dass die Daten anschließend wieder konsistent sind. Dieser Prozess kann automatisch oder nach Anforderung angestoßen werden, ist jedoch bei Chipkarten-Betriebssystemen aufgrund der hohen Sicherheitsanforderungen selten realisiert. Eine andere Strategie der Konsistenzhaltung von Daten im Fehler- oder Abbruchfall ist die → <i>roll back</i> -Funktionalität.
ROM (<i>read only memory</i>)	Nichtflüchtige Speicherart, die in Chipkarten Verwendung findet. Sie dient vornehmlich zur Speicherung von Programmen und statischen Daten, da sich der Inhalt eines ROM nicht verändern lässt. ⁴⁰
romed application	Diese Bezeichnung wird für Chipkarten-Anwendungen benutzt, die sich nicht im EEPROM befinden, sondern fest im maskenprogrammierten ROM des →

³⁹ Siehe auch Abschnitt 3.4.2 „Speicherarten“.

⁴⁰ Siehe auch Abschnitt 3.4.2 „Speicherarten“.

	<i>Chipkarten-Mikrocontrollern.</i>
ROM-Maske (<i>ROM-mask</i>)	Dieser Begriff wird umgangssprachlich sehr kontextspezifisch verwendet. Die ursprüngliche Bedeutung einer ROM-Maske ist die halbleitertechnische Belichtungsmaske für die Herstellung des ROM bei der Halbleiterfertigung. Die Bezeichnung Maske wird jedoch nur verwendet, wenn bei der Belichtung des → <i>Wafers</i> gegenüber der Maske keine Verkleinerung stattfindet. Werden hingegen die Strukturen bei der Abbildung auf den Wafer verkleinert, wird die „Maske“ als Retikel bezeichnet. Der Ausdruck „Maske“ bezeichnet jedoch auch den Dateninhalt des ROMs bei → <i>Chipkarten-Mikrocontrollern</i> und ist in manchen Fällen sogar das Synonym für das ganze → <i>Chipkarten-Betriebssystem</i> (→ <i>Softmaske, Hardmaske</i>).
Round-trip Engineering	Hier wird innerhalb des Software-Entwicklungsprozesses sequentiell an Design und Implementierung gearbeitet, wobei sich beide Tätigkeiten gegenseitig beeinflussen. Die Software-Architektur und der Programmcode werden durch ein Programm automatisch konsistent zueinander gehalten. Die Grundlage bildet dabei eine formale Modellierungssprache (z. B. UML), aus der dann durch automatische Programmcodegenerierung zumindest ein Rumpfcodes des Programms erstellt wird. Die Erkenntnisse und Änderungen, die durch Verfeinerung und Test dieses Programmcodes gewonnen werden, fließen dann in einem Reverse Engineering Prozess wieder in die Modellierung des Programms zurück. Bei mehrmaligem Durchlaufen der Schleife Codegenerierung-Reverse Engineering erhält man in relativ kurzer Zeit praxisbezogene Software mit einer zum Sourcecode konsistenten Architektur. Angewandt wird das Round-trip Engineering fast ausschließlich bei objektorientierten Programmiersprachen (z. B. C++, Java) in Verbindung mit UML.
RSA (Ronald L. Rivest, Adi Shamir, Leonard Adleman)	Bekanntester und meistverbreiteter asymmetrische kryptografische Algorithmus (→ <i>Kryptoalgorithmus</i>). Er wurde von Ronald L. Rivest, Adi Shamir und Leonard Adleman im Jahr 1978 publiziert und ist nach den Anfangsbuchstaben der drei Familiennamen benannt. Das sehr einfache Funktionsprinzip basiert auf der Arithmetik großer Ganzzahlen. ⁴¹
R-UIM (<i>removable user identity module</i>)	Übliche Bezeichnung für die GSM-spezifische Chipkarte. Sie ist ein optionales Sicherheitsmodul, das sich austauschbar in mobilen Endgeräten des Mobilfunksystems CDMA 2000 befindet. Die R-UIM hat eine ähnliche Funktionalität wie die → <i>SIM</i> , jedoch mit dem Kryptoalgorithmus CAVE (<i>cellular authentication, voice privacy and encryption</i>), der für eine Vielzahl von kryptografisch gesicherten Funktionen in der R-UIM eingesetzt wird. Angelehnt an das SIM Application Toolkit, ist für die R-UIM auch ein UIM Application Toolkit (UATK) spezifiziert.
salt	Zufallssequenz, die zur Verlängerung von Passwörtern verwendet wird, um Wörterbuchangriffe auf die gespeicherten Passwörter zu erschweren.
SAM (<i>secure application module</i>)	→ <i>Sicherheitsmodul</i>
Sammelbeauftragter	→ <i>Acquirer</i>
Sandbox (<i>sandbox</i>)	→ <i>Virtual Machine</i>
Schlechtfall (<i>bad case</i>)	Der Fall bei einer logischen Entscheidung, der zum ungünstigeren oder ungewollten Ergebnis führt.
Schlüssel (<i>key</i>)	Bezeichnet bei einem → <i>Kryptoalgorithmus</i> denjenigen Parameter, der die Ver- oder Entschlüsselung individualisiert. Schlüssel müssen im Falle von symmetrischen Kryptoalgorithmen zur Gewährleistung der Sicherheit ein Geheimnis sein oder dürfen bei asymmetrischen Kryptoalgorithmen im Falle eines öffentlichen Schlüssels auch bekannt sein.
Schlüsselmanagement (<i>key management</i>)	Alle Verwaltungsfunktionen für die Erzeugung, Verteilung, Speicherung, Aktualisierung, Vernichtung und Adressierung von kryptografischen Schlüsseln.
SCOPE (<i>smart card open platform environment</i>)	Die Spezifikation einer Art → <i>HAL (hardware abstraction layer)</i> von → <i>Global Platform</i> .
Scrambling	Vermischte Anordnung der Busse (Adress-, Daten- und Steuerbus) auf dem Chip eines Mikrocontrollern, so dass eine Zuordnung nach Funktionen ohne Hintergrundinformationen nicht mehr möglich ist. Statisches Scrambling bedeutet, dass die Busse einer Serie von Mikrocontrollern identisch gescrambelt sind. Beim dynamischen Scrambling sind die Busse chipindividuell oder sogar sit-

⁴¹ Siehe auch Abschnitt 4.7.2 „Asymmetrische Kryptoalgorithmen“.

