Das Glossar aus dem Handbuch der Chipkarten

Version 2.2.1 vom 2. März 2000

Dieses Glossar stammt aus dem Handbuch der Chipkarten von Wolfgang Rankl und Wolfgang Effing, das 1999 in der 3ten Auflage beim Carl Hanser Verlag München erschienen ist.

Diese Datei darf frei kopiert werden, solange ihr Inhalt nicht verändert wird. Sie ist in dem Format A4 problemlos ausdruckbar.

Die Autoren haben den Inhalt dieses Dokuments sorgfältig zusammengestellt, übernehmen jedoch keinerlei Haftung für die Korrektheit der Angaben. Im Zweifelsfalle sollte immer die entsprechende Norm oder Spezifikation zu Rate gezogen werden.

Verbesserungs- und Ergänzungsvorschläge sind jederzeit herzlich willkommen. Diese können an die e-Mail-Adresse „hdc@wrankl.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 Verlags [www.hanser.de] als auch auf der Homepage von Wolfgang Rankl [www.wrankl.de, www.geocities.com/SiliconValley/Foothills/4710] neue Versionen dieses Dokuments veröffentlicht.

Handbuch der Chipkarten
Wolfgang Rankl und Wolfgang Effing
3. Auflage 1999, Carl Hanser Verlag München
ISBN: 3-446-21115-2

Smart Card Handbook
Wolfgang Rankl and Wolfgang Effing
John Wiley & Sons
ISBN: 0-471-96720-3

1 µm, 0,8 µm, ... -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 bei 0,25 µm bzw. 0,18 µm. Größere Strukturen auf dem Chip sind selbstverständlich immer möglich.
µP-Karte	Das Wort µP-Karte ist eine andere Bezeichnung für Mikroprozessorkarte (siehe Mikroprozessorkarte).
3DES	siehe Triple-DES
Acquirer	Eine Instanz, auch Sammelbeauftragter genannt, 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.
AFNOR	Die Association Française de Normalisation ist eine französische Normungsorganisation mit Sitz in Paris.
AID (*application identifier*)	Der AID ist ein Kennzeichen für eine Anwendung auf einer Chipkarte und 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 (*registered identifier*) und PIX (*proprietary identifier*).
ANSI	Das American National Standards Institute ist eine US-amerikanische Normungsorganisation mit Sitz in New York.
Antwort-APDU (*response-APDU*)	Eine Antwort-APDU ist die Antwort der Chipkarte auf eine vom Terminal abgesendete Kommando-APDU. Sie setzt sich aus den optionalen Antwortdaten und den obligatorischen 2 Byte langen Statuswörtern SW1 und SW2 zusammen.
Anwendung	Daten, Kommandos, Abläufe, Zustände, Mechanismen, Algorithmen und Programmcode innerhalb einer Chipkarte, 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.
Anwendungsbetreiber	Eine Instanz, die eine Anwendung auf Chipkarten betreibt. Im allgemeinen identisch mit dem Anwendungsanbieter.
APDU	Eine APDU (*application protocol data unit*) ist ein softwaretechnischer Datencontainer, in den die Daten einer Anwendung verpackt werden um sie zwischen Terminal und Chipkarte auszutauschen. Eine APDU wird vom Übertragungsprotokoll in eine TPDU (*transport protocol data unit*) umgewandelt und dann über die serielle Schnittstelle von Terminal bzw. Chipkarte verschickt. APDUs lassen sich in Kommando-APDU und Antwort-APDU einteilen.
API	Ein Application Programming Interface ist eine detailliert spezifizierte Softwareschnittstelle innerhalb eines Programms, um einen standardisierten Zugriff auf Funktionen dieses Programms für Dritte zu ermöglichen.
Applet	Ein Applet ist ein Programm in der Programmiersprache Java, das in der virtuellen Maschine eines Rechners ausgeführt wird. Die Funktionalität eines Applets ist aus Sicherheitsgründen auf die vorher festgelegte Programmumgebung eingeschränkt. Ein Applet wird im Bereich von Chipkarten manchmal auch Cardlet genannt und entspricht in der Regel einer Chipkarten-Anwendung.
ASN.1	Die abstract syntax notation one ist eine Beschreibungssprache für Daten. Durch sie lassen sich Daten unabhängig vom benutzenden Computersystem eindeutig definieren und darstellen. ASN.1 ist durch ISO/IEC 8824 und ISO/IEC 8825 definiert.
Assembler	Als Assembler wird ein Programm bezeichnet, das Assemblerprogrammcode in von einem Prozessor ausführbare Maschinensprache übersetzt. Nach dem Assembliervorgang muß das Programm üblicherweise noch mit einem Linker gelinkt werden. Der Begriff Assembler wird jedoch auch oft als Kurzform von Assemblerprogrammcode benutzt.
ATR	Der Answer to Reset ist eine Sequenz von Bytes welche eine Chipkarte als Antwort auf den (Hardware-)Reset aussendet. Der ATR beinhaltet u.a. diverse Parameter für das Übertragungsprotokoll zur Chipkarte.
Auswurfleser	Terminal, das eine gesteckte Karte durch ein elektrisches oder mechanisches Signal automatisch auswerfen kann.

