
[Dallas Semi]	Dallas Semiconductor, USA Halbleiterhersteller, Sicherheitsprozessoren http://www.dalsemi.com/
[Datacard]	Datacard, USA Produktionsmaschinen für Chipkarten http://www.datacard.com/
[De La Rue]	De La Rue Card Systems, Großbritannien Chipkartenhersteller http://www.delarue.com/
[DIN]	Deutsches Institut für Normung e.V. (DIN), Deutschland Normen http://www.din.de/
[Diners]	Diners-Club, USA Kartenherausgeber http://www.diners-club.com/
[DPA]	Deutsches Patentamt, Deutschland Patente http://www.deutsches-patentamt.de/
[Drexler]	Drexler Technology Corp., USA Karten mit optisch les- und schreibbarem Bereich http://www.lasercard.com/
[ECBS]	European Committee for Banking Standards Normen, Standards http://www.ecbs.org/
[ECC]	The Error Correcting Codes (ECC) Home Page, Japan Link-Farm zu Fehlererkennungs- und Korrekturcodes http://www.csl.sony.co.jp/person/morelos/ecc/codes.html
[Emosyn]	Emosyn Hersteller von Chipkarten-Mikrocontrollern http://www.emosyn.com/
[EMV]	EMVCO Informationen über EMV http://www.emvco.com/
[Entrust]	Entrust, Kanada Kryptografie http://www.entrust.com/
[Eracom]	Eracom Pty. Ltd., Australien Kryptografie http://www.eracon.com.au/
[ETSI]	ETSI Normen http://www.etsi.fi/

[Europay]	Europay International, Belgien Kartenherausgeber http://www.europay.com/
[Eurosmart]	Eurosmart Informationen über Chipkarten http://www.eurosmart.com
[FD]	F+D Feinwerk- und Drucktechnik GmbH, Deutschland Hersteller von Maschinen für Desktop-Personalisierung http://www.fundo.de/
[FINEID]	FINEID, Finnland Informationen über FINEID http://www.fineid.fi/
[Fischer]	Fischer International Systems Corporation, USA Terminalhersteller http://www.fisc.com/
[GD]	Giesecke & Devrient GmbH, Deutschland Chipkartenhersteller http://www.gieseckedevrient.com/ http://www.gi-de.com/
[Gemplus]	Gemplus S.C.A., Frankreich Chipkartenhersteller http://www.gemplus.com/
[Global Platform]	Global Platform Informationen über Global Plattform http://www.globalplatform.org/
[Groupmark]	Groupmark Ltd., Kanada Chipkartenhersteller http://www.groupmark.com/
[GSM]	GSM Association Informationen über GSM http://www.gsmworld.com/
[Gutmann]	Peter Gutmann's Security and Encryption Links http://www.cs.auckland.ac.nz/~pgut001/
[GZS]	Gesellschaft für Zahlungssysteme (GZS) GmbH, Deutschland elektronischer Zahlungsverkehr, Clearing http://www.gzs.de/
[Hanser]	Carl Hanser Verlag GmbH, Deutschland Handbuch der Chipkarten, The Smart Card Simulator http://www.hanser.de/
[Hekuma]	Hekuma, Germany Spritzgusskarten http://www.hekuma.com/

[Hitachi]	Hitachi Ltd. Japan Hersteller von Chipkarten-Mikrocontrollern http://www.hitachi.com/ http://www.hitachi.co.jp/
[Hypercom]	Hypercom Corp., USA Terminalhersteller http://www.hypercom.com/
[IATA]	International Air Transport Association (IATA) http://www.iata.org/
[ICMA]	ICMA – International Card Manufacturers Association Informationen über Chipkarten http://www.icma.com/
[IEC]	IEC Normen http://www.iec.ch/
[IEEE]	IEEE Normen http://www.ieee.org/
[IMT-2000]	IMT-2000 Informationen über IMT-2000 www.imt-2000-online.com/
[Infineon]	Infineon AG, Deutschland Hersteller von Chipkarten-Mikrocontrollern http://www.infineon.de/
[Ingenico]	Ingenico, Frankreich Terminalhersteller http://www.ingenico.com/
[Innovatron]	Groupe Innovatron, Frankreich Patente, Beratung http://www.innovatron.com/
[Integri]	Integri, Belgien Test von Chipkarten-Betriebssystemen http://www.integri.be/
[Intel]	Intel, USA Halbleiterhersteller http://www.intel.com/
[Iridium]	Iridium, USA Informationen über das Mobilfunknetz Iridium http://www.iridium.com/
[ISO]	ISO Normen http://www.iso.ch/

[ITU]	ITU Normen http://www.itu.ch/
[JavaPOS]	JavaPOS Java für POS-Terminals http://www.javapos.com/
[Javasoft]	Javasoft, USA Java für Chipkarten http://www.javasoft.com/
[JCB]	JCB, USA Kartenherausgeber http://www.jcb.com/
[JCF]	Java Card Forum, USA Informationen und Spezifikationen über Java Card http://www.javacardforum.org/
[JTC1]	ISO, Joint Technical Commettee One Internationale Normung http://www.jtc1.org/
[JYA]	JYA, USA Kryptografie http://www.jya.com/
[Kaba]	Kaba Holding AG, Deutschland kontaktlose Chipkarten http://www.kaba.com/
[Krone]	Krone GmbH, Deutschland Terminalhersteller http://www.krone-gmbh.de/
[Kryptocom]	Kryptokom GmbH, Deutschland Kryptografie http://www.kryptokom.com/
[Logika]	Logika Comp Spa, Italien Personalisierungssysteme http://www.logika.it/
[MagTek]	MagTek Inc., USA Terminalhersteller http://www.magtek.com/
[Maosco]	Maosco Ltd., Großbritannien Chipkarten-Betriebssystem http://www.multos.com/
[Mastercard]	Master Card International, USA Kartenherausgeber http://www.mastercard.com/

[Meinen Ziegel]	Meinen, Ziegel & Co., Deutschland Maschinen für Kartenfertigung http://www.royonix.com/
[Microsoft]	Microsoft, USA Crypto-API, PC/SC http://www.microsoft.com/
[MIPS]	MIPS Hersteller von Prozessoren http://www.mips.com/
[MIT]	Massachusetts Institute of Technology (MIT), USA Kryptografie http://www.mit.edu/
[Mondex]	Mondex International Ltd., Großbritannien elektronische Geldbörse http://www.mondex.com/
[Mühlbauer]	Mühlbauer GmbH, Deutschland Maschinen für Kartenfertigung http://www.muehlbauer.de/
[MUSCLE]	MUSCLE (<i>Movement for the Use of Smart Cards in a Linux Environment</i>) MUSCLE Projekt zur Anbindung von Chipkarten in Linux-Systeme http://www.linuxnet.com/
[NCSC]	National Computer Security Center (NCSC), USA Kryptografie http://www.ncsa.uiuc.edu/
[NIST]	National Institute of Standards and Technology (NIST), USA Normen http://www.nist.gov/
[NSA]	National Security Agency (NSA), USA Informationen über Sicherheit, Kryptografie http://www.nsa.gov/
[Oberthur]	Oberthur Smart Cards, USA Chipkartenhersteller http://www.oberthur.com/
[OCF]	OCF Spezifikation OCF http://www.opencard.com/
[Oki]	Oki, Japan Hersteller von Chipkarten-Mikrocontrollern, Terminalhersteller http://www.oki.com/ http://www.oki.co.jp/

[OMG]	Object Management Group Informationen über UML http://www.omg.com/
[Orga]	Orga GmbH, Deutschland Chipkartenhersteller http://www.orga.com/
[OTP]	Open Trading Protocol Zahlungsverkehr in offenen Netzen http://www.otp.org/
[PC/SC]	PC/SC Arbeitsgruppe, USA Spezifikation PC/SC http://www.smartcardsys.com/
[Philips]	Philips, Deutschland Hersteller von Chipkarten-Mikrocontrollern http://www.philips.com/ http://www.semiconductors.philips.com/
[Protechno]	Protechno Card GmbH, Deutschland Hersteller von Maschinen für Desktop-Personalisierung http://www.protechno-card.com/
[Proton]	Proton elektronische Geldbörse Proton http://www.protonworld.com/
[Radicchio]	Radicchio PKI http://www.radicchio.org/
[Rankl]	Homepage von Wolfgang Rankl Errata Listen des Handbuchs der Chipkarten und Smart Card Handbook, The Smart Card Simulator, diese Liste als HTML-Dokument http://www.wrinkl.de/
[RFC]	RFC Server Internet Standards RFC http://www.rfc.net/
[RFID]	RFID Handbook Informationen über RF-ID http://www.rfid.com/
[RSA]	RSA Inc., USA Kryptografie, PKCS-Standards http://www.rsa.com/
[SCARD]	Smart Card Developer Association, USA Angriffe, Software http://www.scard.org/

[Schlumberger]	Schlumberger Ltd., Frankreich Chipkartenhersteller http://www.slb.com/
[SCIA]	Smart Card Industry Association Informationen über Chipkarten http://www.scia.org/
[Secude]	Secude GmbH, Deutschland Sicherheitstechnik http://www.secude.com/
[Security Dynamics]	Security Dynamics Technologies Inc., USA Sicherheitstechnologie http://www.securid.com/
[SEIS]	SEIS Swedish Secured Electronic Information in Society Specification, Schweden Normen http://www.seis.se/
[Semper]	SEMPER E-Commerce http://www.semper.org/
[SEPT]	SEPT, Frankreich Normen http://www.sept.fr/
[SET]	Secure Electronic Transaction LLC, USA SET Homepage http://www.setco.org/
[SETEC]	SETEC, Finnland Chipkartenhersteller http://www.setec.fi/
[Siemens]	Siemens, Deutschland Chipkarten-Betriebssystem http://www.siemens.com/
[SIM Alliance]	SIM Alliance S@T-Browser http://www.simalliance.org/
[Smart Card Club]	The Smart Card Club http://www.smartcardclub.co.uk/
[Smarttrust]	Smarttrust Mikrobrowser-Technologie für Chipkarten http://www.smarttrust.com/
[STM]	ST Microelectronics, Frankreich Hersteller von Chipkarten-Mikrocontrollern http://www.st.com/

[Tatu]	Tatu Ylönen's Security and Encryption Links, Finnland Link-Farm über Kryptografie http://www.ssh.fi/tech/crypto/
[TC]	TC Trustcenter GmbH, Deutschland Trustcenter http://www.trustcenter.de/
[Techno Data]	Techno Data, Deutschland Magnetstreifenkarten, Chipkarten http://www.techndata-ibk.com/
[Telesec]	Telesec, Deutschland Chipkarten-Betriebssystem http://www.telesec.de/
[Teletrust]	Teletrust, Deutschland http://www.teletrust.de/
[TETRA]	TETRA Informationen über TETRA http://www.tetramou.com/
[TI]	Texas Instruments Inc., USA Halbleiterhersteller http://www.ti.com/
[TIA]	Telecommunications Industry Association Normen http://www.tiaonline.org/
[TNO]	TNO – Netherlands Organization for Applied Research, Niederlande Hardwaretests von Mikrocontrollern http://www.tno.nl/
[Topac]	Topac GmbH Hologramme http://www.topac.de/
[Ubiq]	UbiQ Inc., USA Personalisierung http://www.ubiqinc.com/
[UCL]	UCL – Microelectronics Laboratory, Belgien Kryptografie http://www.dice.ucl.ac.be/
[UMTS-Forum]	UMTS Forum Informationen über UMTS http://www.umts-forum.org/
[Uni Siegen]	Universität Siegen, Deutschland Kryptografie http://www.uni-siegen.de/

[Unicode]	Unicode Konsortium Informationen über Unicode <i>http://www.unicode.org/</i>
[USB]	USB <i>http://www.usb.org/</i>
[Utimaco]	Utimaco AG, Deutschland Terminalhersteller <i>http://www.utimaco.com/</i>
[Verifone]	Verifone Inc., USA Terminalhersteller <i>http://www.verifone.com/</i>
[Visa]	Visa International, USA Kartenherausgeber <i>http://www.visa.com/</i> <i>http://www.visa.de/</i>
[WAP]	WAP Forum Informationen über WAP <i>http://www.wapforum.org/</i>
[Wiley]	John Wiley & Sons, Inc., Großbritannien Smart Card Handbook <i>http://www.wiley.co.uk/</i>
[Zeitcontrol]	Zeitcontrol Cardsystems GmbH, Deutschland Chipkartenhersteller <i>http://www.zeitcontrol.de/</i>

16.11 Kennwerte und Tabellen

16.11.1 Zeitbereich für den ATR

Diese Tabelle definiert den Zeitraum, in dem der ATR nach einem Reset ausgesendet werden muss.