	zungsindividuell gescrembelt. ⁴²
Scratch-Karte (<i>scratch card</i>)	Karte im üblichen → <i>ID-1-Format</i> , jedoch mit geringerer Kartendicke, die mit einer Geheimzahl oder einem Passwort unter einer abkratzbaren und undurchsichtigen Deckschicht bedruckt ist. Diese Schicht wirkt als Siegel, so dass die Unversehrtheit vor Benutzung visuell geprüft werden kann. Eine Scratch-Karte verfügt somit über eine ähnliche Funktionalität wie ein PIN-Brief. Scratch-Karten werden oft als Voucher zur Verteilung von Einmalpasswörtern zum Wiederaufladen von → <i>prepaid SIMs</i> benutzt.
SDMA (<i>space division multiple access</i> – Raumvielfachzugriff)	Vielfachzugriffsverfahren zur parallelen Datenübertragung von mehreren Sendern zu einem Empfänger auf einer Frequenz. Dazu verwenden die Sender richtungsselektive Antennen, die auf den jeweiligen Empfänger ausgerichtet werden. Dies lässt sich aufgrund des hohen Aufwandes im Mobilfunkbereich nur bei den Basisstationen, beispielsweise mit Antennenarrays (adaptive Antennen), realisieren. ⁴³
SECCOS (<i>security card operating system</i>)	Name des Multiapplication-Chipkarten-Betriebssystems (→ <i>Chipkarten-Betriebssystem</i>) für die deutsche ec-Karte mit Chip bzw. → <i>Geldkarte</i> .
Secret-Key-Algorithmus	→ <i>Kryptoalgorithmus</i>
Secure Messaging	Alle Mechanismen, Protokolle und Kryptoalgorithmen, um die Datenübertragung von und zu einer → <i>Chipkarte</i> gegen Manipulationen oder Abhören zu schützen. ⁴⁴
Security Environment (SE, Sicherheitsumgebung)	Bezeichnet bei einer Chipkarte einen logischer Container, der eine Menge von vollständig definierten Sicherheitsmechanismen enthält, die von sicherheitsrelevanten → <i>Kommandos</i> und → <i>Secure Messaging</i> benutzt werden. Security Environments eignen sich beispielsweise sehr gut für die sicherheitstechnische Absicherung der unterschiedlichen Lebenszyklen (siehe auch Lebenszyklus) einer Chipkarte. Im einfachsten Fall würde man in diesem Beispiel für Personalisierung und späteren Betrieb unterschiedliche Security Environments definieren, sodass die → <i>Zugriffsbedingungen</i> auf die Dateien je nach Lebensabschnitt der Chipkarte unterschiedlich festgelegt sind. Im Falle der Personalisierung dürfte man dann auf alle Dateien schreibend zugreifen, und im Falle des Betriebs wären die Zugriffsbedingungen entsprechend der eigentlichen → <i>Anwendung</i> gesetzt.
Security Target (Sicherheitsvorgabe)	Die Sicherheitsvorgaben beschreiben im Rahmen einer → <i>Evaluierung</i> die zu prüfenden Mechanismen beim → <i>Target of Evaluation</i> . Sie sind damit eine Art Anforderungskatalog für die Evaluierung. Die Sicherheitsvorgaben für bestimmte Arten und Anwendungsgebiete von Targets of Evaluation können in → <i>Protection Profiles</i> beschrieben sein.
seed number (Initialzahl)	Auch <i>seed</i> ; der aus einer Zufallszahl bestehende Startwert für Pseudozufallszahlengeneratoren.
Seitenorientierung	Zusammenfassung von mehreren Bytes in einem Speicher, die nur als Ganzes geschrieben oder gelöscht werden können. Eine Seitenorientierung gibt es bei → <i>Chipkarten-Mikrocontrollern</i> nur für Speicher des Typs EEPROM oder Flash-EEPROM. Typische Größen von Speicherseiten sind 4 Byte, 32 Byte, 64 Byte und 128 Byte. Allerdings gibt es mittlerweile auch Mikrocontroller, die keine fixe Seitenorientierung mehr haben, sondern eine Variable in einem bestimmten Bereich, z. B. 1 Byte bis 128 Byte.
serielle Datenübertragung	Hier werden die einzelnen Datenbits nacheinander auf einer Datenleitung übertragen (→ <i>parallele Datenübertragung</i>).
SET (<i>secure electronic transaction standard</i>)	Zahlungsverkehrsprotokoll zur Abwicklung von sicheren Kreditkartenzahlungen im Internet. Es wurde von Visa und Mastercard 1996 veröffentlicht. SET verlangt beim Bezahler nicht zwangsläufig eine Chipkarte, sondern kann dort vollständig in Software auf dem PC realisiert sein. Eine Erweiterung von SET namens C-SET (Chip-SET) ist bislang nur in Frankreich von Relevanz und nicht international standardisiert.
shall, should, may	In internationalen Normen kommen diese drei englischsprachigen Hilfsverben normalerweise in vielen Bereichen vor. Ihre Bedeutung ist genau geregelt und weicht daher teilweise vom verbreiteten laxen umgangssprachlichen Gebrauch dieser Wörter ab. „Shall“ bedeutet, dass der bezeichnete Sachverhalt entsprechend der Beschreibung verpflichtend realisiert werden muss. „Should“ hingegen entspricht nur im Ansatz einer Empfehlung, da das Beschriebene wenn irgendwie möglich erfüllt werden muss. Eine echte Entscheidungsmöglichkeit bei

⁴² Siehe auch Abschnitt 8.2.4.1 „Angriffe auf der physikalischen Ebene“.

⁴³ Siehe auch Abschnitt 13.1.1 „Vielfachzugriffsverfahren“.

⁴⁴ Siehe auch Abschnitt 6.6 „Sicherung der Datenübertragung“.

	der Realisierung ist nur bei „may“ gegeben.
Short-FID (<i>SFI</i>)	5 Bit langes Kennzeichen für EFs und hat den Wertebereich 1 bis 31. Es wird zur impliziten Selektion eines EFs innerhalb eines Schreib- oder Lesekommandos (z. B. READ BINARY) an die Chipkarte benutzt. ⁴⁵
Shrink	Bezeichnet die Flächenreduzierung eines Halbleiterchips durch Verwendung einer Halbleitertechnologie mit kleinerer Strukturbreite. Auf Grund des reduzierten Flächenbedarfs können pro Wafer mehr Halbleiterchips untergebracht werden. Dies reduziert wiederum die Kosten der Halbleiterchips, da der Chip-Preis annähernd proportional zum Platzbedarf auf dem Wafer ist.
Shutter	Mechanische Vorrichtung in Terminals, die gegebenenfalls alle von der Chipkarte aus dem Terminal führenden Drähte abschneidet. Damit soll eine Manipulation der Kommunikation verhindert werden. Falls ein Abschneiden nicht möglich ist, wird die gesteckte Chipkarte elektrisch nicht aktiviert.
Sicherheitsmodul	Ein sowohl mechanisch als auch informationstechnisch abgesichertes Bauteil, das zur Aufbewahrung von geheimen Daten und zur Ausführung von Kryptoprogrammen dient. Andere Namen für Sicherheitsmodul sind SAM (<i>secure application module</i>) und HSM (<i>hardware security module</i> oder <i>host security module</i>).
Signalburst	Oft auch kurz Burst genannt; ein zusammenhängendes Datenpaket, das über die Luftschnittstelle zwischen Feststation und Mobilstation übertragen wird.
Signaturgesetz (SigG)	Im Allgemeinen ein Gesetz, das den Gebrauch und Einsatz von → <i>digitalen Signaturen</i> regelt. In Deutschland versteht man darunter das „Gesetz über Rahmenbedingungen für elektronische Signaturen“ vom 22. Mai 2001. Darin ist der Rahmen für den Einsatz von digitalen Signaturen in Deutschland vorgegeben, ⁴⁶ welche in der → <i>Signaturverordnung</i> konkretisiert werden.
Signaturkarte (<i>signature card</i>)	→ <i>Chipkarte</i> mit → <i>Mikrocontroller</i> , deren Hauptaufgabe die sichere Aufbewahrung und Nutzung von geheimen Schlüsseln für → <i>digitale Signaturen</i> ist.
Signaturverordnung (SigV)	In der deutschen Signaturverordnung vom 8. Oktober 1997 werden die Rahmenbedingungen, die vom → <i>Signaturgesetz</i> vorgegeben sind, so weit konkretisiert, dass darauf aufbauend konkrete Maßnahmenkataloge als Vorschläge zur praktischen Anwendung von digitalen Signaturen erstellt werden können. Die Signaturverordnung beschreibt beispielsweise die notwendigen Verfahren für die Erzeugung von Signaturschlüsseln und Identifikationsdaten sowie notwendige Sicherheitskonzepte und die notwendigen Prüfstufen nach ITSEC für die Signaturkomponenten. ⁴⁷
SIM (<i>subscriber identity module</i>)	Übliche Bezeichnung für die GSM-spezifische Chipkarte. ⁴⁸ Sie ist ein obligatorisches Sicherheitsmodul, das sich austauschbar in mobilen Endgeräten des GSM-Mobilfunksystems befindet. Sie kann die herkömmliche Kreditkartengröße ID-1 haben oder auch als kleine Plug-In-Karte in ID-000 ausgeführt sein. Das SIM ist der Träger der Identität des Teilnehmers und hat als Hauptaufgabe die Sicherstellung der Echtheit der Mobilstation gegenüber dem Netzwerk. Zusätzliche Aufgaben sind die manipulationssichere Ausführung von Programmen (Authentisierung), die Benutzeridentifizierung (mittels PIN) und die Speicherung von Daten, wie beispielsweise Telefonnummern. Das Äquivalent des SIM bei UMTS ist das → <i>USIM</i> . ⁴⁹
SIM Alliance [SIM Alliance]	Ein im Jahr 1999 von Gemplus, G + D, ORGA und Schlumberger gegründetes Konsortium, um Dienstleistungen, die für WAP entwickelt wurden, auch auf nicht WAP-fähigen Mobiltelefonen zu ermöglichen. Dazu muss die SIM über einen SIM Alliance-fähigen Browser verfügen und das Mobiltelefon die Phase 2+ von GSM unterstützen. Damit ist die → <i>SIM</i> fähig, das Mobiltelefon über → <i>SIM Application Toolkit</i> so weit zu steuern, dass darauf ein Großteil von WAP-Inhalten und deren Funktionalität abgebildet werden kann. ⁵⁰
SIM Application Toolkit (SAT, unüblich und veraltet STK)	Baukastenähnliche Erweiterung der GSM 11.11-Spezifikation (genormt in GSM 11.14), die es der SIM-Karte erlaubt, eine aktive Rolle bei der Steuerung des Mobiltelefons zu übernehmen. Mit dem SIM Application Toolkit ist es bei-

⁴⁵ Siehe auch Abschnitt 5.6.2 „Dateinamen“.