Authentisierung	Eine Authentisierung ist der Vorgang des Nachweises der Echtheit einer Instanz (z.B. einer Chipkarte) durch kryptografische Verfahren. Vereinfacht ausgedrückt stellt man bei der Authentisierung durch ein festgelegtes Verfahren fest, ob jemand auch derjenige ist, der er vorgibt zu sein
Authentizität	Echtheit und Unverändertheit einer Instanz oder Nachricht.
Automat	In der Informationstechnik ein Teil eines Programms, das einen Ablauf auf der Grundlage eines vorher definierten Zustandsdiagramms (d.h. Zustände mit Zustandsübergängen) bestimmt.
Autorisierung	Die Prüfung, ob eine bestimmte Aktion ausgeführt werden darf wird Autorisierung genannt, d.h. jemand wird für etwas ermächtigt. Wird beispielsweise eine Kreditkartentransaktion durch den Kreditkartenherausgeber 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 auf der Authentisierung der betreffenden Instanz (z.B.: einer Chipkarte) zustande kommen. Vereinfacht ausgedrückt erteilt man bei der Autorisierung jemanden die Erlaubnis etwas bestimmtes zu tun.
Bellcore-Angriff (*Bellcore-Attack*)	siehe differentielle Fehleranalyse
Benutzer	Die Person, die eine Chipkarte verwendet. Sie muß nicht unbedingt Karteninhaber sein.
Betriebssystemhersteller	Eine Instanz, die Programmierung und Test eines Betriebssystems durchführt.
big Endian	siehe Endianness
binärkompatibler Programmcode	siehe Nativcode
Black List	siehe Sperrliste
Blackbox Test	Beim Blackbox Test geht man davon aus, daß die testende Instanz keine Kenntnisse über die internen Abläufe, Funktionen und Mechanismen der zu prüfenden Software hat.
Boot-Loader	Ein Boot-Loader ist ein (kleines) Programm, mit dem weitere und umfangreichere Programme, beispielsweise über eine serielle Schnittstelle, nachgeladen werden. Der Boot-Loader wird in der Regel dazu benutzt, den eigentlichen Programmcode in einen neuen Chip oder in ein neues elektronisches Gerät zu laden. Oftmals kann der Boot-Load-Vorgang nur ein einziges Mal ausgeführt werden.
Börsenanbieter (*purse provider*)	Unter einem Börsenanbieter versteht man die Organisation, die für die Gesamtfunktionalität und Sicherheit eines Börsensystems verantwortlich ist. Er ist im Regelfall auch der Herausgeber des elektronischen Kartengeldes und garantiert auch für die Einlösung.
Börseninhaber (*purse holder*)	Ein Börseninhaber ist die Person, welche die Chipkarte mit der elektronischen Geldbörse besitzt.
Brute-force-Angriff	Angriff auf ein kryptografisches System durch die Berechnung aller Möglichkeiten eines Schlüssels.
BSI	Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde 1990 gegründet und ist der Nachfolger der deutschen Zentralstelle für das Chiffrierwesen. Das BSI berät Behörden und setzt Rahmenbedingungen für Kryptografieanwendungen in Deutschland. Daneben bietet es unter anderem auch als Dienstleistung die Bewertung, also die Zertifizierung der Sicherheitseigenschaften von informationstechnischen Systemen an.
Buffern	Typischer Angriff bei Magnetstreifenkarten. Lesen eines Magnetstreifens und Zurückschreiben, nachdem ein Terminal Daten (z.B. den Fehlbedienungszähler) darauf verändert hat.
Bug fix	Ein Bug fix ist in der Softwareentwicklung die Ausbesserung eines bekannten Fehlers durch zusätzlichen Programmcode, z.B.: durch einen work around.
Bytecode	Als Bytecode wird 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.

CAP-Datei (*CAP-file*)	Die CAP-Datei (*card appplication file – CAP-file*) ist das Datenaustauschformat zwischen der Java Offcard Virtual Machine und der Java Oncard Virtual Machine.
Cardlet	siehe Applet
Class-Datei (*classfile*)	Die compilierten, d.h. in Bytecode übersetzten, und mit zusätzlichen Informationen versehenen Java-Programme werden in einer sogenannten Class-Datei abgespeichert. Nach dem Laden werden sie von der Java Virtual Machine ausgeführt.
CCITT	Das Comité Consultatif International Télégraphique et Téléphonique war ein internationaler Ausschuß für Telefon- und Telegraphendienste mit Sitz in Genf. Die CCITT ist mittlerweile unter Erweiterung der Aufgaben in ITU umgetauft worden.
CCS	Die Cryptographic Checksum ist eine 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 MAC (*message authentication code*).
CEN	Die europäische Normungsorganisation Comité Européen de Normalisation (CEN) in Brüssel, Belgien setzt sich aus den nationalen Normungsorganisationen aller europäischen Länder zusammen und ist die offizielle Institution der EU für europäische Normung.
CEPT	Die Conférence Européenne des Postes et Télécommunications ist eine europäische Normungsorganisation der nationalen Telekommunikationsgesellschaften.
Certificate Authority (CA)	Eine Certificate Authority ist eine Zertifizierungsstelle, die öffentliche Schlüssel für digitale Signaturen beglaubigt, d.h. sich für ihre Echtheit verbürgt. Dazu unterschreibt die CA mit ihrem geheimen Schlüssel die öffentlichen Schlüssel der Anwender und stellt bei Bedarf die signierten öffentlichen Schlüssel in einem Verzeichnis zur Verfügung. Die CA kann die dazu notwendigen Schlüsselpaare (geheimer und öffentlicher Schlüssel) selber generieren.
Chipkarte	Chipkarte ist der allgemeine Begriff für eine Karte, meist auf Kunststoff, die ein oder mehrere Halbleiterchips enthält. Eine Chipkarte kann entweder eine Speicherkarte (siehe Speicherkarte) oder eine Mikroprozessorkarte (siehe Mikroprozessorkarte) sein.
Clearing	Die Funktion der Abrechnung im elektronischen Zahlungsverkehr zwischen dem Akzeptanten einer elektronischen Zahlung (in der Regel ein Händler) und seiner Bank.
Clearingsystem	Ein rechnergestütztes Hintergrundsystem, das die zentrale Abrechnung im Rahmen einer Anwendung für elektronischen Zahlungsverkehr übernimmt.
Combikarte	siehe Dual-Interface-Karte
Compiler	Als Compiler wird ein Programm bezeichnet, das eine Programmiersprache wie BASIC oder C in von einem Prozessor ausführbare Maschinensprache übersetzt. Nach dem Compilationsvorgang muß das Programm üblicherweise noch mit einem Linker gelinkt werden.
COS	Für Chipkarten-Betriebssysteme hat sich in der Vergangenheit weltweit die Bezeichnung COS (*card operating system*) eingebürgert. Sie ist auch häufig in Produktnamen (z.B.: STARCOS, MPCOS, ...) zu finden.
CRC	Der cyclic redundancy check ist ein einfacher und weit verbreiteter Fehlererkennungscode (EDC) zur Sicherung von Daten. Der CRC muß durch einen Startwert und ein Teilerpolynom vor seiner Anwendung festgelegt werden.
Debitkarte	Eine Karte mit oder ohne Chip, die einen Verfügungsrahmen aufweist, bei der aber die Bezahlung zeitgleich nach Erhalt des Gutes oder der Dienstleistung stattfindet. Schlagwort dazu: „pay now“. Das typische Beispiel ist die ec-Karte.
Debugging	Debugging ist die Fehlersuche und -beseitigung mit dem Zweck, möglichst viele Fehler einer Software zu erkennen und zu korrigieren. Das Debugging wird in der Regel vom Softwareentwickler durchgeführt und ist nicht identisch mit dem Testing.
Delamination	Als Delamination bezeichnet man das unerwünschte 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.