Tabelle 16.9 Bitbereich, in dem der ATR von der Chipkarte gesendet werden muss

Takt	Mindestzeit – 400 Takte	Maximalzeit – 40 000 Takte
1,0000 MHz	0,400 ms	40,000 ms
2,0000 MHz	0,200 ms	20,000 ms
3,0000 MHz	0,133 ms	13,333 ms
3,5712 MHz	0,112 ms	11,201 ms
4,0000 MHz	0,100 ms	10,000 ms
4,9152 MHz	0,081 ms	8,138 ms
5,0000 MHz	0,080 ms	8,000 ms
6,0000 MHz	0,067 ms	6,667 ms
7,0000 MHz	0,057 ms	5,714 ms
8,0000 MHz	0,050 ms	5,000 ms
9,0000 MHz	0,044 ms	4,444 ms
10,0000 MHz	0,040 ms	4,000 ms

16.11.2 Umrechnungstabelle für Datenelemente des ATR

Grundlage für diese Tabelle ist die Definition der Datenelemente CWT und BWT im ATR nach ISO/IEC 7816-3. Die Zeitwerte wurden für eine Taktfrequenz von 3,5712 MHz berechnet.

Tabelle 16.10 Umrechnungstabelle für CWT
(alle Zeitangaben beziehen sich auf einen Takt von 3,5712 MHz)

CWI	CWT	CWT (für Teiler 93)	CWT (für Teiler 186)	CWT (für Teiler 372)
0	12 etu	0,313 ms	0,625 ms	1,250 ms
1	13 etu	0,339 ms	0,677 ms	1,354 ms
2	15 etu	0,391 ms	0,781 ms	1,563 ms
3	19 etu	0,495 ms	0,990 ms	1,979 ms
4	27 etu	0,703 ms	1,406 ms	2,813 ms
5	43 etu	1,120 ms	2,240 ms	4,479 ms
6	75 etu	1,953 ms	3,906 ms	7,813 ms
7	139 etu	3,620 ms	7,240 ms	14,479 ms

Tabelle 16.10 (Fortsetzung)

CWI	CWT	CWT (für Teiler 93)	CWT (für Teiler 186)	CWT (für Teiler 372)
8	267 etu	6,953 ms	13,906 ms	27,813 ms
9	523 etu	13,620 ms	27,240 ms	54,479 ms
10	1 035 etu	26,953 ms	53,906 ms	107,813 ms
11	2 059 etu	53,620 ms	107,240 ms	214,479 ms
12	4 107 etu	106,953 ms	213,906 ms	427,813 ms
13	8 203 etu	213,620 ms	427,240 ms	854,479 ms
14	16 395 etu	426,953 ms	853,906 ms	1 707,813 ms
15	32 779 etu	853,620 ms	1 707,240 ms	3 414,47 ms

Tabelle 16.11 Umrechnungstabelle für BWT
(alle Angaben beziehen sich auf einen Takt von 3,5712 MHz)

BWI	BWT	BWT (für Teiler 93)	BWT (für Teiler 186)	BWT (für Teiler 372)
0	1011 etu	26,328 msec	52,656 msec	105,313 msec
1	2011 etu	52,370 msec	104,740 msec	209,479 msec
2	4011 etu	104,453 msec	208,906 msec	417,813 msec
3	8011 etu	208,620 msec	417,240 msec	834,479 msec
4	16011 etu	416,953 msec	833,906 msec	1 667,813 msec
5	32011 etu	833,620 msec	1 667,240 msec	3 334,479 msec
6	64011 etu	1 666,953 msec	3 333,906 msec	6 667,813 msec
7	128011 etu	3 333,620 msec	6 667,240 msec	13 334,479 msec
8	256011 etu	6 666,953 msec	13 333,906 msec	26 667,813 msec
9	512011 etu	13 333,620 msec	26 667,240 msec	53 334,479 msec

16.11.3 Tabelle zur Ermittlung der Übertragungsgeschwindigkeit

Tabelle 16.12 Übliche Übertragungsgeschwindigkeiten bei 3,5712 MHz Takt, die sich aus der Verwendung der genormten Werte für den Teiler F und den Übertragungsanpassungsfaktor D ergeben

Takt	F=372, D=1/64 ⇒ 8	F=372, D=1/32 ⇒ 16	F=372, D=1/16 ⇒ 32	F=372, D=1/8 ⇒ 64
1,0000 MHz	125 000 bit/s	62 500 bit/s	31 250 bit/s	15 625 bit/s
2,0000 MHz	250 000 bit/s	125 000 bit/s	62 500 bit/s	31 250 bit/s
3,0000 MHz	375 000 bit/s	187 500 bit/s	93 750 bit/s	46 875 bit/s
3,5712 MHz	446 400 bit/s	223 200 bit/s	111 600 bit/s	55 800 bit/s
4,0000 MHz	500 000 bit/s	250 000 bit/s	125 000 bit/s	62 500 bit/s
4,9152 MHz	614 400 bit/s	307 200 bit/s	153 600 bit/s	76 800 bit/s

Tabelle 16.12 (Fortsetzung)

Takt	F=372, D=1/64 ⇒ 8	F=372, D=1/32 ⇒ 16	F=372, D=1/16 ⇒ 32	F=372, D=1/8 ⇒ 64
5,0000 MHz	625 000 bit/s	312 500 bit/s	156 250 bit/s	78 125 bit/s
6,0000 MHz	750 000 bit/s	375 000 bit/s	187 500 bit/s	93 750 bit/s
7,0000 MHz	875 000 bit/s	437 500 bit/s	218 750 bit/s	109 375 bit/s
8,0000 MHz	1 000 000 bit/s	500 000 bit/s	250 000 bit/s	125 000 bit/s
9,0000 MHz	1 125 000 bit/s	562 500 bit/s	281 250 bit/s	140 625 bit/s
10,0000 MHz	1 250 000 bit/s	625 000 bit/s	312 500 bit/s	156 250 bit/s
Takt	F=372, D=1/4 ⇒ 93	F=372, D=1/2 ⇒ 186	F=372, D=1 ⇒ 372	F=512, D=1 ⇒ 512
1,0000 MHz	10 753 bit/s	5 376 bit/s	2 688 bit/s	1 953 bit/s
2,0000 MHz	21 505 bit/s	10 753 bit/s	5 376 bit/s	3 906 bit/s
3,0000 MHz	32 258 bit/s	16 129 bit/s	8 065 bit/s	5 859 bit/s
3,5712 MHz	38 400 bit/s	19 200 bit/s	9 600 bit/s	6 975 bit/s
4,0000 MHz	43 011 bit/s	21 505 bit/s	10 753 bit/s	7 813 bit/s
4,9152 MHz	52 852 bit/s	26 426 bit/s	13 213 bit/s	9 600 bit/s
5,0000 MHz	53 763 bit/s	26 882 bit/s	13 441 bit/s	9 766 bit/s
6,0000 MHz	64 516 bit/s	32 258 bit/s	16 129 bit/s	11 719 bit/s
7,0000 MHz	75 269 bit/s	37 634 bit/s	18 817 bit/s	13 672 bit/s
8,0000 MHz	86 022 bit/s	43 011 bit/s	21 505 bit/s	15 625 bit/s
9,0000 MHz	96 774 bit/s	48 387 bit/s	24 194 bit/s	17 578 bit/s
10,0000 MHz	107 527 bit/s	53 763 bit/s	26 882 bit/s	19 531 bit/s

16.11.4 Tabelle mit Abtastzeitpunkten

Grundlage für diese Tabelle ist die Datenübertragung nach ISO/IEC 7816-3. Die Zeitwerte wurden für eine Taktfrequenz von 3,5712 MHz berechnet.

Tabelle 16.13 Datenübertragung mit Teiler 372

	Start	untere Toleranz	Mitte	obere Toleranz	Ende
Startbit	0 Takte	112 Takte	186 Takte	260 Takte	372 Takte
	0,000 µs	31,250 µs	52,083 µs	72,917 µs	104,167 µs
Datenbit 1/8	372 Takte	484 Takte	558 Takte	632 Takte	744 Takte
	104,167 µs	135,417 µs	156,250 µs	177,083 µs	208,333 µs
Datenbit 2/7	744 Takte	856 Takte	930 Takte	1 004 Takte	1 116 Takte
	208,333 µs	239,583 µs	260,417 µs	281,250 µs	312,500 µs
Datenbit 3/6	1 116 Takte	1 228 Takte	1 302 Takte	1 376 Takte	1 488 Takte
	312,500 µs	343,750 µs	364,583 µs	385,417 µs	416,667 µs
Datenbit 4/5	1 488 Takte	1 600 Takte	1 674 Takte	1 748 Takte	1 860 Takte

Tabelle 16.13 (Fortsetzung)

	Start	untere Toleranz	Mitte	obere Toleranz	Ende
Datenbit 5/4	416,667 µs	447,917 µs	468,750 µs	489,583 µs	520,833 µs
	1 860 Takte	1 972 Takte	2 046 Takte	2 120 Takte	2 232 Takte
	520,833 µs	552,083 µs	572,917 µs	593,750 µs	625,000 µs
Datenbit 6/3	2 232 Takte	2 344 Takte	2 418 Takte	2 492 Takte	2 604 Takte
	625,000 µs	656,250 µs	677,083 µs	697,917 µs	729,167 µs
	2 604 Takte	2 716 Takte	2 790 Takte	2 864 Takte	2 976 Takte
Datenbit 7/2	729,167 µs	760,417 µs	781,250 µs	802,083 µs	833,333 µs
	2 976 Takte	3 088 Takte	3 162 Takte	3 236 Takte	3 348 Takte
	833,333 µs	864,583 µs	885,417 µs	906,250 µs	937,500 µs
Paritätsbit	3 348 Takte	3 460 Takte	3 534 Takte	3 608 Takte	3 720 Takte
	937,500 µs	968,750 µs	989,583 µs	1 010,417 µs	1 041,667 µs
	3 720 Takte	3 832 Takte	3 906 Takte	3 980 Takte	4 092 Takte
Guardtime/ Stopbit 1	1 041,667 µs	1 072,917 µs	1 093,750 µs	1 114,583 µs	1 145,833 µs
Guardtime/ Stopbit 2	4 092 Takte	4 204 Takte	4 278 Takte	4 352 Takte	4 464 Takte
	1 145,833 µs	1 177,083 µs	1 197,917 µs	1 218,750 µs	1 250,000 µs

16.11.5 Tabelle der wichtigsten Chipkarten-Kommandos

Die folgenden Tabellen enthalten eine Aufstellung der wichtigsten Chipkarten-Kommandos mit einer kurzen Erklärung der Funktion. Dabei wurden die folgenden Normen und Standards berücksichtigt: ISO/IEC 7816-4, -7, -8, -9, EMV, GSM (GSM 11.11, GSM 11.14), UICC (TS 31.111, TS 102.221, TS 102 222, TS 102 223), OP (*open platform*) und EN 1546.