⁴⁶ Siehe auch Abschnitt 14.4 „Digitale Signatur“.

⁴⁷ Siehe auch Abschnitt 14.4 „Digitale Signatur“.

⁴⁸ Siehe auch Abschnitt 13.2 „Das GSM-System“.

⁴⁹ Siehe auch Abschnitt 13.3 „Das UMTS-System“.

⁵⁰ Siehe auch Abschnitt 13.5 „Die WIM“.

	<p>spielsweise einer SIM möglich, Anzeigen auf dem Display auszugeben, Eingaben über die Tastatur anzufordern und Nachrichten über die Luftschnittstelle zu senden und zu empfangen. Das SIM Application Toolkit ist die Grundlage für die meisten Zusatzanwendungen bei Mobiltelefonen. Das Äquivalent des SIM Application Toolkit bei UMTS ist das → <i>USIM Application Toolkit</i> (USAT),⁵¹ und bei der → <i>R-UIM</i> ist es das UATK (UIM Application Toolkit). Die von der Expertengruppe → <i>EP SCP</i> definierte zukünftige generische Grundlage für alle Application Toolkits von Chipkarten im Mobilfunk wird das CAT (<i>card application toolkit</i>) sein.</p>
SIM Lock (SIM Sperre)	<p>Verfahren, das Mobiltelefone fest mit einer bestimmten → <i>Chipkarte</i>, d. h. einem → <i>SIM</i>, verbindet. Dazu liest entweder das Mobiltelefon aus der <i>SIM</i> bestimmte Daten aus und vergleicht diese mit im Mobiltelefon gespeicherten Daten oder das <i>SIM</i> liest eindeutige Daten aus dem Mobiltelefon und vergleicht diese mit gespeicherten Daten. Sind die Daten gleich, dann kann das Mobiltelefon benutzt werden. Es ist in der Regel möglich, entweder über die Luftschnittstelle oder durch Eingabe eines geheimen Schlüssels am Mobiltelefon, die <i>SIM-Lock-Funktion</i> abzuschalten, so dass anschließend auch andere <i>Chipkarten</i> verwendet werden können. Die <i>SIM-Lock-Funktion</i> wird benutzt, um vom Netzbetreiber subventionierte Mobiltelefone für eine gewisse Zeit an eine bestimmte <i>Chipkarte</i> und deren Bezahlmodalität (→ <i>prepaid</i>) zu binden.⁵²</p>
SIM Toolkit	<p>Kurzform von → <i>SIM Application Toolkit</i>.</p>
SIMEG (<i>subscriber identity module expert group</i>)	<p>Die SIMEG war eine 1988 gegründete Expertengruppe, die im Rahmen von → <i>ETSI</i> die Spezifikation für die Schnittstelle zwischen <i>Chipkarte</i> und Mobiltelefon festgelegt hat (GSM 11.11). Der Name SIMEG wurde 1994 in → <i>SMG9</i> geändert.</p>
Simulator (<i>simulator</i>)	<p>Software, die die Funktionsweise eines Geräts (des Zielsystems) nachahmt. Die Nachahmung mittels Hardware bezeichnet man hingegen als → <i>Emulator</i>. Simulatoren werden oft zur Entwicklung von Software für noch nicht existierende Zielsysteme eingesetzt. Ein <i>Chipkarten-Simulator</i> ist beispielsweise eine Software, die eine echte <i>Chipkarte</i> auf logischer Ebene vollständig nachbildet. Simulatoren sind in der Regel langsamer als Emulatoren, d. h. sie simulieren oft nicht in Echtzeit.</p>
Single-Sign-On (SSO, Einfachanmeldung)	<p>Hierbei werden mehrere unterschiedliche Benutzeridentifizierungen für verschiedene Anwendungen durch eine einzelne zentrale Benutzeridentifizierung ersetzt. Realisiert wird dies durch eine Software, die aufgrund der korrekten zentralen Benutzeridentifizierung die entsprechenden Identifizierungsnamen (→ <i>Identifizierung</i>) und Passwörter an die zugehörigen Identifizierungsinstanzen sendet. Damit entfällt für den Benutzer die Notwendigkeit, sich viele verschiedene Passwörter zu merken.</p>
Sitzung (<i>session</i>)	<p>Zeitspanne zwischen An- und Abschaltsequenz einer <i>Chipkarte</i>, in der sowohl der gesamte Datenaustausch als auch die dazu notwendigen informationstechnischen Mechanismen ablaufen.</p>
skimming	<p>Typischer Angriff bei Magnetstreifenkarten. Dazu werden die Daten des Magnetstreifens von einer fremden Magnetstreifenkarte unerlaubterweise gelesen und auf den Magnetstreifen einer Blankokarte kopiert. Diese Karte kann nun bezüglich des Magnetstreifens wie die Originalkarte verwendet werden.</p>
Skript (<i>script</i>)	<p>Interpretiertes Programm hauptsächlich zur Realisierung von einfachen kurzen Anwendungen und zur Automatisierung von immer wiederkehrenden Abläufen.</p>
Smart Card	<p>Anderer Ausdruck für Mikroprozessorkarte. Er steht für eine <i>Chipkarte</i>, die „smart“, also schlau ist, weshalb Speicherkarten nicht mehr unter diesen Überbegriff fallen.</p>
Smart Label	<p>Datenträger in dünner Bauform, mit denen mittels kontaktloser Datenübertragung kommuniziert werden kann. Dabei können in der einfachsten Variante (oft auch ohne Chip) Daten lediglich vom Smart Label gelesen werden. Höher entwickelte Varianten von Smart Labels ermöglichen es, auch Daten zu schreiben bzw. Daten analog einer → <i>Chipkarte</i> im Smart Label zu verarbeiten.</p>
Smart Object	<p>→ <i>Chipkarten-Mikrocontroller</i>, verpackt in einer zur üblichen Kartenform alternativen Bauform. Beispiele für Smart Objects sind USB-Stecker oder Ringe, die mit einem <i>Chipkarten-Mikrocontroller</i> ausgerüstet sind.</p>
Smartcard [Groupmark]	<p>Dieser Begriff ist ein eingetragenes Warenzeichen der kanadischen Firma Groupmark.</p>

⁵¹ Siehe auch Abschnitt 13.3 „Das UMTS-System“.

⁵² Siehe auch Abschnitt 13.2 „Das GSM-System“.