deterministisch	Als deterministisch wird ein Verfahren oder Algorithmus bezeichnet, der bei identischen Ausgangsbedingungen immer zum gleichen Ergebnis kommt. Das Gegenteil ist probabilistisch.
DF-Name	Der DF-Name ist neben dem FID ein weiteres Merkmal für ein DF und hat eine Länge zwischen 1 und 16 Byte. Er wird zur Selektion des DFs benutzt und kann einen registrierten 5 bis 16 Byte langen AID (*application identifier*) enthalten, der das DF weltweit eindeutig macht.
DF	Ein Dedicated File ist ein Verzeichnis im Dateisystem einer Chipkarte. Eine Variante des DFs ist das Root-Verzeichnis MF.
Die, Dice	Ein Siliziumkristall in Form eines Plättchens, auf dem sich ein einzelner halbleitertechnisch aufgebauter elektronischer Schaltkreis (z.B.: Mikrocontroller) befindet.
Diensteanbieter (*service provider*)	Eine Diensteanbieter ist die Instanz, welche gegen Bezahlung einen Dienst (z.B.: Verkauf von Gütern oder Dienstleistungen) anbietet.
differentielle Fehleranalyse (DFA)	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. Jedoch wurde diese Angriffsmethode innerhalb einiger Monate sehr schnell weiterentwickelt [Anderson 96 a], so daß nunmehr prinzipiell mit der differentiellen Fehleranalyse alle Kryptoalgorithmen angegriffen werden können, sofern sie keine besonderen Schutzmaßnahmen aufweisen.
differentielle Kryptoanalyse	Bei der differentielle Kryptoanalyse 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.
digitale Signatur	Die digitale Signatur wird 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 Signaturgesetz (siehe Signaturgesetz). Digitale Signaturen werden manchmal auch elektronische Unterschriften genannt.
digitaler Fingerabdruck (*digital fingerprint*)	Der Hash-Wert einer Nachricht (z.B.: mit SHA-1 erstellt) wird oft auch als digitaler Fingerabdruck bezeichnet.
Download	Übertragen von Daten von einem übergeordneten System (Hintergrundsystem, Host) an ein untergeordnetes System (z.B. Terminal). Das Gegenteil ist der „Upload“.
DRAM	Ein dynamic random access memory ist ein RAM-Speicher in dynamischer Bauweise und benötigt zum Erhalt des Speicherinhalts eine konstante Stromversorgung sowie eine zyklische Wiederauffrischung des Inhalts. DRAM-Speicher sind aus Kondensatoren aufgebaut. Sie benötigen weniger Platz auf dem Chip als SRAM-Speicher und sind deshalb billiger. Allerdings ist die Zugriffszeit auf SRAMs geringer.
Dual-Interface-Karte	Der Begriff Dual-Interface-Karte ist die Bezeichnung für eine Chipkarte mit kontaktbehafteter und kontaktloser Schnittstelle für die Datenübertragung von und zur Karte. Ein anderer Begriff dafür ist Combikarte.
Dual Slot Handy	Bezeichnung für ein Mobiltelefon, das neben der Benutzerkarte (z.B.: SIM) noch eine von außen zugängliche Kartenkontakttiereinheit für ID-1 Chipkarten besitzt. Mit Dual Slot Handys lassen sich beispielsweise Zahlungen über das Mobilfunknetz mit bestehenden elektronischen Geldbörsen auf Chipkarten abwickeln.
duplizieren	Übertragen von echten Daten auf eine zweite Karte zum Zwecke der Herstellung einer oder mehrerer identischer (geklonter) Karten. Der Begriff ist in der Regel identisch mit „klonen“ (siehe klonen).
ECC	Der error correction code ist eine Prüfsumme über Daten. Mit einem ECC können Fehler in den Daten mit einer bestimmten Wahrscheinlichkeit erkannt und ggf. auch fehlerfrei korrigiert werden. Das Kürzel ECC steht auch für Kryptosysteme auf der Grundlage von elliptischen Kurven (*elliptic curve cryptosystem*).

e-Commerce	Unter dem Begriff electronic Commerce versteht man vor allem alle Formen von Dienstleistung, Handel und darauf aufbauenden Zahlungsverkehr in offenen Netzen, d.h. vor allem im Internet.
EDC	Ein error detection code ist ein 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.
EEPROM	Ein electrical erasable read only memory ist eine nichtflüchtige Speicherart, die in Chipkarten Verwendung findet. Ein EEPROM ist in Speicherseiten eingeteilt, und sein Inhalt kann verändert und gelöscht werden, wobei es aber eine physikalisch bedingte Obergrenze der Anzahl der schreibenden bzw. löschenden Zugriffe gibt.
EF	Elementary Files stellen die eigentlichen Datenspeicher im Dateibaum einer Chipkarte dar. 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, ...).
Einwegfunktion (*one-way function*)	Eine Einwegfunktion ist eine mathematische Funktion, die sich einfach berechnen läßt, deren Umkehrfunktion aber einen sehr großen Rechenaufwand erfordert.
elektronische Geldbörse (*e-purse*)	Eine Karte mit Chip, die vor der Bezahlung mit einem Geldbetrag aufgeladen werden muß. Schlagwort dazu: „pay before“. Typische Beispiele sind die deutsche Geldkarte, Visa Cash oder Mondex. Elektronische Geldbörsen können die Eigenschaft von Purso-to-Purse-Transaktionen haben.
Embossing	siehe Hochprägung
EMV	Gemeinsame Spezifikation für Zahlungsverkehrskarten mit Chip sowie dazugehörige Terminals der Firmen Europay, Master Card und Visa. Diese Spezifikationen sind zum weltweiten Industriestandard für Kredit-, Debit und Börsenkarten avanciert und damit das Pendant des Zahlungsverkehrs zur Telekommunikationsnorm GSM 11.11.
EMV-Spezifikation	siehe EMV
Endianness	Die Endianness gibt die Reihenfolge der Byte 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 niederwertigste Byte ist am Anfang und das höherwertigste Byte am Schluß.
EPROM	Ein erasable read only memory ist eine nichtflüchtige Speicherart, die in Chipkarten nur noch sehr selten Verwendung findet. Ein EPROM kann nur durch UV-Licht gelöscht werden, weshalb es im Chipkartenbereich nur als WORM-Speicher (*write once, read multiple*) verwendet werden kann.
ETS	ETS (European Telecommunication Standard) ist die Bezeichnung der von ETSI herausgegebenen Normen, die sich in erster Linie mit europäischer Telekommunikation beschäftigen.
ETSI	Das European Telecommunications Standards Institute mit Sitz in Sophia Antipolis, Frankreich, ist das Normungsinstitut der europäischen Telekommunikationsgesellschaften und beschäftigt sich mit der Normung im Bereich der europäischen Telekommunikation. Die im Chipkartenbereich wichtigste ETSI-Norm ist die GSM-Normenreihe (GSM 11.11 u.a.).
etu	Eine elementary time unit ist die Dauer eines Bits bei der Datenübertragung zu Chipkarten. Die absolute Zeitdauer für ein etu ist nicht fix festgelegt, sondern in Abhängigkeit vom an die Chipkarte angelegten Takt und des Clock Rate Conversion Factors definiert.
Falltür (*trap door*)	Vorsätzlich angelegter Mechanismus in einer Software oder in einem Algorithmus, mit dem Sicherheitsfunktionen oder Schutzmechanismen umgangen werden können.
fault tree analysis	Als Fault Tree Analysis wird beim Testen die Methode bezeichnet, bei der zur Fehlersuche jeder mögliche Programmablauf im Programmcode durchlaufen wird.