Tabelle 16.14 Überblick über wichtige genormte Chipkarten-Kommandos

Kommando	Funktion	Codierung	Norm der INS
ACTIVATE FILE	Reversibles Entblocken einer Datei.	'44'	ISO/IEC 7816-9
APPEND RECORD	Einfügen eines neuen Records in eine Datei der Struktur „linear fixed“.	'E2'	ISO/IEC 7816-4
APPLICATION BLOCK	Reversibles Blocken einer Anwendung.	'1E'	EMV
APPLICATION UNBLOCK	Entblocken einer Anwendung.	'18'	EMV
ASK RANDOM	Anforderung einer Zufallszahl von der Chipkarte.	'84'	EN 726-3
CHANGE CHV	Ändern der PIN.	'24'	GSM 11.11
CHANGE REFERENCE DATA	Ändern der Daten zur Benutzeridentifizierung (z. B. PIN).	'24'	ISO/IEC 7816-8
CLOSE APPLICATION	Rücksetzen aller erreichten Zugriffsbedingungen.	'AC'	EN 726-3
CONVERT IEP CURRENCY	Währungsumrechnung.	'56'	EN 1546-3

Tabelle 16.14 (Fortsetzung)

Kommando	Funktion	Codierung der INS	Norm
CREATE FILE	Erzeugen einer neuen Datei.	'E0'	ISO/IEC 7816-9
CREATE RECORD	Erzeugen eines neuen Records in einer Record-orientierten Datei.	'E2'	EN 726-3
CREDIT IEP	Aufladen der Börse (IEP).	'52'	EN 1546-3
CREDIT PSAM	Bezahlen der IEP gegenüber dem PSAM.	'72'	EN 1546-3
DEACTIVATE FILE	Reversibles Blocken einer Datei.	'04'	ISO/IEC 7816-9
DEACTIVATE FILE	Entblocken einer Datei.	'44'	ISO/IEC 7816-9
DEBIT IEP	Bezahlen mit der Börse.	'54'	EN 1546-3
DECREASE	Erniedrigen eines Zählers in einer Datei.	'30'	EN 726-3
DECREASE STAMPED	Erniedrigen eines Zählers in einer Datei, die mit einer kryptografischen Prüfsumme abgesichert ist.	'34'	EN 726-3
DELETE	Löschen eines eindeutig identifizierbaren Objekts (z. B. Ladedatei, Anwendung, Schlüssel).	'E4'	OP
DELETE FILE	Löschen einer Datei.	'E4'	ISO/IEC 7816-9
DISABLE CHV	Abschalten der PIN-Abfrage.	'26'	GSM 11.11 EN 726-3
DISABLE VERIFICATION REQUIREMENT	Abschalten der Benutzeridentifikation (z. B. PIN-Abfrage).	'26'	ISO/IEC 7816-8
ENABLE CHV	Einschalten der PIN-Abfrage.	'28'	GSM 11.11 EN 726-3
ENABLE VERIFICATION REQUIREMENT	Einschalten der Benutzeridentifikation (z. B. PIN-Abfrage).	'28'	ISO/IEC 7816-8
ENVELOPE	Einbetten eines weiteren Kommandos in ein Chipkarten-Kommando.	'C2'	ISO/IEC 7816-4
ERASE BINARY	Setzen des Inhalts einer Datei der Struktur „transparent“ auf den gelöschten Zustand.	'0E'	ISO/IEC 7816-4
EXECUTE	Ausführen einer Datei.	'AE'	EN 726-3
EXTEND	Erweitern einer Datei.	'D4'	EN 726-3
EXTERNAL AUTHENTICATE	Authentisierung der äußeren Welt durch die Chipkarte.	'82'	ISO/IEC 7816-4
GENERATE AUTHORIZATION CRYPTOGRAM	Erzeugung einer Signatur für eine Zahlungstransaktion.	'AE'	EMV-2
GENERATE PUBLIC KEY PAIR	Erzeugung eines Schlüsselpaares für einen asymmetrischen Kryptoalgorithmus.	'46'	ISO/IEC 7816-8
GET CHALLENGE	Anforderung einer Zufallszahl von der Chipkarte.	'84'	ISO/IEC 7816-4

Tabelle 16.14 (Fortsetzung)

Kommando	Funktion	Codierung der INS	Norm
GET DATA	Lesen von TLV-codierten Datenobjekten.	'CA'	ISO/IEC 7816-4
GET PREVIOUS IEP SIGNATURE	Wiederhole Berechnung und Ausgabe der letzten erhaltenen Signatur von der IEP.	'5A'	EN 1546-3
GET PREVIOUS PSAM SIGNATURE	Wiederhole Berechnung und Ausgabe der letzten erhaltenen Signatur vom PSAM.	'86'	EN 1546-3
GET RESPONSE	T=0 Kommando zur Anforderung von Daten von der Chipkarte.	'C0'	GSM 11.11 ISO/IEC 7816-4
GET STATUS	Lesen von Zustandsinformation des Lebenszyklus von Card Manager, Anwendung und Ladedatei.	'F2'	OP
GIVE RANDOM	Senden einer Zufallszahl zur Chipkarte.	'86'	EN 726-3
INCREASE	Erhöhen eines Zählers in einer Datei.	'32'	GSM 11.11 EN 726-3
INCREASE STAMPED	Erhöhen eines Zählers in einer Datei, die mit einer kryptografischen Prüfsumme abgesichert ist.	'36'	EN 726-3
INITIALIZE IEP	Initialisierung einer IEP für ein nachfolgendes Börsenkommando.	'50'	EN 1546-3
INITIALIZE PSAM	Initialisierung eines PSAM für ein nachfolgendes Börsenkommando.	'70'	EN 1546-3
INITIALIZE PSAM for offline Collection	Initialisierung eines PSAM zur Offline-Abrechnung der Beträge.	'7C'	EN 1546-3
INITIALIZE PSAM for online Collection	Initialisierung eines PSAM zur Online-Abrechnung der Beträge.	'76'	EN 1546-3
INITIALIZE PSAM for Update	Initialisierung eines PSAM zur Änderung der Parameter.	'80'	EN 1546-3
INSTALL	Installation einer Anwendung durch Aufrufen verschiedener Oncard-Funktionen des Card Managers und/oder der Security Domain.	'E6'	OP
INTERNAL AUTHENTICATE	Authentisierung der Chipkarte durch die äußere Welt.	'88'	ISO/IEC 7816-4
INVALIDATE	Reversibles Blocken einer Datei.	'04'	GSM 11.11 EN 726-3
ISSUER AUTHENTICATE	Überprüfung einer Signatur des Kartenherausgebers.	'82'	EMV-2
Kommando	Funktion	Codierung der INS	Norm
LOAD	Laden einer Anwendung durch Übertragung der Ladedatei.	'E8'	OP

Tabelle 16.14 (Fortsetzung)

Kommando	Funktion	Codierung der INS	Norm
LOAD KEY FILE	Kryptografisch gesichertes Laden von Schlüsseln in Dateien.	'D8'	EN 726-3
LOCK	Irreversibles Sperren einer Datei.	'76'	EN 726-3
MANAGE CHANNEL	Steuerung der logischen Kanäle einer Chipkarte.	'70'	ISO/IEC 7816-4
MANAGE SECURITY ENVIRONMENT	Ändern der Parameter für die Benutzung kryptografischer Algorithmen in der Chipkarte.	'22'	ISO/IEC 7816-8
MUTUAL AUTHENTICATE	Gegenseitige Authentisierung von Chipkarte und Terminal.	'82'	ISO/IEC 7816-8
PERFORM SCQL OPERATION	Ausführen einer SCQL Anweisung.	'10'	ISO/IEC 7816-7
PERFORM SECURITY OPERATION	Ausführen eines kryptografischen Algorithmus in der Chipkarte.	'2A'	ISO/IEC 7816-8
PERFORM TRANSACTION OPERATION	Ausführen einer Transaktionsanweisung für SCQL.	'12'	ISO/IEC 7816-7
PERFORM USER OPERATION	Verwalten von Benutzern im Rahmen von SCQL.	'14'	ISO/IEC 7816-7
PSAM COLLECT	Ausführung der PSAM Online-Abrechnung der Beträge.	'78'	EN 1546-3
PSAM COLLECT Acknowledgement	Beendigung der PSAM Online-Abrechnung der Beträge.	'7A'	EN 1546-3
PSAM COMPLETE	Beendigung der Zahlung einer IEP gegenüber dem PSAM.	'74'	EN 1546-3
PSAM VERIFY COLLECTION	Beendigung der PSAM Offline-Abrechnung der Beträge.	'7E'	EN 1546-3
PUT DATA	Schreiben von TLV-codierten Datenobjekten.	'DA'	ISO/IEC 7816-4
PUT KEY	Schreiben eines oder mehrerer neuer Schlüssel oder Ersetzen bereits vorhandener Schlüssel.	'D8'	OP
READ BINARY	Lesen aus einer Datei mit transparenter Struktur.	'B0'	GSM 11.11 ISO/IEC 7816-4
READ BINARY STAMPED	Lesen aus einer Datei mit transparenter Struktur, die mit einer kryptografischen Prüfsumme abgesichert ist.	'B4'	EN 726-3
READ RECORD/READ RECORD(S)	Lesen aus einer Datei mit Record-orientierter Struktur.	'B2'	GSM 11.11 ISO/IEC 7816-4
READ RECORD STAMPED	Lesen aus einer Datei mit Record-orientierter Struktur, die mit einer kryptografischen Prüfsumme abgesichert ist.	'B6'	EN 726-3
REHABILITATE	Entblocken einer Datei.	'44'	GSM 11.11 EN 726-3
RESET RETRY COUNTER	Rücksetzen eines Fehlbedienungs-zählers.	'2C'	ISO/IEC 7816-8

Tabelle 16.14 (Fortsetzung)