SMG9 (<i>special mobile group 9</i>)	Die SMG9 war eine Expertengruppe, die im Rahmen von → <i>ETSI</i> die Spezifikation für die Schnittstelle zwischen Chipkarte und Mobiltelefon festgelegt hat (z. B.: GSM 11.11, GSM 11.14, ...). Sie setzte sich aus Vertretern von Karten-, Mobiltelefonherstellern und Netzbetreibern zusammen. Der frühere Name der SMG9 war → <i>SIMEG</i> . Im Jahr 2000 wurde die SMG9 aufgelöst und die Aufgaben auf zwei neue Expertengruppen verteilt. Für die applikationsspezifische Schnittstelle Mobiltelefon zu → <i>SIM</i> bzw. → <i>USIM</i> ist die 3GPP Expertengruppe T3 verantwortlich und alle generischen Themen im Bereich von Chipkarten im Bereich der Telekommunikation werden von der ETSI-Expertengruppe EP SCP (<i>ETSI project smart card platform</i>) bearbeitet.
SMS (<i>short message service</i> , Kurzmitteilungsdienst)	Kurzmitteilungsdienst von GSM mit einer maximalen Nachrichtenlänge von 160 alphanumerischen Zeichen. SMS-Nachrichten werden über den Signalisierungskanal und nicht über den Datenkanal übertragen, d. h. sie können auch während eines aktiven Telefonats gesendet und empfangen werden. Der SMS-Dienst wird nicht nur zur Übermittlung von Kurznachrichten für die Teilnehmer verwendet, sondern auch als → <i>Bearer</i> -Dienst zur Übertragung von Daten an das Mobiltelefon beispielsweise bei → <i>WAP</i> oder an die SIM (→ <i>OTA</i>).
Softmaske (<i>soft mask</i>)	Dieser Begriff bedeutet, dass sich, aufbauend auf einem → <i>Chipkarten-Betriebssystem</i> , im ROM ein Teil des Programmcodes im EEPROM befindet (→ <i>ROM-Maske</i>). Programme im EEPROM lassen sich durch Überschreiben leicht ändern, sind also „soft“. Der Ausdruck „Maske“ ist in diesem Zusammenhang eigentlich falsch, da man für ein Programm im EEPROM keine halbleitertechnische Belichtungsmaske erstellen muss. Softmasken werden üblicherweise nicht für große Stückzahlen (z. B. für Feldversuche) bei → <i>rapid prototyping</i> oder für Erweiterungen verwendet. Das Gegenteil einer Softmaske ist die → <i>Hardmaske</i> , bei der die wesentlichen Funktionen Teile des ROMs sind.
SPA (<i>simple power analysis</i>)	Die einfache Leistungsanalyse ist eine Angriffsmethode auf Chipkarten, bei der mit hoher zeitlicher Auflösung der Stromverbrauch eines Mikrocontrollers gemessen wird. Aufgrund des Stromverbrauchs kann auf die internen Abläufe und verarbeiteten Daten des Mikrocontrollers geschlossen werden. Bekannt wurde die SPA durch eine Veröffentlichung von Paul Kocher, Joshua Jaffe und Benjamin Jun im Juni 1998 [Kocher 98] (→ <i>DPA</i>). ⁵³
SPA/DPA-resistent	Eigenschaft eines Kryptoalgorithmus, dass der benutzte geheime Schlüssel nicht durch eine → <i>SPA</i> - bzw. → <i>DPA</i> -Analyse herausgefunden werden kann.
Speicherkarte (<i>memory card</i>)	Karte mit Chip, der eine einfache Logikschaltung mit zusätzlichem Schreib- und lesbaren Speicher besitzt. Speicherkarten können zusätzlich noch Sicherheitsbaugruppen aufweisen, die beispielsweise eine Authentisierung ermöglichen.
Sperrliste (<i>blacklist</i>)	Liste in einer Datenbank, auf der alle Chipkarten oder Geräte vermerkt sind, die in einer bestimmten → <i>Anwendung</i> nicht mehr verwendet werden dürfen (→ <i>Hotlist</i> , <i>Greylist</i> , <i>Whitelist</i>).
Spezifikation (<i>specification</i>)	Eindeutige, vollständige und redundanzfreie Beschreibung einer Software. Ihr Inhalt darf keine auslegungsfähigen Teile enthalten und muss von allen Lesergruppen mit unterschiedlicher Funktion (Entwickler, Tester, Qualitätssicherer, ...) in vertretbarer Zeit verstanden werden können.
SRAM (<i>static random access memory</i>)	RAM-Speicher in statischer Bauweise, der zum Erhalt des Speicherinhalts lediglich eine konstante Stromversorgung und keine zyklische Wiederauffrischung des Inhalts benötigt. Die Zugriffszeit auf SRAM-Speicher ist geringer als auf DRAM-Speicher, allerdings benötigen SRAMs mehr Platz auf dem Chip und sind deshalb auch teurer. ⁵⁴
Stack	Datenstruktur, in der die zuletzt abgelegten Objekte als Erste wieder entfernt werden können (<i>last in first out</i> – LIFO). Der wohl bekannteste Stack ist der Programmstack, auf dem beim Aufruf von Unterprogrammen die Rücksprungadressen abgelegt werden.
Standard	Damit werden in diesem Buch und in der Regel alle normungsähnlichen Dokumente bezeichnet, die beispielsweise von Firmen oder im industriellen Umfeld publiziert werden und nicht von einem nationalen oder internationalen Normungsgremium erstellt bzw. veröffentlicht worden sind (→ <i>Norm</i>). Verwirrenderweise werden in Deutschland die beiden Begriffe Norm und Standard oft gleichwertig verwendet, was streng genommen nicht korrekt ist.
STARCOS	Markenname eines Multiapplication-Chipkarten-Betriebssystems (→ <i>Chipkar-</i>

⁵³ Siehe auch Abschnitt 8.2.4.1 „Angriffe auf der physikalischen Ebene“.

⁵⁴ Siehe auch Abschnitt 3.4.2 „Speicherarten“.

	<i>ten-Betriebssystem</i>) von Giesecke und Devrient [GD], das seit 1991 in verschiedenen Version erhältlich ist.
Steganografie	Zweck der Steganografie ist es, Nachrichten in anderen Nachrichten so zu verbergen, dass sie von einem unbedarften Beobachter (Mensch oder Maschine) nicht mehr erkannt werden können. Beispielsweise könnte ein Text codiert und in einer Bilddatei versteckt werden, so dass das betreffende Bild sich nur geringfügig ändert, und deshalb die Bildmodifikation praktisch nicht mehr wahrnehmbar ist (→ <i>digitales Wasserzeichen</i>). Mit einem entsprechenden Analyseprogramm könnte man jedoch den in der Bilddatei versteckten Text zu einem späteren Zeitpunkt wiederherstellen und so beispielsweise einen Copyright-Vermerk wieder zum Vorschein bringen.
Super Smart Card	Chipkarte mit integrierten aufwändigen Kartenelementen wie Display und Tastatur. Seit einigen Jahren hat sich jedoch anstelle von Super Smart Card der Begriff → <i>System-on-Card</i> eingebürgert.
symmetrischer Kryptoalgorithmus	→ <i>Kryptoalgorithmus</i>
synchrone Datenübertragung	Hier werden die Daten abhängig von einem fest vorgegebenen Zeitraster übertragen. Das Zeitraster kann beispielsweise von der an dem Chip angelegten Taktfrequenz abgeleitet sein (→ <i>asynchrone Datenübertragung</i>).
System-on-Card	Bezeichnet in der Chipkartenwelt eine um zusätzliche Kartenelemente neben dem Chipmodul erweiterte Chipkarte. Die üblicherweise aufgeführten Kartenelemente sind Display, Stromversorgung (Batterie, Solarzellen), Tastatur, Antenne, Sensoren für biometrische Benutzeridentifizierung (z. B. Fingerabdruck) und Lautsprecher. Die Ansteuerung dieser Kartenelemente kann vom Chip im Modul aus geschehen, muss aber nicht. Ein anderer, mittlerweile jedoch seltener benutzter Begriff für System-on-Card ist Super-Smart-Card.
T = 0	Dieses Übertragungsprotokoll regelt die Datenübertragung zwischen Terminal und Chipkarte und war das erste international genormte Übertragungsprotokoll für Chipkarten. Es ist ein byteorientiertes Halbduplex-Protokoll, das asynchron betrieben wird, und ist für minimalen Speicherbedarf und maximale Einfachheit ausgelegt. Dieses Protokoll wird weltweit in der GSM-Karte verwendet und hat deshalb den größten Verbreitungsgrad aller Chipkarten-Protokolle. Genormt ist T = 0 in ISO/ IEC 7816-3, dazu kompatible Spezifikationen sind in der GSM 11.11, TS 102.221 und dem EMV-Standard enthalten.
T = 1	Dieses Übertragungsprotokoll regelt die Datenübertragung zwischen Terminal und Chipkarte. Es ist ein blockorientiertes Halbduplex-Protokoll, das asynchron betrieben wird, und bietet eine Trennung zwischen Datenübertragung und → <i>Anwendung</i> . Genormt ist T = 1 in ISO/ IEC 7816-3, dazu kompatible Spezifikationen sind in TS 102.221 und dem EMV-Standard enthalten.
T3	→ <i>SMG9</i>
Tag (engl.)	Kennzeichnung für Datenobjekte, die unter anderem vor allem bei ASN.1-Codierungen zum Einsatz kommt. ⁵⁵
tape out	Zeitpunkt, an dem das Chipdesign fertiggestellt ist und die dabei erzeugten Daten an die Maskenherstellung (→ <i>ROM-Maske</i>) überführt werden. Dies ist ein wichtiger Meilenstein bei der Chipherstellung. Der Begriff rührt daher, dass früher die Maskendaten auf Magnetbändern (tape) übergeben (out) wurden.
Target of Evaluation (TOE)	Das zu evaluierende informationstechnische System (→ <i>Evaluierung</i>), d. h. das zu prüfende Objekt. Ein TOE kann beispielsweise eine Mikrocontroller-Chipkarte (→ <i>Chipkarten-Mikrocontroller</i>) mit integrierter Software sein, die bestimmte Sicherheitsvorgaben, die → <i>Security Targets</i> , erfüllen muss.
TCSEC (<i>trusted computer system evaluation criteria</i>)	Kriterienkatalog zur Entwicklung und → <i>Evaluierung</i> der Sicherheit von informationstechnischen Systemen im US-amerikanischen Bereich und wurden 1983 vom National Computer Security Center → <i>NCSC</i> veröffentlicht. Der Nachfolger der nationalen TCSEC sind die international gültigen Common Criteria (→ <i>CC</i>).
TD/CDMA (<i>time division/code division multiple access</i>)	→ <i>CDMA</i>
TDES	anderer Ausdruck für → <i>Triple-DES</i>
TDMA (<i>time division multiple access</i> –	Vielfachzugriffsverfahren zur quasi parallelen Datenübertragung von mehreren Sendern zu einem Empfänger auf einer Frequenz. Dazu erhält jeder Sender ei-