Fehlbedienungszähler	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).
FID	Der FID (*file identifier*) ist ein zwei Byte großes Merkmal für eine Datei. Sowohl MF als auch DF und EF besitzen einen FID. Der FID des MFs ist immer '3F00'.
FIPS	Der Begriff Federal Information Processing Standard bezeichnet die von NIST herausgegebenen US-amerikanischen Normen.
Floorlimit	Das Floorlimit gibt an, ob eine Zahlung von einer dritten Instanz autorisiert werden muß. Unterhalb dieser Grenze ist eine Autorisierung nicht notwendig, und oberhalb dieser Grenze muß eine Autorisierung vorgenommen werden, da sonst die Zahlung nicht möglich oder garantiert ist.
flüchtiger Speicher (*volatile memory*)	Eine Speicherart (z.B. RAM), die ihren Inhalt nur bei dauernder Stromzufuhr behält.
Garbage Collection	Die Garbage Collection sammelt den von einer Anwendung nicht mehr benutzten Speicher und stellt ihn wieder als Freispeicher zur Verfügung. Die Garbage Collection wurde früher als 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.
geschlossene Anwendung	Anwendung auf einer Chipkarte, die nur dem Anwendungsbetreiber zur Verfügung steht und nicht allgemein verwendet werden kann.
geschlossene Börse	Realisation einer geschlossenen Anwendung für eine elektronische Geldbörse. Sie kann nur in dem vom Anwendungsbetreiber freigegebenen Rahmen und nicht für allgemeine Zahlungstransaktionen verwendet werden.
Greybox Test	Der Greybox Test ist eine Mischform zwischen Whitebox Test und Blackbox Test. Die testende Instanz kennt dabei teilweise die internen Abläufe, Funktionen und Mechanismen der zu prüfenden Software.
GSM	Das Global System for Mobile Communications ist eine Spezifikation für ein länderübergreifendes, bodengebundenes Mobiltelefonsystem. Ursprünglich für wenige Länder in Zentraleuropa gedacht, hat es sich zu einem Weltstandard für Mobiltelefone entwickelt. Der designierte Nachfolger von GSM wird das UMTS (*Universal Telecommunication System*) sein.
Gutfall	Der Fall bei einer logischen Entscheidung, der zum günstigeren oder beabsichtigten Ergebnis führt.
Hardmaske (*hard mask*)	Der Begriff Hardmaske bedeutet, daß sich der gesamte Programmcode weitgehend im ROM befindet. Dies spart gegenüber einer Softmaske Platz, da ROM-Zellen wesentlich kleiner als EEPROM-Zellen sind. Es hat aber den Nachteil, daß eine echte Belichtungsmaske für die Halbleiterproduktion erstellt werden muß. Die Durchlaufzeit steigt aus diesem Grund erheblich gegenüber einer Softmaske. Hardmasken werden üblicherweise für große Stückzahlen bei weitgehend einheitlicher Funktionalität der Chipkarten verwendet. Das Gegenteil einer Hardmaske ist die Softmaske, bei der wesentliche Funktionen im EEPROM sind.
Hash-Funktion	Eine Hash-Funktion ist ein Verfahren zur Komprimierung von Daten mittels einer Einwegfunktion, so daß 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.
Hintergrundsystem	Alle Computersysteme, die die Verarbeitung und Verwaltung von Daten ab der Hierarchie der Terminals übernehmen.
Hochprägung	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	Eine fotografische Aufnahme bei der Holographie wird als Hologramm bezeichnet. 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.
Hot List	Liste in einer Datenbank, auf der alle Chipkarten vermerkt sind, die wahrscheinlich manipuliert sind und keinesfalls akzeptiert werden dürfen.
Hybridkarte	Hybridkarte ist die Bezeichnung für eine Karte mit zwei unterschiedlichen Kartentechnologien. Typische Beispiele sind eine Karte mit Magnetstreifen und zusätzlichem Chip oder eine Chipkarte mit optischem Speicher an der Kartenoberfläche.
ID-1 Karte	Das Standardformat für Chipkarten (Breite: ≈ 85,6 mm, Höhe: ≈ 54 mm, Dicke: ≈ 0,76 mm).
Identifizierung	Vorgang des Nachweises der Echtheit eines Gerätes oder einer Person durch Vergleich eines übergebenen Paßwortes mit einem gespeicherten Referenzpaßwort.
IEC	Die International Electrotechnical Commission [IEC] wurde 1906 gegründet und hat ihren Sitz in Genf, Schweiz. Die Aufgabe der IEC ist die weltweite Normung im Bereich der Elektrotechnik.
Initialisierer	Die Instanz, die die Initialisierung durchführt.
Initialisierung	Laden der festen und personenunabhängigen Daten einer Anwendung in das EEPROM. Ein Synonym ist die Vorpersonalisierung.
Inlettfolie	Eine Inlettfolie ist die Folie, die sich nach dem Zusammenlaminieren aller Folien im Innern des Kartenkörpers befindet, deshalb heißt sie manchmal auch 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.
Intelligente Speicherkarte	Speicherkarte mit erweiterter Logikschaltung für zusätzliche Sicherheitsfunktionen, die den Speicherzugriff überwachen.
Interpreter	Ein Interpreter ist ein Programm, das eine Programmiersprache wie BASIC oder Java zur Laufzeit in von einem Prozessor ausführbare Maschinensprache übersetzt und auch sofort ausführt. Aufgrund des zur Laufzeit stattfindenden Übersetzungsvorgangs sind interpretierte Programme immer langsamer als compilierter Programmcode. Interpreter lassen jedoch wesentlich hardwareunabhängigere Programme als Compiler zu.
ISO	Die International Standardisation Organisation [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 beschäftigte sich mit Temperaturen bei Längenmessungen.
ITSEC	Die Information Technique System Evaluation Criteria wurden 1991 veröffentlicht und sind ein Kriterienkatalog zur Beurteilung und Zertifizierung der Sicherheit von informationstechnischen Systemen im europäischen Bereich. Die Weiterentwicklung der ITSEC und Vereinheitlichung mit diversen nationalen Kriterienkatalogen sind die Common Criteria.
ITU	Die International Telecommunications Union ist eine internationale Organisation für Koordinierung, Normung und Entwicklung von globalen Telekommunikationsdiensten mit Sitz in Genf. Die Vorgängerorganisation war die CCITT [ITU].
Java	Eine von der Firma Sun entwickelte hardwareunabhängige und objektorientierte Programmiersprache, 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 sogenannten virtuellen Maschine auf der jeweiligen Zielhardware (Intel, Motorola, ...) und Betriebssystemplattform (Windows, MacOS, Unix, ...) interpretiert wird. Es gibt bereits erste Prozessoren (Pico Java), die den Bytecode von Java direkt ausführen können.
Kaltreset	siehe Reset
Kartenakzeptant	Eine Instanz, bei der Karten für eine bestimmte Form von Interaktion (z.B.: Bezahlung) verwendet werden können. Das typische Beispiel ist ein Händler, der Kreditkarten zur Bezahlung akzeptiert.