Kommando	Funktion	Codierung der INS	Norm
RUN GSM ALGORITHM	Ausführen des GSM-spezifischen Kryptalgorithmus.	'88'	GSM 11.11
SEARCH BINARY	Suchen eines Textes in einer Datei mit transparenter Struktur.	'A0'	ISO/IEC 7816-9
SEARCH RECORD	Suchen eines Textes in einer Datei mit Record-orientierter Struktur.	'A2'	ISO/IEC 7816-9
SEEK	Suchen eines Textes in einer Datei mit Record-orientierter Struktur.	'A2'	GSM 11.11 EN 726-3
SELECT/SELECT (FILE)	Auswahl einer Datei.	'A4'	GSM 11.11 ISO/IEC 7816-4
SET STATUS	Schreiben von Zustandsinformation des Lebenszyklus von Card Manager, Anwendung und Ladedatei.	'F0'	OP
SLEEP	Obsoletes Kommando, um die Chipkarte in einen energiesparenden Zustand zu versetzen.	'FA'	GSM 11.11
STATUS	Lesen von verschiedenen Informationen zur aktuell selektierten Datei.	'F2'	GSM 11.11 EN 726-3
TERMINATE CARD USAGE	Irreversibles Sperren einer Chipkarte.	'FE'	ISO/IEC 7816-9
TERMINATE DF	Irreversibles Sperren eines DFs.	'E6'	ISO/IEC 7816-9
TERMINATE EF	Irreversibles Sperren eines EFs.	'E8'	ISO/IEC 7816-9
UNBLOCK CHV	Zurücksetzen des abgelaufenen PIN-Fehlbedienungs Zählers.	'2C'	GSM 11.11 EN 726-3
UPDATE BINARY	Schreiben in eine Datei mit transparenter Struktur.	'D6'	GSM 11.11 EN 726-3 ISO/IEC 7816-4
UPDATE IEP PARAMETER	Ändern der Rahmenparameter der Börse.	'58'	EN 1546-3
UPDATE PSAM Parameter (offline)	Ausführung der Offline-Änderung von Parametern im PSAM.	'84'	EN 1546-3
UPDATE PSAM Parameter (online)	Ausführung der Online-Änderung von Parametern im PSAM.	'82'	EN 1546-3
UPDATE RECORD	Schreiben in eine Datei mit Record-orientierter Struktur.	'DC'	GSM 11.11 ISO/IEC 7816-4
VERIFY	Überprüfung von übergebenen Daten (z. B. PIN).	'20'	ISO/IEC 7816-4 EMV-2
VERIFY CHV	Überprüfen der PIN.	'20'	GSM 11.11 EN 726-3
WRITE BINARY	Schreiben durch logische AND/OR-Verknüpfung in eine Datei mit transparenter Struktur.	'D0'	ISO/IEC 7816-4
WRITE RECORD	Schreiben durch logische AND/OR-Verknüpfung in eine Datei mit Record-orientierter Struktur.	'D2'	ISO/IEC 7816-4

16.11.6 Übersicht über die verwendeten Instruction-Bytes

Der grau hinterlegte Bereich der ungeraden Zahlen darf nicht für die Codierung von Kommandos verwendet werden, da das Übertragungsprotokoll T=0 diesen Bereich zur Steuerung der Programmierspannung benutzt.⁷⁵

Tabelle 16.15 Überblick über die verwendeten Codierungen des Instruction-Bytes (INS) bei einem Class-Byte (CLA) von '00'. Dieses Class-Byte wird von den Normen ISO/IEC 7816-4, -7, -8, -9 festgelegt. Die Tabelle enthält jeweils die Nummer des entsprechenden Normenteils.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0y					9										4	
1y	7		7		7											
2y	4		8		8		8		8		8		8			
3y																
4y	9				9		8									
5y																
6y																
7y	4															
8y			4, 8		4			4								
9y																
Ay	9		9		4											
By	4		4													
Cy	4		4								4					
Dy	4		4			4					4		4			
Ey	9		4		9	9		9								
Fy															9	

Tabelle 16.16 Überblick über die verwendeten Codierungen des Instruction-Bytes (INS) bei einem Class-Byte (CLA) von '80'. Dieses Class-Byte wird von den Normen EMV, EN 1546 und OP festgelegt. Die Tabelle enthält jeweils eine Referenz in Form der Anfangsbuchstaben auf die entsprechende Norm.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0y																
1y							OP		OP						OP	
2y					OP											
3y																
4y																
5y	EN		EN		EN		EN				EN					
6y																
7y	EN		EN		EN		EN		EN		EN		EN		EN	
8y	EN		EN, EMV		EN		EN									
9y																
Ay								OP							EMV, OP	
By																
Cy											OP					
Dy								OP								
Ey																
Fy	OP		OP		OP		OP									

⁷⁵ Siehe auch Abschnitt 6.4.2 „Übertragungsprotokoll T=0“. Ein Verbesserungsvorschlag für die Überarbeitung der ISO/IEC 7816-3 beinhaltet, dass die Steuerung einer externen Programmierspannung über das Instruction-Byte in Zukunft nicht mehr vorgesehen ist.

Tabelle 16.17 Überblick über die verwendeten Codierungen des Instruction-Bytes (INS) bei einem Class-Byte (CLA) von 'A0'. Dieses Class-Byte wird von der Norm GSM 11.11 festgelegt.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0y					X											
1y	X			X	X											
2y	X				X		X		X				X			
3y				X												
4y					X											
5y																
6y																
7y																
8y									X							
9y																
Ay					X											
By	X			X												
Cy	X			X												
Dy							X		X							
Ey																
Fy				X							X					

16.11.7 Codierung von Chipkarten-Kommandos

Die folgenden Tabellen geben die wichtigsten Codierungen für einige beispielhafte Kommandos für Chipkarten an. Der Übersicht halber wurde davon ausgegangen, dass kein Secure Messaging und keine Adressierung über logische Kanäle verwendet wird. Für die vollständige Codierung dieser und weiterer Kommandos sei auf die Norm ISO/IEC 7816-4 verwiesen.⁷⁶

Tabelle 16.18 Codierung des Case-4-Kommandos SELECT FILE mit den wichtigsten Optionen

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816 Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'A4'	Das Instruction-Byte für SELECT FILE, d. h. das Kommando zur Auswahl von Dateien (MF, DFs oder EFs).
P1	...	P1 = '00' $\wedge$ Lc = 0 Selektion des MF P1 = '00' $\wedge$ Lc $\neq$ 0 Selektion einer Datei mit FID (FID in DATA enthalten) P1 = '04' Selektion eines DF mit dem DF Name (DF Name in DATA enthalten) P1 = '08' Selektion einer Datei durch die Angabe des FID-basierten Pfades (Pfad in DATA enthalten) vom MF aus. P1 = '09' Selektion einer Datei durch die Angabe des FID-basierten Pfades (Pfad in DATA enthalten) vom aktuellen DF aus.
P2	...	P2 = '00' Rückgabe von optionalen FCI P2 = '04' Rückgabe von optionalen FCP P2 = '08' Rückgabe von optionalen FMD
Lc	...	Codierung in der Beschreibung von P1 enthalten.
DATA	...	Codierung in der Beschreibung von P1 enthalten.
Lc	Le = 0	Rückgabe aller zur Selektion gehörenden Daten.

⁷⁶ Siehe auch Abschnitt 6.5.1 „Struktur der Kommando-APDUs“.

Tabelle 16.19 Codierung des Case-2-Kommandos READ BINARY nach ISO/IEC 7816-4 mit den wichtigsten Optionen

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816 Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'B0'	Das Instruction-Byte für READ BINARY, d. h. das Kommando zum Lesen von Daten aus Dateien der Struktur „transparent“.
P1	...	P1.b8 = 0 Lese Daten aus der aktuell selektierten Datei mit Offset; Offset = (P1.b7 ... P1.b1 P2) P1.b8 = 1 Lese Daten nach impliziter Dateiselektion durch Short-FID und mit Offset; Short-FID = (P1.b5 ... P1.b1), Offset = P2
P2	...	Codierung in der Beschreibung von P1 enthalten.
Le	...	Le = 0 Lese alle Daten bis zum Ende der Datei. Le > 0 Le ist die Anzahl der zu lesenden Bytes.

Tabelle 16.20 Codierung des Case-3-Kommandos UPDATE BINARY nach ISO/IEC 7816-4 mit den wichtigsten Optionen

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816 Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'D6'	Das Instruction-Byte für UPDATE BINARY, d. h. das Kommando zum Schreiben von Daten in Dateien der Struktur „transparent“.
P1	...	P1.b8 = 0 Schreibe Daten in die aktuell selektierte Datei mit Offset; Offset = (P1.b7 ... P1.b1 P2) P1.b8 = 1 Schreibe Daten nach impliziter Dateiselektion durch Short-FID und mit Offset; Short-FID = (P1.b5 ... P1.b1), Offset = P2
P2	...	Codierung in der Beschreibung von P1 enthalten.
Lc	...	Lc ist die Anzahl der zu schreibenden Bytes.
DATA	...	Die zu schreibenden Bytes mit der Länge Lc.

Tabelle 16.21 Codierung des Case-2-Kommandos READ RECORD nach ISO/IEC 7816-4 mit den wichtigsten Option

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816 Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'B2'	Das Instruction-Byte für READ RECORD, d. h. das Kommando zum Lesen von Daten aus Dateien mit Record-orientierter Struktur.
P1	...	P1 = 0 Lese den aktuellen Record P1 ≠ 0 Lese den Record mit der in P1 angegebenen Recordnummer oder Record Identifier.
P2	...	P2.b8 ... P2.b4 = °00000° Lese Daten aus der aktuell selektierten Datei P2.b8 ... P2.b4 ≠ °00000° Lese Daten nach impliziter Dateiselektion durch Short-FID Short-FID = (P2.b8 ... P2.b4) P2.b3 ... P2.b1 = °000° Lese den ersten (<i>first</i>) Record mit dem Record Identifier, übergeben in P1

Tabelle 16.21 (Fortsetzung)

Datenelement	Codierung	Bemerkung
		$P2.b3 \dots P2.b1 = {}^{\circ}001^{\circ}$ Lese den letzten (<i>last</i>) Record mit dem Record Identifier, übergeben in P1 $P2.b3 \dots P2.b1 = {}^{\circ}010^{\circ}$ Lese den nächsten (<i>next</i>) Record mit dem Record Identifier, übergeben in P1 $P2.b3 \dots P2.b1 = {}^{\circ}011^{\circ}$ Lese den vorherigen (<i>previous</i>) Record mit dem Record Identifier, übergeben in P1 $P2.b3 \dots P2.b1 = {}^{\circ}100^{\circ} \wedge P1 = 0$ Lese den aktuellen Record $P2.b3 \dots P2.b1 = {}^{\circ}100^{\circ} \wedge P1 \neq 0$ Lese den Record mit der Recordnummer, übergeben in P1. $P2.b3 \dots P2.b1 = {}^{\circ}101^{\circ}$ Lese alle Records ab der in P1 übergebenen Recordnummer bis zum Ende der Datei. $P2.b3 \dots P2.b1 = {}^{\circ}110^{\circ}$ Lese alle Records vom Ende der Datei bis zu der in P1 übergebenen Recordnummer.
Le	...	$Le = 0$ Lese alle Bytes bis zum Ende des Records/der Records. $Le > 0$ Le ist die Länge des Records/der Records.