⁵⁵ Siehe auch Abschnitt 4.1 „Strukturierung von Daten“.

Zeitvielfachzugriff)	nen bestimmten Zeitschlitz, in dem er exklusiv senden darf, was eine sehr genaue Synchronisation erfordert. TDMA wird in Verbindung mit FDMA bei GSM auf der Luftschnittstelle zwischen Mobiltelefon und Basisstation benutzt. ⁵⁶
Teiler	In der Chipkartenwelt die gebräuchliche Kurzform von <i>clock rate conversion factor</i> (CRCF). Der CRCF gibt die Dauer eines Bits bei der Datenübertragung in der Anzahl der Takte auf der Clock-Leitung an.
Terminal (<i>terminal</i>)	Das Gegenstück zur Chipkarte ist das (Chipkarten-)Terminal. Es ist ein Gerät, z. T. mit Tastatur und Display, das die elektrische Versorgung und den Datenaustausch mit der Chipkarte ermöglicht. Nach ISO ist die normgerechte Bezeichnung für ein Chipkarten-Terminal IFD (<i>interface device</i>) und im Zahlungsverkehr ist die übliche Bezeichnung für ein Terminal CAD (<i>card accepting device</i>).
Test (<i>test</i>)	Hier wird ein bereits gedebugtes Programm in systematischer Vorgehensweise auf seine Funktionsfähigkeit und die Erfüllung der bei der → <i>Analyse</i> ermittelten Anforderungen geprüft. Das vorrangige Ziel ist nicht die Suche nach Fehlern im Programm, sondern die Prüfung der geforderten Funktionen. Das Testing ist deshalb nicht identisch mit dem → <i>Debugging</i> .
TETRA (<i>terrestrial trunked radio</i> , früher: <i>trans european trunked radio</i>)	Spezifikation für ein digitales Bündelfunksystem im 380 MHz bis 420 MHz Bereich mit → <i>TDMA</i> -Vielfachzugriff und wird von → <i>ETSI</i> herausgegeben. Zur Teilnehmeridentifikation ist bei TETRA analog → <i>GSM</i> eine → <i>SIM</i> vorgesehen, die üblicherweise TETRA-SIM genannt wird. Die TETRA-SIM ist jedoch optional, kann also auch als Software in der Mobilstation realisiert werden.
TETRA-SIM	→ <i>TETRA</i>
Thread	→ <i>Multithreading</i>
TLV-Format	Umgangssprachlicher Ausdruck für → <i>BER</i> -codierte Datenobjekte nach → <i>ASN.1</i> , bei dem ein Datum (<i>value</i>) durch ein vorangestelltes Kennzeichen (<i>tag</i>) und die Länge (<i>length</i>) eindeutig beschrieben wird.
TPDU	→ <i>APDU</i>
Transaktion (<i>transaction</i>)	Aufeinanderfolgender Ablauf von mehreren zusammengehörigen → <i>Kommandos</i> zu einer Chipkarte, um eine bestimmte Aufgabe zu erledigen. Ein typisches Beispiel für eine Transaktion sind die Kommandos für das Laden einer elektronischen Geldbörse.
Transaktionsnummer (TAN) (<i>transaction number</i>)	Eine TAN ist im Gegensatz zu einer PIN nur für eine einzige Transaktion gültig und kann deshalb nur einmal verwendet werden. Üblicherweise erhält man mehrere TANs in Form einer Tabelle mit fünfstelligen Zahlen, ausgedruckt auf Papier, die dann exakt in der vorgegebenen Reihenfolge für die einzelnen Transaktionen bzw. Sitzungen benutzt werden müssen.
Transferkarte (<i>transfer card</i>)	→ <i>Chipkarte</i> , die als Transportmedium zwischen zwei Instanzen genutzt wird. Dazu besitzt sie einen großen Datenspeicher und in der Regel Schlüssel für eine Authentisierung, die prüft, ob die zu transferierenden Daten von der jeweiligen Stelle gelesen bzw. geschrieben werden dürfen.
Transistenz (<i>transient</i>)	Fähigkeit eines Objekts, nur während der Ausführungszeit eines Prozesses zu existieren; das Gegenteil ist die → <i>Persistenz</i> .
Transportprotokoll	Unüblicher Ausdruck für → <i>Übertragungsprotokoll</i> .
trapdoor (Falltür)	Eine in eine Software bewusst eingebaute Möglichkeit, unter Umgehung von Sicherungsmaßnahmen auf Daten und Programme eines Systems zuzugreifen.
Triple-Band-Mobiltelefon	Mobiltelefon, das in drei Frequenzbändern (z. B. GSM 900, GSM 1800, und GSM 1900) arbeiten kann.
Triple-DES	auch TDES und 3 DES genannt; eine modifizierte DES-Verschlüsselung durch aufeinander folgenden dreifachen Aufruf des DES-Algorithmus mit abwechselnder Ver- und Entschlüsselung. Wird für die drei DES-Aufrufe der gleiche Schlüssel verwendet, entspricht die Triple-DES-Verschlüsselung einer normalen DES-Verschlüsselung. Werden hingegen zwei bzw. drei unterschiedliche Schlüssel verwendet, dann stärkt dies die DES-Verschlüsselung erheblich gegenüber einer einfachen DES-Verschlüsselung. ⁵⁷

⁵⁶ Siehe auch Abschnitt 13.1.1 „Vielfachzugriffsverfahren“.

⁵⁷ Siehe auch Abschnitt 4.7.1 „Symmetrische Kryptoalgorithmen“.