Kartenbenutzer	Der Kartenbenutzer ist die Person, die eine Karte benutzt. Sie ist deshalb der Kartenbesitzer, aber nicht unbedingt der Karteneigentümer.
Kartenbesitzer	Der Kartenbesitzer ist die Person, die die tatsächliche Verfügungsgewalt über eine Karte hat. Der Kartenbesitzer muß nicht zwangsläufig der Karteneigentümer sein.
Karteneigentümer	Der Karteneigentümer ist die natürliche oder juristische Person, die die rechtliche Herrschaft über die Karte hat und mit dieser nach Belieben verfahren kann. Bei Kredit- und Debitkarten sind sehr oft die kartenherausgebenden Banken die Eigentümer der Karten, die kartenbenutzenden Kunden sind dann lediglich die Kartenbesitzer.
Kartenherausgeber, Kartenemittent (*card issuer*)	Diejenige Instanz, die für die Ausgabe von Karten verantwortlich ist. Bei Mono-applikationskarten ist der Kartenherausgeber zugleich Anwendungsanbieter, muß es aber nicht zwangsläufig sein.
Kartenhersteller	Eine Instanz, die Kartenkörper herstellt und in sie 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	Ein mechanisch und elektrisch einfach aufgebautes Gerät, das zur Aufnahme und galvanischen Kontaktierung einer Chipkarte 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	Als Kavität wird die üblicherweise gefräste Aussparung im Kartenkörper für das zu implantierende Modul bezeichnet.
Kernfolie	siehe Inlettfolie
Kinegramm	Ein Kinegramm zeigt unter verschiedenen Blickwinkeln unterschiedliche Darstellungen. Das Kinegramm kann einen scheinbaren und ruckartigen Bewegungsablauf zeigen, oder es zeigt unterschiedliche Motive in Abhängigkeit vom Betrachtungswinkel. Kinegramme sind ähnlich, aber nicht identisch den Hologrammen, die ein 3-dimensionales Bild zeigen.
klonen	Angriff auf ein Chipkartensystem durch vollständiges Kopieren von ROM und EEPROM eines Mikrocontrollers.
Kommando-APDU (*command-APDU*)	Eine Kommando-APDU ist ein Kommando vom Terminal an die Chipkarte und 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.
komplettieren	Vervollständigen des Betriebssystems durch Laden der EEPROM-Teile. Dies ermöglicht nachträgliche Änderungen und Anpassungen ohne daß eine neue ROM-Maske erstellt werden muß. Beim Komplettieren werden in jede Chipkarte identische Daten geschrieben, es ist also dem Prinzip nach eine Art Initialisierung.
kontaktlose Karte	Karte, bei der die Energie- und Datenübertragung berührungslos durch elektromagnetische Felder erfolgt.
Kreditkarte	Eine Karte mit oder ohne Chip, die einen Verfügungsrahmen aufweist, bei der aber die Bezahlung zeitlich nach Erhalt des Gutes oder der Dienstleistung stattfindet. Schlagwort dazu: „buy now – pay later“. Das typische Beispiel sind hochgeprägte Kreditkarten.
kryptografischer Algorithmus	Ein kryptografischer Algorithmus ist eine Rechenvorschrift mit mindestens einem geheimen Parameter (dem Schlüssel), 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.
Ladebeauftragter (*load agent*)	Der Ladebeauftragte ist diejenige Instanz, welche das Laden von elektronischen Geldeinheiten auf eine elektronische Geldbörse vornimmt. Er ist sozusagen das Gegenstück zum Leistungsanbieter.
Laminieren	Das Verkleben von dünnen Materialschichten unter Druck und Hitze bezeichnet man als Laminierung.

Lasergravur	Verfahren zur Schwärzung von speziellen Kunststoffschichten durch Verbrennen mit einem Laser. Der Vorgang der Lasergravur wird umgangssprachlich oft auch „lasern“ genannt.
Leistungsanbieter (*service provider*)	Der Leistungsanbieter ist 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.
Linker	Ein Linker hat die Aufgabe, die symbolischen Speicheradressen eines compilierten oder assemblierten Programmcodes in absolute oder relative Speicheradressen umzusetzen.
little Endian	siehe Endianness
MAC	Der MAC (*message authentication code* – Datensicherungscode) ist eine 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 (*cryptographic checksum*).
Magnetkarte	Eine oft verwendete und sachlich nicht korrekte Kurzform des Begriffs Magnetstreifenkarte (siehe Magnetstreifenkarte).
Magnetstreifenkarte	Karte mit einem Magnetstreifen, auf dem Daten geschrieben und wieder gelesen werden können. Der Magnetstreifen enthält meist 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.
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.
Mikroprozessorkarte	Eine Mikroprozessorkarte ist eine Karte mit Chip, welcher einen Mikrocontroller mit CPU, flüchtigem (RAM) und nichtflüchtigem (ROM, EEPROM, ...) Speicher besitzt. Mikroprozessorkarten können noch einen numerischen Coprozessor (NPU) haben, um Public-Key-Kryptoalgorithmen schnell ausführen zu können. Diese Art von Karten werden manchmal auch Kryptokarten oder Kryptocontrollerkarten genannt.
Modul	Der Träger und die Halterung für ein Die mit darauf angeordneten Kontaktelementen wird als Modul bezeichnet.
Modulhersteller	Eine Instanz, die Dice in Module einbaut und eine elektrische Verbindung durch Bonden mit den Kontaktelementen herstellt.
Monoapplication-Chipkarte	Der Begriff Monoapplication-Chipkarte sagt aus, daß sich auf einer Chipkarte nur eine Anwendung befindet.
monofunktionale Chipkarte	Monofunktionale Chipkarten sind Prozessorchipkarten, deren Betriebssystem nur eine einzige Anwendung unterstützt und unter Umständen sogar auf diese Anwendung hin optimiert wurde. Verwaltungsfunktionen für Anwendungen (z.B.: Generieren und Löschen von Dateien) werden von monofunktionalen Chipkarten entweder überhaupt nicht, oder nur in sehr eingeschränkter Form unterstützt.
MoU	Das Memorandum of Understanding ist die gemeinsame rechtliche Grundlage aller GSM-Netzbetreiber.
Multiapplication-Chipkarte	Der Begriff Multiapplication-Chipkarte sagt, aus, daß sich auf einer Prozessorchipkarte mehrere Anwendungen befinden, z.B. eine Bankkarte mit Telefonfunktion.
multifunktionale Chipkarte	Unter dem Begriff der „multifunktionalen Chipkarte“ versteht man üblicherweise Prozessorchipkarten, die mehrere Anwendungen unterstützen und die entsprechende Verwaltungsfunktionen für die Anlage und das Löschen von Anwendungen und Dateien haben. Die Bezeichnung „multifunktional“ wird allerdings in so inflationärer Form benutzt, das heute beinahe kein Chipkarten-Betriebssystem mehr existiert, daß nicht mit „Multifunktionalität“ aufwarten kann. Spötter meinen manchmal, daß jede Karte grundsätzlich immer mehrere Funktionen hat. Als Eiskratzer für vereiste Autoscheiben läßt sie sich zumindest allemal verwenden.