Tabelle 16.22 Codierung des Case-3-Kommandos UPDATE RECORD nach ISO/IEC 7816-4 mit den wichtigsten Optionen

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816-Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'DC'	Das Instruction-Byte für UPDATE RECORD, d. h. das Kommando zum Schreiben von Daten in Dateien mit Record-orientierter Struktur
P1	...	$P1 = 0$ Schreibe den aktuellen Record $P1 \neq 0$ Schreibe den Record mit der in P1 übergebenen Recordnummer.
P2	...	$P2.b8 \dots P2.b4 = {}^{\circ}00000^{\circ}$ Schreibe Daten in die aktuell selektierte Datei $P2.b8 \dots P2.b4 \neq {}^{\circ}00000^{\circ}$ Schreibe Daten nach impliziter Dateiselektion durch Short-FID Short-FID = (P1.b8 ... P1.b4) $P2.b3 \dots P2.b1 = {}^{\circ}000^{\circ}$ Schreibe den ersten (first) Record $P2.b3 \dots P2.b1 = {}^{\circ}001^{\circ}$ Schreibe den letzten (last) Record $P2.b3 \dots P2.b1 = {}^{\circ}010^{\circ}$ Schreibe den nächsten (next) Record $P2.b3 \dots P2.b1 = {}^{\circ}011^{\circ}$ Schreibe den vorherigen (previous) Record $P2.b3 \dots P2.b1 = {}^{\circ}100^{\circ}$ Schreibe den Record mit der in P1 übergebenen Recordnummer
Lc	...	Lc ist die Länge des zu schreibenden Records.
DATA	...	Der zu schreibende Record.

Tabelle 16.23 Codierung des Case-3-Kommandos VERIFY nach ISO/IEC 7816-4 mit den wichtigsten Optionen

Daten- element	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816-Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'20'	Das Instruction-Byte für VERIFY, d. h. das Kommando zum Vergleich von übergebenen Daten mit Referenzdaten (typischerweise einer PIN).
P1	'00'	---
P2	...	P2 = '00' Explizite Informationen werden nicht übergeben. P2.b8 = °0° Es werden für die ganze Chipkarte gültige Referenz- daten verwendet (global reference data). P2.b8 = °1° Es werden für eine oder mehrere Anwendungen gülti- ge Referenzdaten verwendet (specific reference data). P2.b7 P2.b6 = °00° RFU Bits P2.b5 ... P2.b1 Nummer der Referenzdaten.
Lc	...	Lc ist die Länge des übergebenen Vergleichswertes.
DATA	...	Der übergebene Vergleichswert (in der Regel eine PIN).

16.11.8 Chipkarten-Returncodes

Die im Folgenden beschriebenen Returncodes sind in das Schema für Returncodes nach ISO/IEC 7816-4 eingeteilt.⁷⁷ Dabei wurde folgende Kennzeichnung verwendet:

NP	Prozess ausgeführt, normale Bearbeitung	(process completed, normal pro- cessing)
WP	Prozess ausgeführt, Warnung	(process completed, warning pro- cessing)
EE	Prozess abgebrochen, Ausführungsfehler	(process aborted, execution error)
CE	Prozess abgebrochen, Prüfungsfehler	(process aborted, checking error)

Tabelle 16.24 Ausgewählte und genormte Chipkarten-Returncodes nach ISO/IEC 7816-4

Returncode	Status	Bedeutung	Norm
'61xx'	NP	Kommando erfolgreich ausgeführt, xx Byte Daten sind als Antwort vorhanden und können mit GET RESPONSE angefordert werden.	ISO/IEC 7816-4
'6281'	WP	Die zurückgegebenen Daten können u.U. fehlerhaft sein	ISO/IEC 7816-4
'6282'	WP	Es konnten weniger als Le Bytes gelesen werden, da das Dateiende vorher erreicht wurde.	ISO/IEC 7816-4
'6283'	WP	Die selektierte Datei ist reversibel gesperrt (invalidated).	ISO/IEC 7816-4
'6284'	WP	Die File Control Information (FCI) ist nicht nach ISO/IEC 7816-4 strukturiert.	ISO/IEC 7816-4

⁷⁷ Siehe auch Abschnitt 6.5.2 „Struktur der Antwort-APDUs“.

Tabelle 16.24 (Fortsetzung)

Returncode	Status	Bedeutung	Norm
'62xx'	WP	Warnung; Zustand des nichtflüchtigen Speichers unverändert	ISO/IEC 7816-4
'63Cx'	WP	Zähler hat den Wert x erreicht ($0 \leq x \leq 15$) (die genaue Bedeutung ist vom jeweiligen Kommando abhängig)	ISO/IEC 7816-4
'63xx'	WP	Warnung; Zustand des nichtflüchtigen Speichers verändert	ISO/IEC 7816-4
'64xx'	EE	Ausführungsfehler; Zustand des nichtflüchtigen Speichers unverändert	ISO/IEC 7816-4
'6581'	EE	Speicherfehler (z. B. bei Schreiboperation)	ISO/IEC 7816-4
'65xx'	EE	Ausführungsfehler; Zustand des nichtflüchtigen Speichers verändert	ISO/IEC 7816-4
'6700'	CE	Länge falsch	GSM 11.11 ISO/IEC 7816-4
'67xx' ... '6Fxx'	CE	Prüfungsfehler	ISO/IEC 7816-4
'6800'	CE	Funktionen im Class Byte werden nicht unterstützt (allgemein)	ISO/IEC 7816-4
'6881'	CE	Logische Kanäle werden nicht unterstützt	ISO/IEC 7816-4
'6882'	CE	Secure Messaging wird nicht unterstützt	ISO/IEC 7816-4
'6900'	CE	Kommando nicht erlaubt (allgemein)	ISO/IEC 7816-4
'6981'	CE	Kommando inkompatibel zur Dateistruktur	ISO/IEC 7816-4
'6982'	CE	Sicherheitszustand nicht erfüllt	ISO/IEC 7816-4
'6983'	CE	Authentisierungsmethode gesperrt	ISO/IEC 7816-4
'6984'	CE	referenzierte Daten sind reversibel gesperrt (<i>invalidated</i>)	ISO/IEC 7816-4
'6985'	CE	Benutzungsbedingungen nicht erfüllt	ISO/IEC 7816-4
'6986'	CE	Kommando nicht erlaubt (kein EF selektiert)	ISO/IEC 7816-4
'6987'	CE	erwartete Secure Messaging-Datenobjekte fehlen	ISO/IEC 7816-4
'6988'	CE	Secure Messaging Datenobjekte inkorrekt	ISO/IEC 7816-4
'6A00'	CE	Falsche Parameter P1/P2 (allgemein)	ISO/IEC 7816-4
'6A80'	CE	Parameter im Datenteil sind falsch	ISO/IEC 7816-4
'6A81'	CE	Funktion wird nicht unterstützt	ISO/IEC 7816-4
'6A82'	CE	Datei wurde nicht gefunden	ISO/IEC 7816-4
'6A83'	CE	Record wurde nicht gefunden	ISO/IEC 7816-4
'6A84'	CE	Ungenügend Speicherplatz in der Datei	ISO/IEC 7816-4
'6A85'	CE	Lc inkonsistent mit TLV Struktur	ISO/IEC 7816-4
'6A86'	CE	Inkorrekte Parameter P1/P2	ISO/IEC 7816-4

Tabelle 16.24 (Fortsetzung)

Returncode	Status	Bedeutung	Norm
'6A87'	CE	Lc inkonsistent mit P1/P2	ISO/IEC 7816-4
'6A88'	CE	referenzierte Daten nicht gefunden	ISO/IEC 7816-4
'6B00'	CE	Parameter 1 oder 2 falsch	ISO/IEC 7816-4 GSM 11.11
'6Cxx'	CE	falsche Länge Le; xx gibt die korrekte Länge an	ISO/IEC 7816-4
'6D00'	CE	Kommando (Instruction) wird nicht unterstützt	ISO/IEC 7816-4 GSM 11.11
'6E00'	CE	Class wird nicht unterstützt	ISO/IEC 7816-4 GSM 11.11
'6F00'	CE	Kommando abgebrochen – genauere Diagnose nicht möglich (z. B. Fehler im Betriebssystem)	ISO/IEC 7816-4 GSM 11.11
'9000'	NP	Kommando erfolgreich ausgeführt	ISO/IEC 7816-4 GSM 11.11
'920x'	NP	Schreiben ins EEPROM nach x-maligem Versuch erfolgreich	GSM 11.11
'9210'	CE	Ungenügend Speicherplatz	GSM 11.11
'9240'	EE	Schreiben ins EEPROM nicht erfolgreich	GSM 11.11
'9400'	CE	kein EF selektiert	GSM 11.11
'9402'	CE	Adressbereich überschritten	GSM 11.11
'9404'	CE	FID nicht gefunden, Record nicht gefunden, Vergleichsmuster nicht gefunden	GSM 11.11
'9408'	CE	Selektierter Dateityp unpassend zum Kommando	GSM 11.11
'9802'	CE	Keine PIN definiert	GSM 11.11
'9804'	CE	Zugriffsbedingungen nicht erfüllt, Authentisierung fehlgeschlagen	GSM 11.11
'9835'	CE	ASK RANDOM/GIVE RANDOM nicht ausgeführt	GSM 11.11
'9840'	CE	PIN-Prüfung nicht erfolgreich	GSM 11.11
'9850'	CE	INCREASE/DECREASE kann nicht ausgeführt werden, da Grenzwert erreicht	GSM 11.11
'9Fxx'	NP	Kommando erfolgreich ausgeführt, xx Byte Daten sind als Antwort vorhanden und können mit GET RESPONSE angefordert werden.	GSM 11.11

16.11.9 Ausgewählte Chips für Speicherkarten

Die folgenden Tabellen zeigen eine Auswahl von typischen Speicherchips für Chipkarten ohne Anspruch auf Vollständigkeit und Korrektheit. Der Zweck dieser Tabelle besteht vor allem darin, einen Überblick über die sehr große Bandbreite von Speicherchips zu vermitteln. Es sei an dieser Stelle explizit erwähnt, dass Tabellen dieser Art aufgrund der stetigen technischen Weiterentwicklung verhältnismäßig schnell veralten. Aktuelle technische Überblicksdaten erhält man vorzugsweise direkt über den Web-Server des jeweiligen Herstellers, wie z. B. bei Infineon [Infineon], Philips [Philips], und ST Microelectronics [STM]. Ähnliche Bausteine werden auch von diversen anderen Herstellern angeboten.