Trivial-PIN	Leicht zu erratende → <i>PIN</i> , wie beispielsweise "1234" (→ <i>0-PIN</i>).
trojanisches Pferd	Historisch gesehen das Holzpferd, mit dem es Odysseus gelang, sich Zugang zur stark befestigten Stadt Troja zu verschaffen. In der modernen Fassung ein Programm, das vordergründig eine definierte Aufgabe erfüllt, doch zusätzliche und unbekannt Funktionen ausführen kann. Es wird bewusst in ein Computersystem oder Wirtsprogramm eingebracht und kann sich im Gegensatz zu Viren nicht vermehren.
Trustcenter (<i>trust center</i> – TC)	Neben der → <i>Signaturkarte</i> das wesentliche Element bei einer → <i>PKI</i> . Es ist die Instanz, die Zertifikate erzeugt, verteilt und verwaltet. Sie übernimmt damit je nach Ausprägung die Aufgaben einer → <i>Zertifizierungsinstanz</i> , einer → <i>Registrierungsinstanz</i> , eines → <i>Verzeichnisdienstes</i> und eines <i>Zeitstempeldienstes</i> (→ <i>Zeitstempel</i>).
Trusted-Third-Party (TTP – vertrauenswürdige dritte Partei)	Instanz, die von zwei oder mehreren anderen Instanzen als vertrauenswürdig anerkannt wird und beispielsweise → <i>Zertifikate</i> herausgibt.
tunneling	Kryptografisch gesicherte → <i>Ende-zu-Ende-Verbindung</i> zweier Instanzen unter Zuhilfenahme von Kommunikationspfaden einer oder mehrerer weiterer Instanzen, die jedoch den Informationsgehalt des eigentlichen Datenaustausches nicht verändern.
UART (<i>universal asynchronous receiver transmitter</i>)	Universell einsetzbarer und unabhängig vom → <i>Mikroprozessor</i> asynchron arbeitender Baustein zum Senden und Empfangen von Daten. Somit ist es nicht mehr notwendig, dass die Kommunikation auf Bit- und Byteebene vom Mikroprozessor erledigt wird. Dies führt zu einer Vereinfachung der Kommunikationsprotokolle und kann auch zur Realisierung von höheren Datenübertragungsgeschwindigkeiten als bei einer reinen Softwarelösung durch den Mikroprozessor benutzt werden. ⁵⁸
Übertragungsprotokoll (<i>transport protocol</i>)	Bezeichnet in der Chipkartenwelt die Mechanismen zum Senden und Empfangen von Daten zwischen Terminal und Chipkarte. Das Übertragungsprotokoll beschreibt im Detail die benutzten OSI-Protokollschichten, den Datenaustausch im Gutfall, Fehlererkennungsmechanismen und Reaktionsmechanismen bei Fehlern. ⁵⁹
UCS (<i>universal character set</i>)	Weiterentwicklung von ASCII und Unicode zur Codierung von Schriftzeichen und ist in der internationalen Norm ISO/IEC 10646 festgelegt. UCS verwendet 32 Bit für die Codierung eines Zeichens, wobei jedoch nur die Hälfte des möglichen Adressraums genutzt wird ($2^{32}/2 = 2\,147\,483\,648$). Mit diesem Adressraum können alle Schriftzeichen in allen Sprachen dieser Welt dargestellt werden. UCS ist so definiert, dass → <i>Unicode</i> eine Untermenge davon darstellt und die Codierung der ersten 128 Zeichen der ASCII-Codierung entspricht. ⁶⁰
UICC (<i>universal integrated chip card</i>)	→ <i>Chipkarte</i> mit einem für Chipkarten-Anwendungen (→ <i>Anwendung</i>) in der Telekommunikation optimierten → <i>Chipkarten-Betriebssystem</i> nach ISO/IEC 7816. Die normative Grundlage für die UICC ist die TS 102.221, die von → <i>ETSI</i> herausgegeben wird. Die UICC ist die Grundlage für die → <i>USIM</i> . Sie kann die herkömmliche Kreditkartengröße ID-1 haben oder auch als kleine Plug-In-Karte in ID-000 ausgeführt sein.
UIM (<i>user identity module</i>)	Veralteter Begriff für → <i>USIM</i> .
UML (<i>unified modeling language</i>) [OMG]	Grafisch orientierte methodenunabhängige Modellierungssprache zur abstrakten Beschreibung statischer und dynamischer Aspekte von objektorientierten Programmen. Die aktuelle Version der UML ist 1.3. Die Grundlagen zur Notation und Semantik von UML wurden in den 90er Jahren von Grady Booch, James Rumbaugh und Ivar Jacobson geschaffen. UML ist unabhängig von einem bestimmten → <i>Vorgehensmodell</i> zur Softwareentwicklung. ⁶¹ Die Object Management Group (OMG) ist verantwortlich für die Weiterentwicklung der UML.
UMTS (<i>universal mobile telecommunication system</i>)	Der europäische Nachfolger von GSM; gehört zur → <i>IMT-2000-Familie</i> . UMTS ist ein digitales, zelluläres, betreiberübergreifendes, länderübergreifendes und bodengebundenes Mobilfunksystem der dritten Generation (→ <i>3G</i>). Der diesem Mobilfunksystem zugewiesene Frequenzbereich liegt bei 2 000 MHz. Das UMTS-System ist durch eine Reihe von Spezifikationen definiert, die unter der Schirm-

⁵⁸ Siehe auch Abschnitt 3.4.3 „Zusatzhardware“.

⁵⁹ Siehe auch Kapitel 6 „Datenübertragung zur Chipkarte“.

⁶⁰ Siehe auch Abschnitt 4.2 „Codierung alphanumerischer Daten“.

⁶¹ Siehe auch Abschnitt 15.7 „Vorgehensmodelle“.

	herrschaft von → <i>3GPP</i> erstellt wurden und deren Herausgeber → <i>ETSI</i> ist. UMTS stellt den nächsten großen Evolutionschritt nach → <i>GSM</i> dar. Die wesentlichen Änderungen gegenüber GSM sind eine neue Luftschnittstelle in → <i>CDMA</i> -Technik und deutlich höhere Datenübertragungsraten von bis zu 2 MBit/s. ⁶²
Unicode [Unicode]	Weiterentwicklung der bekannten ASCII-Codierung von Schriftzeichen. Im Gegensatz zum 7-Bit-ASCII-Code verwendet Unicode 16 Bit für die Codierung. Dies ermöglicht es, die Schriftzeichen der am meisten verbreiteten Sprachen dieser Welt zu unterstützen. Die ersten 256 Zeichen von Unicode sind mit ASCII nach ISO 8859-1 identisch. ⁶³
Uplink	Verbindung von einem untergeordneten System (z. B. Mobiltelefon) zu einem übergeordneten System (z. B. Basisstation). Das Gegenteil ist der → <i>Downlink</i> .
Upload	Übertragen von Daten von einem untergeordneten System (z. B. Terminal) an ein übergeordnetes System (Hintergrundsystem, Host). Das Gegenteil ist der → <i>Download</i> .
URL (<i>uniform resource locator</i>)	Eindeutige alphanumerische Adresse im → <i>WWW</i> .
USIM (<i>universal subscriber identity module</i>)	Übliche Bezeichnung für die Chipkarten-Anwendung (→ <i>Anwendung</i>) für UMTS, ⁶⁴ die auf einer → <i>UICC</i> residiert. In der Praxis wird der Begriff USIM jedoch nicht nur für die Anwendung, sondern auch für die UMTS-Chipkarte verwendet, obwohl dies eigentlich nicht ganz korrekt ist. Die USIM ist der Träger der Identität des Teilnehmers und hat als Hauptaufgabe die Sicherstellung der Echtheit der Mobilstation gegenüber dem Netzwerk und umgekehrt. Zusätzliche Aufgaben sind die manipulationssichere Ausführung von Programmen (Authentisierung), die Benutzeridentifizierung (mittels PIN) und die Speicherung von Daten, wie beispielsweise Telefonnummern. Die normative Grundlage für die USIM ist die TS 31.102, die von → <i>ETSI</i> herausgegeben wird. Das Äquivalent der USIM bei → <i>GSM</i> ist die → <i>SIM</i> . ⁶⁵
USIM Application Toolkit (USAT)	Genormt in TS 31.111; erlaubt einer USIM-Karte, eine aktive Rolle bei der Steuerung des Mobiltelefons zu übernehmen. Mit dem USIM Application Toolkit ist es beispielsweise einer USIM möglich, Anzeigen auf dem Display auszugeben, Eingaben über die Tastatur anzufordern und Nachrichten über die Luftschnittstelle zu senden und zu empfangen. Das USIM Application Toolkit ist die Grundlage für die meisten Zusatzanwendungen bei Mobiltelefonen. Das Äquivalent des USIM Application Toolkit bei GSM ist der → <i>SIM Application Toolkit</i> (SAT). ⁶⁶
verbindungsorientiert (<i>circuit-switched</i>)	Bei verbindungsorientierten Datenübertragungen wird zum Datenaustausch eine direkte Verbindung (d. h. eine Leitung) zwischen zwei Instanzen hergestellt. In der Regel wird dabei die Zeitdauer der Verbindung abgerechnet und nicht die übertragene Datenmenge (→ <i>paketorientiert</i>). Ein ebenfalls benutzter und äquivalenter Ausdruck ist leitungsorientiert. Typische Beispiele für verbindungsorientierten Datenübertragungen sind analoge Telefonanschlüsse ans Festnetz und ISDN.
vertikaler Prototyp	→ <i>Prototyp</i>
Verwaltungsdaten	Daten, die nur der Verwaltung von → <i>Nutzdaten</i> dienen und für eine → <i>Anwendung</i> ansonsten keinerlei Bedeutung haben.
Verzeichnisdienst (<i>directory service</i>)	Dienst, der in einer Datenbank Listen mit bestimmten Informationen für Anfrager zur Verfügung stellt. Ein typisches Beispiel dafür sind → <i>Zertifikatswiderverzeichnisse</i> , in denen bei einer → <i>PKI</i> alle nicht mehr gültigen und akzeptierten Zertifikate aufgeführt sind.
Vielfachzugriffsverfahren (<i>multiple access</i>)	Funk- und informationstechnische Methoden, um eine begrenzte Frequenzbandbreite einer Funkübertragung gleichzeitig oder scheinbar gleichzeitig möglichst vielen Teilnehmern zur Verfügung zu stellen. Die üblichen vier Verfahren sind Frequenzvielfachzugriff (→ <i>FDMA</i>), Zeitvielfachzugriff (→ <i>TDMA</i>), Codevielfachzugriff (→ <i>CDMA</i>) und Raumvielfachzugriff (→ <i>SDMA</i>). ⁶⁷
Virginalkarte	Karte, die noch nicht mit einem Chip versehen und noch nicht optisch oder elektrisch personalisiert ist. Eine Virginalkarte ist im Wesentlichen ein bedruck-