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.
Nativcode (*native code*)	Unter Nativcode versteht man ein Programm in dem spezifischen Maschinencode für den Prozessor, auf dem er ausgeführt wird.
NBS	National Bureau of Standards war die frühere (vor 1988) Bezeichnung des NIST.
NCSC	Das US amerikanische National Computer Security Center ist eine Unterorganisation des NSA, zuständig für die Prüfung von Sicherheitsprodukten und Herausgeber von Kriterien für sichere Computersysteme, u.a. der TCSEC.
negative file	siehe Black List
Nibble	Die vier höherwertigen oder niederwertigen Bits eines Bytes.
Nichtabstreitbarkeit (*non-repudiation*)	Unter Nichtabstreitbarkeit einer Nachricht versteht man kryptografische Verfahren, die sicherstellen, daß der Empfänger den 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 Rückanwort“ bei der konventionellen Briefpost.
nichtflüchtige Speicher (*non-volatile memory*)	Eine Speicherart (z.B. ROM, EPROM, EEPROM), die ihren Inhalt auch ohne Stromzufuhr behält.
NIST	Das US-amerikanische National Institute of Standards and Technology 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	Eine Norm ist ein 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 einen nationalen oder internationalen Normungsgremium (z.B.: ISO, CEN, ANSI, ETSI) benutzt. Eine Norm ist nicht mit einem Standard gleichzusetzen (siehe auch: Standard).
NSA	Die US-amerikanische National Security Agency 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 dekodieren. Die Entwicklung neuer Kryptoalgorithmen und Beschränkung des Einsatzes von bestehenden fällt ebenfalls in das Aufgabengebiet dieser Behörde.
Nutzdaten	Diejenigen Daten, die direkt für eine Anwendung notwendig sind.
Nutzen	Ein Nutzen ist 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.
offene Anwendung	Anwendung auf einer Chipkarte, die unterschiedlichen Leistungsanbietern (z.B.: Händlern, Dienstleistern) ohne notwendige Rechtsbeziehung untereinander zur Verfügung steht.
offene Börse	Realisation einer offenen Anwendung für eine elektronische Geldbörse. Mit ihr können allgemeine Zahlungstransaktionen für unterschiedliche Leistungsanbieter getätigt werden.

Optische Speicherkarte	Karte, bei der Informationen in einer reflektierenden Schicht auf der Kartenoberfläche eingebrannt sind (analog einer CD).
Padding	Unter Padding versteht man die Erweiterung eines Datenstrings mit 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.
Passivierung	Schutzschicht auf einem Halbleiter, um ihn vor Oxidation und anderen chemischen Vorgängen zu schützen. Vor einer Manipulation des Halbleiters muß sie entfernt werden.
Patch	Ein Patch ist in der Softwareentwicklung ein kurzes Programm, oft direkt in Maschinencode geschrieben, das die Funktionalität eines vorgegebenen Programms ergänzt oder abändert. Patches werden in der Regel zur schnellen und unkomplizierten Korrektur eines Programmfehlers benutzt.
Patent	Ein Patent ist ein 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	Der Ausdruck „Pay before“ 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 elektronischen Geldbörsen, die vor dem Einkauf mit elektronischem Geld geladen werden müssen.
Pay later	Der Ausdruck „Pay later“ 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 before 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.
Pay now	Der Ausdruck „Pay now“ 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 Bezahlenden auf das Konto des Händlers zu transferieren.
Personalisierer	Die Instanz, die die Personalisierung durchführt.
Personalisierung	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.
PIN-Pad	Ein PIN-Pad ist im ursprünglichem Sinne die mechanisch und kryptografisch besonders geschützte Eingabetastatur bei Terminals. Im allgemeinen Sprachgebrauch wird aber oft auch das ganze Terminal als PIN-Pad bezeichnet.
PKCS #1 ... 11	Die Public Key Cryptografy Standards sind von der Firma RSA Inc. veröffentlichte Regelwerke für die Anwendung von asymmetrischen Kryptoalgorithmen, wie z.B. RSA.
Plug-In	Chipkarte in sehr kleinem Format, die vor allem im GSM-Bereich Verwendung findet (Breite: ≈ 25 mm, Höhe: ≈ 15 mm, Dicke: ≈ 0,76 mm).
polling	Laufendes programmgesteuertes Abfragen eines Eingabekanals zur Detektion einer eingehenden Nachricht. Polling benötigt je nach Wiederholrate der stattfindenden Abfragen unter Umständen große Rechenleistung. Üblicherweise wird eine von der Rechnerhardware unterstützte Abfrage mittels Interrupt bevorzugt.
Prozessor	Die wichtigste Funktionseinheit auf einem Mikrocontroller. Sie führt die im Programm festgelegten Maschinenbefehle und Speicherzugriffe aus. Der Begriff CPU (*central processing unit*) wird oft als Synonym zu Prozessor gebraucht.
Prozessorkarte	Der Ausdruck Prozessorkarte ist die Kurzform von Mikroprozessorkarte (siehe Mikroprozessorkarte).
Purse-to-Purse-Transaktion	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 (Hauptschlüssel) benützen müssen.