Tabelle 16.25 Überblick über ausgewählte Chips für Speicherkarten

Hersteller und Typ	Speicher		Detailinformationen	
Infineon SLE 4404	ROM:	16 Bit	Vcc:	5 V
	PROM:	144 Bit	Strom:	3 mA
	EEPROM:	256 Bit	W/E-Zykl.:	100 000
			Dauer W/E:	5 ms
			HW:	---
Infineon SLE 4406S	ROM:	24 Bit	Vcc:	5 V
	PROM:	72 Bit	Strom:	1 mA
	EEPROM:	32 Bit	W/E-Zykl.:	100 000
			Dauer W/E:	3 ms
			HW:	Zähler für $\approx 20\,000$ Einheiten
Infineon SLE 44R35	ROM:	---	Vcc:	5 V
	PROM:	---	Strom:	3 mA
	EEPROM:	1 kByte	W/E-Zykl.:	100 000
			Dauer W/E:	2 ms
			HW:	PIN-Logik für zusätzlichen Schreibschutz einseitige Authentisierung für kontaktlose Speicherkarten
Infineon SLE 5536	ROM:	24 Bit	Vcc:	5 V
	PROM:	177 Bit	Strom:	2,5 mA
	EEPROM:	36 Bit	W/E-Zykl.:	100 000
			Dauer W/E:	3 ms
			HW:	Zähler für $\approx 20\,000$ Einheiten einseitige Authentisierung
Infineon SLE 4442	ROM:	---	Vcc:	5 V
	PROM:	32 Bit	Strom:	10 mA
	EEPROM:	256 Byte	W/E-Zykl.:	100 000
			Dauer W/E:	2,5 ms
			HW:	---
Infineon SLE 7736	ROM:	24 Bit	Vcc:	3 – 5 V
	PROM:	177 Bit	Strom:	1 mA
	EEPROM:	36 Byte	W/E-Zykl.:	100 000
			Dauer W/E:	3 ms
			HW:	Zähler für $\approx 20\,000$ Einheiten
Philips MF1 S70	ROM:	---	Vcc:	⊗
	PROM:	---	Strom:	⊗
	EEPROM:	4 kByte	W/E-Zykl.:	100 000
			Dauer W/E:	⊗
			HW:	4 Byte Seriennummer, einseitige Authentisierung, kontaktlose Schnittstelle nach ISO/IEC 14 443A
Philips I-Code SLI ICPCB 7960	ROM:	---	Vcc:	⊗
	PROM:	---	Strom:	⊗
	EEPROM:	896 Bit	W/E-Zykl.:	⊗
			Dauer W/E:	⊗
			HW:	8 Byte Seriennummer, kontaktlose Schnittstelle nach ISO/IEC 15 693
ST Micro-electronics LR1512	ROM:	---	W/E-Zykl.:	100 000
	PROM:	---	Dauer W/E:	5 ms
	EEPROM:	512 Bit	HW:	ISO/IEC 15 693
ST Micro-electronics M35101	ROM:	---	W/E-Zykl.:	100 000
	PROM:	---	Dauer W/E:	5 ms
	EEPROM:	2048 Bit	HW:	ISO/IEC 14 443 B
ST Micro-electronics ST1335D	ROM:	16 Bit	Vcc:	5 V
	PROM:	---	Strom:	500 μ A
	EEPROM:	272 Bit	W/E-Zykl.:	500 000
			Dauer W/E:	3,5 ms
			HW:	Zähler bis 32 767, einseitige Authentisierung

16.11.10 Ausgewählte Mikrocontroller für Chipkarten

Die folgenden Tabellen zeigen eine Auswahl von typischen Mikrocontrollern für Chipkarten ohne Anspruch auf Vollständigkeit und Korrektheit. Der Zweck diese Tabelle besteht vor allem darin, einen Überblick über die sehr große Bandbreite von Chipkarten-Mikrocontrollern zu vermitteln. Es sei an dieser Stelle explizit erwähnt, dass Tabellen dieser Art aufgrund der stetigen technischen Weiterentwicklung verhältnismäßig schnell veralten. Aktuelle technische Überblicksdaten erhält man vorzugsweise direkt über den Web-Server des jeweiligen Herstellers, wie z. B. bei Atmel [Atmel], Hitachi [Hitachi], Infineon [Infineon], Philips [Philips], und ST Microelectronics [STM]. Ähnliche Bausteine werden auch von diversen anderen Herstellern angeboten.

Folgende Abkürzungen finden in den Tabellen Verwendung:

Vcc:	Spannungsbereich
Takt:	Taktbereich
Strom:	Stromaufnahme des Chips bei der angegebenen Taktfrequenz (erster Wert im Betrieb, zweiter Wert im Energiesparzustand mit Takt, dritter Wert im Energiesparzustand ohne Takt)
Größe (optional):	Größe des Die
min. Breite:	minimale Strukturbreite auf dem Chip
EEPROM Pg.:	Größe einer Speicherseite im EEPROM
W/E-Zykl.:	Anzahl der garantierten Schreib-/Löschzyklen pro EEPROM-Speicherseite
Dauer W/E:	Dauer des Löschens bzw. Schreibens einer EEPROM-Speicherseite
HW:	zusätzliche Hardware auf dem Chip
UART:	Hardware-unterstützte Datenübertragung (<i>universal asynchronous receiver transmitter</i>)
Timer:	Zähler zum Messen von Takten
CRC:	Recheneinheit für CRC
PLL: i	interne Taktvervielfachung (<i>phase locked loop</i>)
MMU:	Speicherverwaltungshardware (<i>memory management unit</i>)
RNG:	Zufallszahlengenerator
DES:	DES-Beschleuniger i.d.R. incl. Triple-DES-Beschleuniger
AES:	AES-Beschleuniger
RSA:	RSA-Beschleuniger i.d.R. inklusive EC-Beschleuniger
⊗	keine Informationen zu diesem Punkt öffentlich verfügbar

Tabelle 16.26 Überblick über ausgewählte Mikrocontroller für Chipkarten

Hersteller und Typ Speicher			Detailinformationen	
Atmel AT90 SC6464C	Flash:	64 kByte	CPU:	AVR
	EEPROM:	64 kByte	Vcc:	2,7 - 3,3 V, 4,5 - 5,5 V
	RAM:	3 kByte	Takt:	1 MHz – 10 MHz
			Strom:	⊗, ⊗
			Größe:	24 mm ²
			min. Breite:	0,35 µm
			EEPROM Pg.:	1 – 128 Byte
			EEPROM W/E-Zykl.:	500 000
			EEPROM Dauer W/E:	5 ms
			Flash Pg.:	128 Byte
			Flash W/E-Zykl.:	500 000
			Flash Dauer W/E:	5 ms
			HW:	RISC CPU, 2 Timer à 16 Bit, MMU, RNG,
				DES, RSA

Tabelle 16.26 (Fortsetzung)

Hersteller und Typ Speicher			Detailinformationen	
Atmel AT90 SC19264RC.	Flash:	192 kByte	CPU:	AVR
	EEPROM:	64 kByte	Vcc:	2,7 – 3,3V, 4,5 V - 5,5 V
	RAM:	6 kByte	Takt:	1 MHz – 16 MHz
			Strom:	③, ④
			Größe:	24 mm ²
			min. Breite:	0,35 µm
			EEPROM Pg.:	1 – 128 Byte
			EEPROM W/E-Zykl.:	500 000
			EEPROM Dauer W/E:	5 ms
			HW:	RISC CPU, UART, 2 Timer à 16 Bit, CRC, PLL, MMU, RNG, DES, RSA
Hitachi H8/3166	ROM:	32 kByte	CPU:	H8
	EEPROM:	2,2 kByte	Vcc:	2,7 – 5,5 V
	RAM:	1 kByte	Takt:	1 MHz – 10 MHz
			Strom:	≤ 10 mA, ≤ 100 µA
			min. Breite:	0,35 µm
			EEPROM Pg.:	32 Byte
			EEPROM W/E-Zykl.:	100 000
			EEPROM Dauer W/E:	3 ms / 1,5 ms
			HW:	RNG
Hitachi AE350	ROM:	48 kByte	CPU:	AE-3
	EEPROM:	32,5 kByte	Vcc:	2,7 – 5,5 V
	RAM:	1 280 kByte	Takt:	1 MHz – 10 MHz
			Strom:	≤ 10 mA, ≤ 100 µA
			min. Breite:	0,35 µm
			EEPROM Pg.:	64 Byte
			EEPROM W/E-Zykl.:	100 000
			EEPROM Dauer W/E:	3 ms / 1,5 ms
			HW:	RNG
Hitachi AE45X-B/C	ROM:	128 kByte	CPU:	AE-4
	EEPROM:	36 kByte	Vcc:	2,7 – 5,5 V
	RAM:	4,5 kByte	Takt:	1 MHz – 10 MHz
			Strom:	≤ 10 mA, ≤ 100 µA
			min. Breite:	0,35 µm
			EEPROM Pg.:	64 Byte
			EEPROM W/E-Zykl.:	500 000
			EEPROM Dauer W/E:	3 ms / 1,5 ms
			HW:	2 Timer à 16 Bit, UART für ISO/IEC 7816 und ISO/IEC 14 443, PLL, MMU, RNG, DES, RSA
Hitachi AE460	ROM:	96 kByte	CPU:	AE-4
	EEPROM:	64,5 kByte	Vcc:	2,7 – 5,5 V
	RAM:	3 kByte	Takt:	1 MHz – 10 MHz
			Strom:	≤ 10 mA, ≤ 100 µA
			min. Breite:	0,35 µm
			EEPROM Pg.:	128 Byte
			EEPROM W/E-Zykl.:	100 000
			EEPROM Dauer W/E:	3 ms / 1,5 ms
			HW:	MMU, RNG, DES
Hitachi AE46C	ROM:	196 kByte	CPU:	AE-4
	EEPROM:	68 kByte	Vcc:	2,7 – 5,5 V
	RAM:	6,5 kByte	Takt:	1 MHz – 10 MHz
			Strom:	≤ 10 mA, ≤ 100 µA
			min. Breite:	0,35 µm
			EEPROM Pg.:	128 Byte
			EEPROM W/E-Zykl.:	500 000
			EEPROM Dauer W/E:	3 ms / 1,5 ms
			HW:	2 Timer à 16 Bit, UART, PLL, MMU, RNG, DES, RSA

Tabelle 16.26 (Fortsetzung)

Hersteller und Typ Speicher			Detailinformationen	
Philips P8WE6004	ROM:	32 kByte	CPU:	CPU: 8051
	EEPROM:	4 kByte	Vcc:	2,7 – 5,5 V
	RAM:	768 Byte	Takt:	1 MHz – 8 MHz
			Strom:	⊗, ⊗
			min. Breite:	0,35 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	100 000
			EEPROM Dauer W/E:	2 ms / 2 ms
			HW:	2 Timer à 16 Bit, UART, RNG, DES
Philips P8RF6004	ROM:	32 kByte	CPU:	CPU: 8051
	EEPROM:	4 kByte	Vcc:	2,7 – 5,5 V
	RAM:	1 280 Byte	Takt:	1 MHz – 8 MHz, 13,56 MHz (für RF)
			Strom:	⊗, ⊗
			min. Breite:	0,35 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	100 000
			EEPROM Dauer W/E:	2 ms / 2 ms
			HW:	2 Timer à 16 Bit, UART für ISO/IEC 7816 und ISO/IEC 14 443A, MMU, RNG, DES
Philips P8RF5016	ROM:	64 kByte	CPU:	CPU: 8051
	EEPROM:	16 kByte	Vcc:	2,7 – 5,5 V
	RAM:	2 300 Byte	Takt:	1 MHz – 8 MHz, 13,56 MHz (für RF)
			Strom:	⊗, ⊗
			min. Breite:	0,35 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	100 000
			EEPROM Dauer W/E:	2 ms / 2 ms
			HW:	2 Timer à 16 Bit, UART für ISO/IEC 7816 und ISO/IEC 14 443A, MMU, RNG, DES, RSA
Philips P16WX064	ROM:	208 kByte	CPU:	CPU: XA2
	EEPROM:	64 kByte	Vcc:	2,7 – 5,5 V
	RAM:	7 kByte	Takt:	1 MHz – 6 MHz
	Flash (optional):	32 kByte	Strom:	⊗, ⊗
			min. Breite:	0,18 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	100 000
			EEPROM Dauer W/E:	2 ms / 2 ms
			HW:	2 Timer à 16 Bit, UART, CRC, MMU, RNG, DES, RSA
Philips P9CC160	ROM:	320 kByte	CPU:	CPU: MIPS
	EEPROM:	64 kByte	Vcc:	1,62 – 5,5 V
	RAM:	7 kByte	Takt:	1 MHz – 6 MHz
	Flash:	96 kByte	Strom:	⊗, ⊗
			min. Breite:	0,18 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	100 000
			EEPROM Dauer W/E:	2 ms / 2 ms
			HW:	2 Timer à 16 Bit, UART, MMU, RNG, DES, AES, RSA