⁶² Siehe auch Abschnitt 13.3 „Das UMTS-System“.

⁶³ Siehe auch Abschnitt 4.2 „Codierung alphanumerischer Daten“.

⁶⁴ Siehe auch Abschnitt 13.2 „Das GSM-System“.

⁶⁵ Siehe auch Abschnitt 13.2.4 „Die SIM“.

⁶⁶ Siehe auch Abschnitt 13.2.4 „Die SIM“.

⁶⁷ Siehe auch Abschnitt 13.1.1 „Vielfachzugriffsverfahren“.

	ter, uniformer → <i>Kartenkörper</i> , wie er in der Massenproduktion von Karten hergestellt wird.
Virtual Machine (VM)	Ein in Software simulierter → <i>Mikroprozessor</i> mit in der Regel eigenem Opcode für die Maschinenbefehle und einem ebenfalls simulierten Adressraum. Auf diese Weise wird eine von den Hardware-Gegebenheiten unabhängige Gestaltung von Software möglich. So kann beispielsweise der virtuelle Adressraum einer VM um ein Vielfaches größer sein als derjenige, welcher durch die Hardware zur Verfügung gestellt wird. Im Umfeld von Java wird für die geschlossene Umgebung der VM oft auch der Begriff „Sandbox“ verwendet. ⁶⁸
virtuelle Chipkarte (<i>virtual smart card</i>)	Die softwaretechnische Simulation einer Chipkarte in einem anderen System, z. B. in einem Sicherheitsmodul oder Mobiltelefon. Ein Spezialfall der virtuellen Chipkarte ist die virtuelle Händlerkarte, bei der die Simulation der Chipkarte im Terminal des Händlers abläuft.
virtuelle Händlerkarte (<i>virtual merchant card</i>)	→ <i>virtuelle Chipkarte</i>
Visa Cash	Markenname von Visa für technologisch unterschiedliche elektronische Geldbörsensysteme mit Chipkarten.
Visa Easy Entry (VEE)	Verfahren für die einfache Migration von magnetstreifenbasierten Kreditkarten hin zu Kreditkarten mit Mikrocontrollerchip. Dazu werden der Name des Kartenbesitzers und alle Daten der Magnetstreifen in einem EF unter einem für Visa reservierten DF abgelegt. Bei einer Kreditkartenzahlung liest das Terminal die für diese Transaktion notwendigen Daten statt vom Magnetstreifen aus dem Chip. Der Vorteil des Verfahrens besteht darin, dass nur am POS das Terminal mit einer Chipkartenkontaktiereinheit umgerüstet werden muss und das gesamte Hintergrundsystem ohne Änderungen weiter betrieben werden kann.
voll duplex (<i>full duplex</i>)	Datenübertragung, bei der miteinander kommunizierende Geräte gleichzeitig senden und empfangen können (→ <i>halbduplex</i>).
VOP	→ <i>OP</i>
Vorgehensmodell (<i>life cycle model</i>)	Auch Prozessmodell genannt; legt in abstrakter Form den organisatorischen Rahmen, die Arbeitsabläufe und die Aktivitäten mit dazugehörigen Voraussetzungen und Ergebnissen für Entwicklungen fest. Zweck ist eine allgemein einsetzbare und einheitliche Arbeitsweise bei Entwicklungen. Beispiele für Vorgehensmodelle sind Wasserfallmodell, V-Modell und zyklische Entwicklungsmodelle. ⁶⁹
Vorpersonalisierung	andere Bezeichnung für → <i>Initialisierung</i>
Wafer	Dünne Scheibe Silizium, auf der mit halbleitertechnischen Mitteln Chips aufgebaut werden. Typische Durchmesser von Wafer sind 150 mm (6 Zoll), 200 mm (8 Zoll) und 300 mm (12 Zoll).
WAP (<i>wireless application protocol</i>) [WAP]	Dieser Begriff wird für eine Reihe von Spezifikationen zur Realisierung der Anbindung von mobilen Endgeräten (Mobiltelefone, PDAs, ...) über ein drahtloses Netzwerk an einen Server zwecks unmittelbaren Informationsaustausches benutzt. Die übliche Anwendung von WAP ist die Realisierung von Internetdiensten auf einem Mobiltelefon, weitgehend unabhängig vom jeweiligen Mobilfunkstandard. Die Bezeichnung Wireless Application Protocol steht im Übrigen neben der Technologie auch noch für das Protokoll zwischen Endgerät und Hintergrundsystem. Das seit Juni 1997 existierende und von den Firmen Phone.com, Ericson, Motorola und Nokia gegründete WAP-Forum ist das international agierende Normungsgremium für WAP und setzt sich aus Vertretern von über 350 Firmen zusammen. ⁷⁰
WAP Forum	→ <i>WAP</i>
Warmreset	→ <i>Reset</i>
WCDMA (<i>wideband code division multiple access</i>)	→ <i>CDMA</i>
Whitelist	Liste in einer Datenbank, auf der alle Chipkarten oder Geräte vermerkt sind, die in einer bestimmten → <i>Anwendung</i> verwendet werden dürfen (→ <i>Sperrliste</i> , <i>White List</i>).
white plastic	Nicht personalisierte Blankokarten, die in betrügerischer Absicht verwendet

⁶⁸ Siehe auch Abschnitt 5.14.1 „Java Card“.

⁶⁹ Siehe auch Abschnitt 15.7 „Vorgehensmodelle“.

⁷⁰ Siehe auch Abschnitt 13.5 „Die WIM“.