RAM (*random access memory*)	Eine 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.
rauschfreiheit	Eigenschaft eines kryptografischen Algorithmus. Dieser benötigt bei Rauschfreiheit unabhängig von Schlüssel, Klar- und Schlüsseltext für die Ver- und Entschlüsselung immer die gleiche Zeit. Ist ein kryptografischer Algorithmus nicht rauschfrei, so kann durch eine Analyse der Berechnungszeit der Schlüsselraum sehr stark eingeschränkt werden. Dadurch kann der Schlüssel wesentlich schneller als bei einer erschöpfenden Schlüsselsuche gefunden werden.
Record	Ein Record (Datensatz) ist eine bestimmte Anzahl von Daten ähnlich einem String.
Red List	siehe Hot List
Reset	Ein Reset bedeutet das Zurücksetzen eines Computers (in diesem Zusammenhang: 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 angeschalten wird. Ein Warmreset wird durch ein Signal auf der Resetleitung zur Chipkarte ausgeführt, die Versorgungsspannung bleibt davon unberührt.
ROM (*read only memory*)	Eine 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.
ROM-Maske	Halbleitertechnische Belichtungsmaske für die Herstellung des ROM bei der Halbleiterfertigung. Der Ausdruck wird aber ebenfalls für den Dateninhalt des ROMs bei Chipkarten-Mikrocontrollern verwendet.
Sammelbeauftragter	siehe Acquirer
Sandbox	siehe Virtual Machine
Schlechtfall	Der Fall bei einer logischen Entscheidung, der zum ungünstigeren oder ungewollten Ergebnis führt.
Schlüsselmanagement (*key management*)	Unter Schlüsselmanagement versteht man alle Verwaltungsfunktionen für die Erzeugung, Verteilung, Speicherung, Aktualisierung, Vernichtung und Adressierung von kryptografischen Schlüsseln.
Scrambling	Vermischte Anordnung der Busse (Adreß-, Daten- und Steuerbus) auf dem Chip eines Mikrocontrollers, 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 gescrambelt.
Secure Messaging	Datenübertragung auf einer Schnittstelle, die gegen Manipulationen (Sicherung mit MAC, d.h. Authentic-Mode) oder Abhören (Verschlüsselung, d.h. Combined-Mode) gesichert ist.
Seitenorientierung	Zusammenfassung von mehreren Bytes in einem Speicher zu sogenannten Seiten, die nur als Ganzes geschrieben oder gelöscht werden können. Eine Seitenorientierung ist bei Chipkarten-Mikrocontrollern nur für das EEPROM vorhanden. Die übliche Größe einer Speicherseite beträgt zur Zeit 4 Byte bzw. 32 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 32 Byte.
SET	Der Secure Electronic Transaction Standard ist ein Zahlungsverkehrsprotokoll zur Abwicklung von sicheren Kreditkartenzahlungen im Internet. Es wurde von Visa und Mastercard definiert. 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 (noch) nicht international standardisiert.
Short-FID	Der Short-FID ist ein 5 Bit langes Kennzeichen für EFs und hat den Wertebereich 1 bis 31. Er wird zur impliziten Selektion eines EFs innerhalb eines Schreib- oder Lesekommandos (z.B.: READ BINARY) an die Chipkarte benutzt.
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 Abscheiden 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 dient (*secure application module – SAM, hardware security module – HSM*).
Signaturgesetz (SigG)	Der Artikel 3 des deutschen „Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG)“ vom 13. Juni 1997 wird als Signaturgesetz bezeichnet. Darin sind die Rahmenbedingungen für den Einsatz von digitalen Signaturen in Deutschland vorgegeben.
Signaturverordnung (SigV)	In der deutschen Signaturverordung vom 8. Oktober 1997 werden die Rahmenbedingungen, die vom Signaturgesetz 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.
SIM	Das Subscriber Identity Module ist eine andere Bezeichnung für die GSM-spezifische Chipkarte. Sie kann die übliche Kreditkartengröße ID-1 haben oder auch als kleine Plug-In-Karte in ID-000 ausgeführt sein. Das SIM ist der Träger der geheimen Authentisierungsinformationen für den Netzbetreiber und enthält zusätzlich noch benutzerspezifische Daten, wie beispielsweise Telefonnummern, für das Mobiltelefon. Der Nachfolger des SIM bei UMTS ist das USIM (siehe: USIM).
SIMEG	Die Subscriber Identity Module Expert Group war eine Expertengruppe, die im Rahmen von ETSI die Spezifikation für die Schnittstelle zwischen Chipkarte und Mobiltelefon festgelegt hat (GSM 11.11). Der Name SIMEG wurde 1994 durch SMG9 ersetzt.
Sitzung	Diejenige Zeitspanne zwischen An- und Abschaltsequenz einer Chipkarte, in der sowohl der gesamte Datenaustausch als auch die dazu notwendigen informationstechnischen Mechanismen ablaufen.
Smart Card	Der Begriff „Smart Card“ ist ein anderer Ausdruck für Mikroprozessorkarte. Er steht für eine Chipkarte, die „smart“, also schlau ist, weshalb Speicherkarten nicht mehr unter diesem Überbegriff fallen.
Smartcard	Der Begriff Smartcard ist ein eingetragenes Warenzeichen der kanadischen Firma Groupmark [Groupmark].
SMG9	Die Special Mobile Group 9 ist eine Expertengruppe, die im Rahmen von ETSI die Spezifikation für die Schnittstelle zwischen Chipkarte und Mobiltelefon festlegt (GSM 11.11). Sie setzt sich aus Vertretern von Karten-, Mobiltelefonherstellern und Netzbetreibern zusammen. Der frühere Name der SMG9 war SIMEG.
Softmaske (*softmask*)	Der Begriff Softmaske bedeutet, daß sich aufbauend auf einem Chipkarten-Betriebssystem im ROM ein Teil des Programmcodes im EEPROM befindet. 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 für kleinere Stückzahlen (z.B.: Feldversuche) bei rapid prototyping verwendet. Das Gegenteil einer Softmaske ist die Hardmaske, bei der die wesentlichen Funktionen Teile des ROMs sind.
Speicherkarte	Eine Karte mit Chip, welcher eine einfache Logikschaltung mit zusätzlichem schreib- und lesbaren Speicher besitzt. Speicherkarten können zusätzlich noch Sicherheitsbaugruppen aufweisen, welche beispielsweise eine Authentisierung ermöglichen.
Sperrliste (*black list*)	Liste in einer Datenbank, auf der alle Chipkarten vermerkt sind, die in einer bestimmten Anwendung nicht mehr verwendet werden dürfen.
SRAM (*static random access memory*)	Ein RAM-Speicher in statischer Bauweise benötigt zum Erhalt des Speicherinhalts lediglich eine konstante Stromversorgung und keine zyklische Wiederauffrischung des Inhalts. Die Zugriffszeit auf SRAM-Speicher ist geringer als auf DRAM-Speicher, allerdings benötigen SRAMs mehr Platz auf dem Chip und sind deshalb auch teurer.