Tabelle 16.26 (Fortsetzung)

Hersteller und Typ Speicher			Detailinformationen	
Philips P16WX064	ROM:	160 kByte	CPU:	CPU: 8051 Derivat
	EEPROM:	64 kByte	Vcc:	1,62 – 5,5 V
	RAM:	4,3 kByte	Takt:	1 MHz – 10 MHz, 13,56 MHz (für RF)
			Strom:	Ⓢ, Ⓢ
			min. Breite:	0,18 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	100 000
			EEPROM Dauer W/E:	2 ms / 2 ms
			HW:	2 Timer à 16 Bit, UART für ISO/IEC 7816, USB und ISO/IEC 14 443A, CRC, MMU, RNG, DES, AES, RSA
ST Micro-electronics ST16SF4x	ROM:	16 kByte	CPU:	6805
	EEPROM:	1,25/2/4/8/16 kByte	Vcc:	2,7 – 5,5 V
	RAM:	384 Byte	Takt:	1 MHz – 5 MHz
			Strom:	Ⓢ, Ⓢ
			min. Breite:	0,7 µm
			EEPROM Pg.:	1 – 32 Byte
			EEPROM W/E-Zykl.:	300 000
			EEPROM Dauer W/E:	2,5 ms
			HW:	MMU, RNG
ST Micro-electronics ST19RF08	ROM:	32 kByte	CPU:	ST7
	EEPROM:	8 kByte	Vcc:	2,7 – 5,5 V
	RAM:	960 Byte	Takt:	1 MHz – 10 MHz
			Strom:	Ⓢ, Ⓢ
			min. Breite:	0,6 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	100 000
			EEPROM Dauer W/E:	1 ms
			HW:	1 Timer à 16 Bit, ISO/IEC 7816 und ISO/IEC 14 443-B, CRC, MMU, RNG, DES
ST Micro-electronics ST19WG34	ROM:	176 kByte	CPU:	ST7
	EEPROM:	34 kByte	Vcc:	1,6 – 5,5 V
	RAM:	6 kByte	Takt:	1 MHz – 10 MHz
			Strom:	Ⓢ, Ⓢ
			min. Breite:	0,18 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	500 000
			EEPROM Dauer W/E:	2 ms
			HW:	3 Timer à 16 Bit, CRC, MMU, RNG, DES
ST Microelectronics ST22WJ64	ROM:	224 kByte	CPU:	ST22
	EEPROM:	64 kByte	Vcc:	2,7 – 5,5 V
	RAM:	8 kByte	Takt:	1 MHz – 30 MHz
			Strom:	Ⓢ, Ⓢ
			min. Breite:	0,18 µm
			EEPROM Pg.:	1 – 128 Byte
			EEPROM W/E-Zykl.:	500 000
			EEPROM Dauer W/E:	2 ms
			HW:	2 Timer à 16 Bit, UART, PLL (bis zu 30 MHz), MMU, RNG, DES
Infineon SLE 66C160P	ROM:	64 kByte	CPU:	8051 Derivat
	EEPROM:	16 kByte	Vcc:	2,7 – 5,5 V
	RAM:	2,3 kByte	Takt:	1 MHz – 10 MHz
			Strom:	Ⓢ, Ⓢ
			min. Breite:	0,25 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	500 000
			EEPROM Dauer W/E:	4,5 ms (schreiben und löschen)
			HW:	2 Timer à 16 Bit, UART, CRC, PLL, DES, MMU, RNG

Tabelle 16.26 (Fortsetzung)

Hersteller und Typ Speicher			Detailinformationen	
Infineon SLE 66C640P	ROM:	136 kByte	CPU:	8051 Derivat
	EEPROM:	64 kByte	Vcc:	2,7 – 5,5 V
	RAM:	4,3 kByte	Takt:	1 MHz – 10 MHz
			Strom:	≤ 10 mA, Ⓢ
			min. Breite:	0,22 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	500 000
			EEPROM Dauer W/E:	4,5 ms (schreiben und löschen)
			HW:	2 Timer à 16 Bit, UART, CRC, PLL, MMU, RNG
Infineon SLE 66CX642P	ROM:	200 kByte	CPU:	8051 Derivat
	EEPROM:	64 kByte	Vcc:	1,62 – 5,5 V
	RAM:	4,3 kByte	Takt:	1 MHz – 15 MHz
			Strom:	≤ 10 mA, Ⓢ
			min. Breite:	0,22 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	500 000
			EEPROM Dauer W/E:	4,5 ms (schreiben und löschen)
			HW:	2 Timer à 16 Bit, UART, CRC, PLL, MMU, RNG, DES, RSA
Infineon SLE 88CX720P	ROM:	240 kByte	CPU:	Infineon 88, 32 Bit
	EEPROM:	80 kByte	Vcc:	1,62 – 5,5 V
	RAM:	8 kByte	Takt:	1 MHz – 15 MHz
			Strom:	≤ 30 mA, Ⓢ
			min. Breite:	0,22 µm
			EEPROM Pg.:	1 – 64 Byte
			EEPROM W/E-Zykl.:	500 000
			EEPROM Dauer W/E:	4,5 ms (schreiben und löschen)
			HW:	2 Timer à 16 Bit, UART, CRC, PLL (bis zu 55 MHz), MMU, RNG, DES, RSA

Sachverzeichnis

µP-Karte · 906
 0-PIN · 906
 1/0, 8/... µm-Technologie · 906
 16-Bit-Code · 161
 1G · 733; 906
 2, 5 G · 734
 2G · 733; 906
 32-Bit-Code · 162
 3DES · 906
 3-DES · 190
 3G · 734; 906
 3GPP · 796; 906
 3GPP2 · 756; 906
 4004 · 68
 4G · 734; 906
 7-Bit-Code · 160
 8-Bit-Code · 160

A
 A2C · 907
 A3 · 907
 A5 · 907
 A8 · 907
 Abbruchtest · 598
 Abgeleitete Schlüssel · 204
 Ablaufpfade · 600
 Ablaufsteuerung · 283; 907
 ABS · 42
 Abschalten der Stromversorgung · 558
 Abschaltsequenz · 63; 907
 abstract syntax notation one · 154; 909
 Abtastzeitpunkte · 1021
 Abtastzone · 383
 access conditions · 271; 955
 Access Control Descriptor · 167
 ACD · 167
 Acquirer · 696; 907
 Acrylnitril-Butadien-Styrol · 42
 ADF · 800
 ADN · 753
 Advanced Encryption Standard · 187; 907
 advanced mobile phone system · 907
 AES · 907
 AFNOR · 907
 AFNOR-Position · 666
 AID · 264; 907
 Algorithmus · 186
 kryptografischer · 930
 American National Standards Institute · 908
 Amplitude Shift Keying · 97; 909
 AMPS · 733; 907
 AMS · 657
 analog · 908
 Analyse · 908
 Analyse einer Chipkarte · 876
 Anbindung von Terminals · 674
 A-Netz · 732
 Anforderungsspezifikation · 880
 Angreifer · 522
 Einstufung von · 525

Angriff
 Auswirkungen eines · 525
 differential fault analysis · 562
 Differential Power Analysis · 548; 946
 Differenzielle Fehleranalyse · 562
 Einstufung von · 523
 fault analysis · 562
 Lawineneffekt · 522
 meet-in-the-middle · 189
 Power Analysis · 548
 Simple Power Analysis · 548
 Timing Analysis · 561
 Try-and-error bei PIN · 367
 Angriffe · 522; 529; 532; 533
 Angriffssattraktivität
 Einstufung der · 527
 Anlegen einer Anwendung · 479
 Anonymisierung · 908
 Anordnung von Kartenelementen · 93
 Anschaltsequenz · 63; 908
 ANSI · 908
 answer to reset · 909
 Answer to Reset · 384
 Answer to Select · 141
 Antennen-Array · 739
 Antikollisionsverfahren · 908
 Antwort · 908
 Antwort-APDU · 429; 432; 908
 Antwortdaten · 646
 Anwendung · 908
 Dateien · 260
 geschlossene · 922
 offene · 934
 Anwendungsbetreiber · 908
 Anwendungsgebiete für Chipkarten · 6
 Anwendungsspezifische Kommandos · 498
 anwendungsübergreifende Zugriffe · 283
 APDU · 429; 908
 A-PET · 44
 API · 908
 Applet · 311; 909
 applet developer · 908
 Applet-Entwickler · 908
 Applet-Managementsysteme · 657
 application · 908
 APPLICATION BLOCK · 479; 480
 application dedicated file · 800
 Application Identifier · 264; 907
 application programming interface · 908
 application protocol data unit · 429; 908
 Application Specific Command · 303
 Applikationsgenerator · 374; 872
 Äquivalenzklassen · 600
 Arimura, Kunitaka · 3
 ARM Prozessor · 70
 Arten von Karten · 17
 ASC · 303
 ASCII · 160
 ASK · 909
 ASK RANDOM · 466
 ASN.1 · 155; 846; 909

- Assembler · 909
- assessment · 893
- asymmetrischer Kryptoalgorithmus · 180; 909
- asynchrone Datenübertragung · 909
- asynchrone Übertragungsprotokolle · 428
- atomarer Ablauf · 293; 909
- ATQB · 132
- ATR · 384; 565; 909
 - Beispiele aus der Praxis · 396
 - Nutzung zu EEPROM-Schreibvorgängen · 385
- ATR-Datei · 393
- ATR-Test · 584
- ATS · 141
- ATTRIB · 135
- Attribut · 909
- Attribute von Dateien · 274
- AuC · 749
- Aufbau einer kontaktlosen Chipkarte · 95
- Aufladebevollmächtigter · 696
- Ausfallcharakteristik des EEPROM · 853
- ausführbaren Spezifikationen · 595
- Ausführungsgeschwindigkeiten von Algorithmen · 854
- Ausnahmebehandlung · 310
- Auswurfleser · 909
- authentication centre · 749
- Authentic-Verfahren · 436
- Authentifizierung · 219; 909
- Authentisierung · 219; 909
- Authentisierungskommandos · 465
- Authentisierungszentrum · 749
- Authentizität · 909
- Automat · 909
- Automatentheorie · 164
- Autorisierung · 910