(weiße Karte)	werden. Der Begriff kommt ursprünglich von den typischen Kartenrohlingen aus weißem Kunststoff zur Herstellung von Testkarten. Mittlerweile versteht man jedoch unter <i>white plastics</i> auch bedruckte Karten mit den unterschiedlichsten → <i>Kartenelementen</i> , wie beispielsweise noch nicht hochgeprägte Kreditkartenrohlinge mit Magnetstreifen und Hologramm.
Whitebox Test	Beim diesem Test, oft auch Glassbox Test genannt, geht man davon aus, dass die testende Instanz vollständige Kenntnis über alle internen Abläufe und Daten der zu prüfenden Software hat.
WIM (<i>wireless application protocol (WAP) identity module</i>)	Sicherheitsmodul für → <i>WAP</i> -Endgeräte. Die Spezifikation beschreibt eine zu PKCS#15 kompatible Chipkarten-Anwendung (→ <i>Anwendung</i>). Die Hauptaufgaben eines WIM sind die Erstellung und Prüfung von → <i>digitalen Signaturen</i> und die Verschlüsselung von Daten. Eine WIM kann damit entweder eine eigene physikalische Chipkarte sein oder eine von mehreren Anwendungen auf einer Multiapplikationskarte. Typischerweise ist die WIM eine Anwendung auf einer → <i>SIM</i> oder → <i>USIM</i> .
Windows for Smart Cards [Microsoft]	Auch WfSC, WSC; offenes → <i>Chipkarten-Betriebssystem</i> , (→ <i>offenes Chipkarten-Betriebssystem</i>) der Firma Microsoft, das mehrere → <i>Anwendungen</i> (→ <i>Multiapplication-Chipkarte</i>) und nachladbare Programme unterstützt. Eine Besonderheit von Windows for Smart Cards ist, dass ein → <i>FAT</i> -basierendes Dateisystem benutzt wird. ⁷¹
Wissensteilung (<i>shared secrets</i>)	Dieses Prinzip besagt, dass es niemanden gibt, der von einem bestimmten System alles weiß. Die bewusste Aufteilung des Wissens verhindert, dass einzelne Personen durch Dritte angreifbar werden oder durch ihr Wissen zu viel Macht über ein System erlangen können. Bei der Entwicklung von Sicherheitskomponenten ist die Wissensteilung auf mehrere Personen ein üblicher Ansatz.
WML (<i>wireless markup language</i>)	Auf XML aufbauende logische Auszeichnungssprache, um Anwendungen für WAP zu erstellen. WML ist sehr ähnlich zu HTML. Die auf einem WAP-Server in einer WML-Seite abgelegte WML-Applikation wird von einem Converter on-the-fly in kompakten WML-Bytecode übersetzt, über das drahtlose Netzwerk zum mobilen Endgerät übertragen und dann dort von einem Microbrowser (→ <i>Browser</i>) interpretiert.
work around	In der Softwareentwicklung die Umgehung eines bekannten Fehlers durch „Um-den-Fehler-Herumprogrammieren“. Der Fehler als solcher wird durch einen work around nicht beseitigt, sondern lediglich seine negativen Auswirkungen auf den Rest des Programms. Beispielsweise werden festgestellte Fehler von ROM-basierten → <i>Chipkarten-Betriebssystemen</i> nachträglich typischerweise mit work arounds im EEPROM durchgeführt, sodass diese Fehler keine negativen Auswirkungen auf das Chipkarten-Betriebssystem haben. Dabei kann jedoch durch den work around durchaus die Funktionalität des Chipkarten-Betriebssystems gegenüber dem ursprünglichen Umfang eingeschränkt werden.
WWW, W3 (<i>world wide web</i>)	Teil des weltweiten Internets, den vor allem die Möglichkeit der beliebigen Verknüpfung von Dokumenten durch Hyperlinks und die Integration von multimedialen Objekten in Dokumente charakterisiert.
X.509	Die von der → <i>ITU</i> herausgegebene X.509-Norm definiert Aufbau und Codierung von → <i>Zertifikaten</i> . Sie ist die weltweit am häufigsten eingesetzte Norm für Zertifikatsstrukturen (→ <i>PKI</i>).
XML (<i>extended markup language</i>)	Logische Auszeichnungssprache und sowohl Nachfolger als auch Ergänzung von HTML. Mit XML lassen sich eigene Sprachelemente festlegen, sodass sich andere Auszeichnungssprachen wie HTML oder WML mittels XML definieren lassen. XML selber ist wiederum eine Untermenge der sehr mächtigen ISO-Norm SGML (<i>standard generalized markup language</i>).
Zeitstempel (<i>time stamp</i>)	Ein mit einer → <i>digitalen Signatur</i> versehene Bescheinigung einer Instanz, dass dieser Instanz bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben (→ <i>PKI</i>).
Zelle (<i>cell</i>)	Im Mobilfunkbereich ist die kleinste geografische Einheit, in der das Netzwerk aufgeteilt ist.
Zellulartechnik	Analoges oder digitales Mobilfunksystem, das in Zellen organisiert ist. Üblicherweise befindet sich im ungefähren Mittelpunkt der Zelle die Sende- und Empfangsstation des Netzwerks, üblicherweise Basisstation genannt. ⁷²

⁷¹ Siehe auch Abschnitt 5.7 „Dateiverwaltung“.

⁷² Siehe auch Abschnitt 13.1.2 „Zellulartechnik“.

Zertifikat (<i>certificate</i>)	Ein von einer vertrauenswürdigen Instanz digital signierter öffentlicher Schlüssel mit dazugehörigen Verwaltungsdaten, damit dieser von Dritten als authentisch anerkannt werden kann (→ <i>PKI</i>). Die verbreitetste und bekannteste Festlegung des Aufbaus und Codierung von Zertifikaten ist die X.509-Norm.
Zertifikatswiderrufsliste (<i>certificate revocation list – CRL</i>)	Liste in einem → <i>Verzeichnisdienst</i> , die alle gesperrten und nicht mehr akzeptierten Zertifikate innerhalb einer → <i>PKI</i> enthält.
Zertifizierung	Der Begriff <i>Zertifizierung</i> wird manchmal und in nicht ganz korrekter Weise als Äquivalent zum Begriff <i>Evaluierung</i> (siehe auch <i>Evaluierung</i>) benutzt.
Zertifizierungsinstanz (<i>CA – certificate authority</i>)	Zertifizierungsstelle in einer Public-Key Infrastruktur (→ <i>PKI</i>), die öffentliche Schlüssel für → <i>digitale Signaturen</i> beglaubigt, d. h. sich für ihre Echtheit verbürgt. Dazu unterschreibt die Zertifizierungsinstanz mit ihrem geheimen Schlüssel die öffentlichen Schlüssel der Anwender und stellt bei Bedarf die signierten öffentlichen Schlüssel in einem Verzeichnis (→ <i>Verzeichnisdienst</i>) in Form eines → <i>Zertifikates</i> zur Verfügung. Die Zertifizierungsinstanz kann die dazu notwendigen Schlüsselpaare (geheimer und öffentlicher Schlüssel) selber erzeugen. Zertifizierungsinstanzen sind oft aus organisatorischen Gründen hierarchisch aufgebaut, wobei die oberste Zertifizierungsinstanz auch als Top-Level-CA oder Root-CA bezeichnet wird.
ziffern	Aufprägen oder Aufdrucken einer Nummer bei Chipkarten. Dies wird typischerweise bei der Produktion von anonymen Telefonwertkarten durchgeführt, um diesen eine sichtbare und einzigartige Nummer zur eindeutigen Identifizierung zu geben.
ZKA	In Deutschland die Koordinierungsinstanz für die elektronischen Zahlungsverfahren der deutschen Banken. Der ZKA setzt sich aus dem Deutsche Sparkassen- und Giroverband (DSGV), dem Bundesverband der Deutschen Volks- und Raiffeisenbanken (BVR), dem Bundesverband deutscher Banken (BdB) und dem Verbund öffentlicher Banken (VÖB) zusammen. Den Vorsitz des ZKA übernimmt jedes Jahr ein anderer der vier Bankenverbände.
Zugriffsbedingungen (<i>access conditions – AC</i>)	Im Zusammenhang mit dem Dateisystem einer Chipkarte versteht man unter den Zugriffsbedingungen einer Datei eine endliche Zahl von Bedingungen für vom Betriebssystem unterstützte Zugriffe (z. B. Lesen, Schreiben, Löschen, ...) auf diese Datei, wobei die Bedingungen für jede Zugriffsart in der Regel unabhängig voneinander sind und die Bedingungen vor dem Zugriff erfüllt sein müssen.
Zusatzanwendungen (<i>VAS – value added service</i>)	Weitere Chipkarten-Anwendungen (→ <i>Anwendung</i>), die sich neben einer Hauptanwendung auf einer Chipkarte befinden. Voraussetzung dafür sind in der Regel → <i>Multiapplication-Chipkarten</i> .