Stack	Ein Stack ist eine Datenstruktur, in dem die zuletzt abgelegten Objekte als erste wieder entfernt werden können (*last in first out – LIFO*). Der wohl bekannteste Stack ist der Programmstack, auf dem beim Aufruf von Unterprogrammen die Rücksprungadressen abgelegt werden.
Standard	Als Standard werden in diesem Buch 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 (siehe auch: Norm). Verwirrenderweise werden in Deutschland die beiden Begriffe Norm und Standard oft gleichwertig verwendet, was in Wirklichkeit nicht korrekt ist.
Steganografie	Der 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. 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.
Super Smart Card	Unter dem Begriff „Super Smart Card“ versteht man eine Chipkarte mit integrierten aufwendigen Kartenelementen wie Display und Tastatur.
TCSEC	Die Information Technique System Evaluation Criteria wurden 1985 vom NCSC veröffentlicht und sind ein Kriterienkatalog zur Beurteilung und Zertifizierung der Sicherheit von informationstechnischen Systemen im US-amerikanischen Bereich. Der Nachfolger der nationalen TCSEC werden die international gültigen Common Criteria.
TDES	siehe Triple-DES
Teiler	In der Chipkartenwelt gebräuchliche Kurzform von clock rate conversion factor (CRCF). Der CRCF gibt die Dauer eines Bits bei der Datenübertragung in der Anzahl der Takte auf der Clock-Leitung an.
Terminal	Das Gegenstück zur Chipkarte ist das Terminal. Es ist ein Gerät, z.T. mit Tastatur und Display, das die elektrische Versorgung und den Datenaustausch mit der Chipkarte ermöglicht.
Testing	Beim Testing wird ein bereits debugtes Programm auf seine Funktionsfähigkeit geprüft. Das vorrangige Ziel ist nicht die Suche nach Fehlern im Programm, sondern die Prüfung der erwarteten Funktionen. Das Testing ist deshalb nicht identisch mit dem Debugging.
Thread	siehe Multithreading
TLV-Format	Ein Datenformat nach ASN.1, bei dem ein Datum (*value*) durch ein vorangestelltes Kennzeichen (*tag*) und die Länge (*length*) eindeutig beschrieben wird. Das TLV-Format läßt auch verschachtelte Datenobjekte zu.
TPDU	siehe APDU
Transaktionsnummer (TAN)	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 (z.B.: in Form einer vierstelligen Zahl) ausgedruckt auf Papier, die dann exakt in der vorgegebenen Reihenfolge für die einzelnen Transaktionen bzw. Sitzungen benutzt werden müssen.
Transferkarte	Eine Chipkarte, die als Transportmedium zwischen zwei Instanzen genutzt wird. Dazu besitzt sie einen großen Datenspeicher und in der Regel Schlüssel für eine Authentisierung, ob die zu transferierenden Daten von der jeweiligen Stelle gelesen bzw. geschrieben werden dürfen.
Transportprotokoll	Ein anderer Ausdruck für Übertragungsprotokoll (siehe Übertragungsprotokoll).
Triple-DES	Der Triple-DES, auch TDES und 3 DES genannt, ist eine modifizierte DES-Verschlüsselung durch aufeinanderfolgenden dreifachen Aufruf des DES-Algorithmus mit abwechselnder Ver- und Entschlüsselung. Wird für die drei DES-Aufrufe der gleiche Schlüssel verwendet, dann entspricht die Triple-DES-Verschlüsselung einer normalen DES-Verschlüsselung. Werden hingegegen zwei bzw. drei unterschiedliche Schlüssel verwendet, dann stärkt dies die DES-Verschlüsselung erheblich gegenüber einer einfachen DES-Verschlüsselung.
trojanisches Pferd	Historisch gesehen, das Holzpferd, in dem es Odysseus gelang, sich Zutritt zur stark befestigten Stadt Troja zu erschleichen. In der modernen Fassung ein Programm, das vordergründig eine definierte Aufgabe erfüllt, aber zusätzliche und unbekannte Funktionen ausführen kann. Es wird bewußt in ein Computersystem oder Wirtsprogramm eingebracht und kann sich im Gegensatz zu Viren nicht vermehren.

Übertragungsprotokoll	Als Übertragungsprotokoll werden in der Chipkartenwelt die Mechanismen für das Senden und Empfangen von Daten zwischen Terminal und Chipkarte bezeichnet. Das Übertragungsprotokoll beschreibt im Detail die benutzten OSI-Protokollschichten, den Datenaustausch im Gutfall, Fehlererkennungsmechanismen und Reaktionsmechanismen bei Fehlern.
UIM (*user identity module*)	Veralteter Begriff für USIM (siehe USIM).
Unicode	Unicode ist eine 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 verbreitetsten Sprachen dieser Welt zu unterstützen. Die ersten 256 Zeichen von Unicode sind mit ASCII nach ISO 8859-1 identisch. Die WWW-Seite des Unicode-Konsortiums ist [Unicode].
Upload	Übertragen von Daten von einem untergeordneten System (z.B. Terminal) an ein übergeordnetes System (Hintergrundsystem, Host). Das Gegenteil ist der „Download“.
USIM (*universal subscriber identity module*)	Das Universal Subscriber Identity Module ist eine andere Bezeichnung für die UMTS-spezifische Chipkarte. Sie kann die übliche Kreditkartengröße ID-1 haben oder auch als kleine Plug-In-Karte in ID-000 ausgeführt sein. Das USIM ist der Träger der geheimen Authentisierungsinformationen für den Netzbetreiber und enthält zusätzlich noch benutzerspezifische Daten, wie beispielsweise Telefonnummern, für das Mobiltelefon.
Verwaltungsdaten	Daten, die nur zur Verwaltung von Nutzdaten dienen und für eine Anwendung keinerlei sonstige Bedeutung haben.
Virginalkarte	Karte, die noch nicht mit einem Chip versehen und noch nicht optisch oder elektrisch personalisiert ist. Eine Virginalkarte ist im wesentlichen ein bedruckter, uniformer Kartenkörper, wie er in der Massenproduktion von Karten hergestellt wird.
Virtual Machine (VM)	Eine Virtual Machine ist ein in Software simulierter Mikroprozessor mit u.U. eigenem Opcode für die Maschinenbefehle und einem (ebenfalls simuliertem) Adreßraum. Dadurch wird eine von den Hardwaregegebenheiten 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.
Visa Easy Entry (VEE)	Visa Easy Entry ist ein Verfahren für die unproblematische Migration von magnetstreifenbasierten Kreditkarten hin zu Kreditkarten mit Mikrocontrollerchip. Dazu werden der Name des Kartenbesitzers und alle Daten der Magnetstreifenspur in einem EF unter einem für Visa reservierten DF abgelegt. Bei einer Kreditkartenbezahlung liest das Terminal die für diese Transaktion notwendigen Daten statt vom Magnetstreifen aus dem Chip. Der Vorteil des Verfahrens ist, daß nur am POS das Terminal mit einer Chipkartenkontaktiereinheit umgerüstet werden muß und das gesamte Hintergrundsystem ohne Änderungen weiter betrieben werden kann.
Vorpersonalisierung	Vorpersonalisierung ist eine andere Bezeichnung für Initialisierung(siehe Initialisierung).
Warmreset	siehe Reset
White List	Liste in einer Datenbank, auf der alle Chipkarten vermerkt sind, die in einer bestimmten Anwendung verwendet werden dürfen.
Whitebox Test	Beim Whitebox 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.
work around	Ein work around ist 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 nur seine negativen Auswirkungen auf den Rest des Programms. Typischerweise werden work arounds im EEPROM von maskenprogrammierten Chipkarten-Betriebssystemen gemacht, da sich der Programmcode im ROM nachträglich nicht mehr verändern läßt.
WWW, W3	Das World Wide Web ist ein Teil des weltweiten Internets und vor allem durch die Möglichkeit der beliebigen Verknüpfung von Dokumenten durch Hyperlinks und die Integration von multimedialen Objekten in Dokumente bekannt.

X.509	Die X.509-Norm definiert Aufbau und Codierung von Zertifikaten. Sie ist die weltweit am häufigsten eingesetzte Norm für Zertifikatsstrukturen.
Zertifikat	Ein Zertifikat ist ein von einer vertrauenswürdigen Instanz digital signierter öffentlicher Schlüssel, damit dieser als authentisch anerkannt werden kann. Die verbreitetste und bekannteste Festlegung des Aufbaus und Codierung von Zertifikaten ist die X.509-Norm.
ziffern	Ziffern ist das 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	Der Zentrale Kreditausschuß (ZKA) ist in Deutschland der Koordinator 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.