- B**
- B2A · 910
- B2B · 910
- B2C · 910
- bad case · 942
- Bad Day Szenario · 910
- Bandspreiztechnik · 738
- Base Station Controller · 749
- Base Transceiver Stations · 749
- Basic Card · 329
- basic encoding rules · 156; 909; 910
- basic multilingual plane · 162
- Basic Test · 602
- BASIC-Interpreter · 300
- baud · 910
- Bearer · 910
- bearer services · 741
- Befehlsabdeckung · 599
- Befehlssatz · 443
 - Ermittlung des · 555
- Behavior Test · 602
- Belastbarkeit · 41
- Belcore-Angriff · 562; 910
- Belcore-Attack · 562; 910
- Benutzer · 910
- Benutzeridentifikation
 - Übertragbarkeit · 510
- Benutzermodus
 - Umschaltung · 545
- Benutzerschnittstelle · 857
- BER · 156; 910
- Beschaltung · 56
- best-fit-Algorithmus · 282
- Besucherregister · 749
- Betriebs- und Wartungszentrum · 749
- Betriebsarten von Blockverschlüsselungsalgorithmen · 187
- Betriebssystem · 235; 910
 - hauptschleife · 346
 - Initialisierung · 346
 - Schichtentrennung · 565
 - undokumentierte Kommandos · 557
- Betriebssystemhersteller · 910
- Betriebssystemkern · 347
- Betriebssystemoperationen
 - Verschleierung · 566
- BEZ · 725
- Bezeichnungen der Kontakte · 56
- BGT · 423
- big Endian · 910
- Binary Phase Shift Keying · 911
- Biometrische Verfahren · 509
- Biometrisches Merkmal
 - dynamische Unterschrift · 519
 - Fingerabdruck · 516
 - Geometrie der Hand · 516
 - Gesicht · 515
 - Iris · 516
 - Netzhaut · 516
 - Schreibrhythmus · 518
 - Stimme · 518
- Blackbox Test · 597
- Blackbox-Test · 911
- Blacklist · 911; 946
- Blacklists · 572
- block guardtime · 423
- block waiting time · 421
- blockorientiert · 179
- Blockschutzzeit · 423
- Blockverkettung · 424
- Blockwartezeit · 421
- Bluetooth · 795; 911
- BMP · 162
- B-Netz · 733
- Bodensatz · 684
- Body · 257; 915
- Bonden · 619
- Bond-out-Chip · 612; 911
- Bootloader · 80; 911
- Börse
 - geschlossene · 922
 - offene · 934
- Börse für Spielautomat · 896
- Börsenanbieter · 695; 911
- Börsenevidenzzentrale · 725
- Börseninhaber · 911
- Bottom-up-Entwurf · 896
- BPSK · 911
- Browser · 911
- brute force attack · 182; 911
- Brute-force-Angriff · 911
- BSC · 749

BSI · 911
 BTS · 749
 Buffern · 912
 Bug fix · 912
 bug fixing · 300
 bumps · 47
 Bundesamt für Sicherheit in der Informationstechnik · 911
 Burst · 912
 business to administration · 910
 business to business · 910
 business to customer · 910
 BWT · 421
 Byte · XVII
 Bytecode · 310; 912
 Byte-Repetition · 410

C

C-450 · 733
 CA · 232; 954
 CAD · 661; 912
 CALCULATE EDC · 487
 CAMEL · 796; 912
 capability maturity model · 890; 914
 Capability Test · 602
 CAP-Datei · 322; 912
 card acceptance device · 912
 card application toolkit · 784
 CARD BLOCK · 482
 card holder verification · 503
 Card Issuer · 928
 card management system · 657
 Card Manager · 296
 Card Modelling Language · 912
 card operating system · 236
 Card Registry · 296
 cardholder verification method · 912
 Cardlet · 311; 912
 CardOS · 236
 CASCADE-Projekt · 70
 case · 431
 CASE · 595
 CAT · 784
 CBC mode
 inner · 190
 outer · 190
 CBC-Mode
 äußerer · 190
 innerer · 190
 CBC-Modus · 188
 CC · 587; 915
 CCITT · 912
 CCR · 661
 CCS · 170; 202; 912
 CDMA · 738; 912
 CDMA · 2000 · 734
 CEN · 13; 913
 central processing unit · 915
 CEPS · 709; 913
 CEPT · 743; 913
 Certificate Authority · 954
 chaining · 424
 Challenge-Response-Verfahren · 220; 913
 CHANGE CHV · 462

CHANGE REFERENCE DATA · 462
 character waiting time · 420
 Check Character · 396
 Chi²-Test · 217
 Chinese Remainder Theorem · 192; 913
 chinesischen Restklassensatz · 192
 chinesischer Restklassensatz · 913
 Chip Accepting Device · 661
 Chip Card Reader · 661
 chip holder verification · 757
 Chipdesign · 538; 611
 Chipgröße · 913
 Chipkarte · 20; 913
 Gewicht der Bauteile · 660
 Lebenszyklus nach ISO 10 202-1 · 609
 Chipkarten
 Anzahl produzierter · 607
 Geschichte der · 2
 Kommandos · 443
 typische Anwendungsfelder · 8
 Chipkarten-Anwendung · 913
 Chipkarten-Betriebssystem · 913
 Hardwareerkennung · 251
 Chipkarten-Kommandos · 1022
 Ausführungszeiten · 870
 Chipkarten-Mikrocontroller · 914
 Chipkartennormung · 13
 Chipkarten-Simulator · 873
 Chipkarten-Terminals · 661
 Chipmodul · 44; 914
 Chip-on-Flex-Modul · 48
 Chip-On-Surface-Verfahren · 51
 Chip-on-Tape · 914
 chosen ciphertext attack · 182
 chosen plaintext attack · 182
 CHV · 503; 757; 914
 CICC · 914
 C-Interpreter · 300
 cipher block chaining · 188
 ciphertext · 179
 ciphertext only attack · 182
 circuit-switched · 951
 CISC · 68
 Class-Datei · 314; 914
 classfile · 914
 Clean Room VM · 914
 Clearing · 690; 914
 Clearingsystem · 914
 CLIP · 914
 CLOSE APPLICATION · 449
 CLOSE CHANNEL · 780
 Close Coupling Card · 101
 Cluster · 740
 CMDA · 735
 CML · 912
 CMM · 890; 914
 CMS · 657
 C-Netz · 732
 code division multiple access · 912; 914
 CODEC · 914
 Code-Inspektion · 597
 Codevielfachzugriff · 738; 912
 Code-Walk-Through · 597
 Codierung alphanumerischer Daten · 160

Codierung mit variabler Länge · 176
 Codierung und Test · 595
 cold reset · 927
 Combikarte · 25; 914
 Combined-Verfahren · 436; 438
 Comité Européen de Normalisation · 913
 command · 929
 Command-APDU · 929
 Common Criteria · 587; 915; 920; 979
 common electronic purse specifications · 709
 COMPARE EEPROM · 488
 COMPARE KEY · 483
 Compiler · 915
 COMPLETION END · 484
 COMPUTE CRYPTO-GRAPHIC CHECKSUM · 471
 COMPUTE DIGITAL SIGNATURE · 473
 Computerviren · 572
 convention · 380
 Coprozessor · 88
 Coprozessor für symmetrische Kryptoalgorithmen · 88
 core foils · 622
 core voltage · 928
 COS · 236; 915
 COT · 914
 Coupon Collector Test · 217
 CP8 · 915
 CPU · 906; 915
 CRC · 915
 CRC-Prüfsumme · 171
 CRC-Recheneinheit · 87
 CREATE FILE · 476
 CRL · 954
 cryptographic checksum · 170; 202; 912
 CSD · 742
 CT-API · 678; 915
 CT-BCS · 678
 CT-ICC · 678
 CVM · 912
 CWT · 420
 CWT-Empfangskriterium · 421
 Cyberflex · 236
 cyclic · 270
 Cyclic Redundancy Check · 171

D

DAM · 755
 D-AMPS · 734; 915
 Danmønt · 6
 DAP · 297
 data authentication pattern · 297
 Data Encryption Algorithm · 183
 Data Encryption Standard · 183; 916
 Database File · 271; 491
 Dateiattribute · 274
 Dateibody · 257; 915
 Dateien · 256
 Selektion · 265
 Dateien bei EN · 1546 · 699
 Dateiheder · 257; 915
 Dateinamen · 261
 Dateistruktur · 267; 915
 Ablaufsteuerung · 271
 cyclic · 270
 Datenbank · 271
 Datenobjekte · 271
 execute · 270
 linear fixed · 268
 linear variable · 269
 transparent · 267
 Dateityp · 258; 915
 Datenaustausch · 856
 Datenelemente von EN · 1546 · 698
 Datenintegrität · 282
 Datenkomprimierung · 176
 Datenobjekt für Chiphersteller · 1003; 1004
 Datensicherungscode · 202
 Datenübertragung · 62; 377
 Abhören der · 557
 hardware-unterstützt · 81
 DBF · 491
 DC/SC · 841
 DCS · 745
 DEA · 183; 915
 DEACTIVATE FILE · 479
 dead locks · 164
 debit card · 915
 Debitkarte · 915
 Debitkarten · 683
 Debugging · 593; 915
 DECIPHER · 472
 Decision Coverage · 599
 Deckfolie · 622; 626
 DECREASE · 459
 DECRYPT · 470
 DECT · 755; 916
 DECT Authentication Module · 755
 Dedicated File · 259
 defined level · 891
 Definierte Stufe · 891
 Definition der Kartenformate · 31
 Defragmentierung · 282; 916
 Delamination · 916
 Delaminierung · 579
 Delegated Management · 298
 DELETE EEPROM · 489
 DELETE FILE · 481
 Depersonalisierung · 654; 916
 DER · 156; 909; 916
 derived key · 204
 DES · 183; 916
 Berechnungszeiten · 185
 DES-3 · 190
 Design · 916
 design pattern · 851
 Detektion der SIM · 758
 deterministisch · 916
 Dethloff, Jürgen · 3
 DF · 259; 916
 DF Name · 264; 916
 DFA · 562; 917
 Dice · 617; 916
 Die · 617; 916
 Die-Bonding · 46; 631
 Diensteanbieter · 917
 differential power analysis · 548
 Differential Power Analysis · 946
 differentielle Fehleranalyse · 917

- differentielle Kryptoanalyse · 917
 - differenzial fault analysis · 562
 - Differenzielle Fehleranalyse · 562
 - Diffusion · 183
 - digital · 917
 - digital cellular system · 745
 - Digital Signature Algorithm · 198
 - Digital Signature Standard · 198
 - digital Signature with Appendix · 229
 - digital Signature with Message recovery · 230
 - digitale Signatur · 202; 229; 831; 917
 - digitale Signaturanwendung · 835
 - digitaler Fingerabdruck · 917
 - digitales Wasserzeichen · 917
 - direct convention · 379
 - direct memory access · 84
 - directory service · 951
 - DISABLE CHV · 464
 - DISABLE VERIFICATION REQUIREMENT · 464
 - Disketten-Terminal · 665
 - diskreten Logarithmusproblem · 198
 - DISPLAY TEXT · 779
 - Distinguished Encoding Rules · 156
 - diversity · 436
 - DMA · 84
 - D-Netz · 743
 - DOV-Modem · 815
 - Downlink · 917
 - Download · 917
 - DPA · 548; 917
 - Draht-Bond-Verfahren · 45; 48
 - DRAM · 81; 917
 - Druckverfahren · 624
 - DSA · 198
 - Berechnungszeiten · 199
 - DSS-Algorithmus · 198
 - Dual Slot Handy · 918
 - Dual-Band-Mobilteléfono · 918
 - Dual-IMSI · 789
 - Dual-Interface-Karte · 25; 918
 - Dual-Mode-Mobilteléfono · 918
 - Dual-Slot-Lösung · 918
 - Dummy-Chipkarte · 554
 - Dummy-Geldausgabeautomaten · 508
 - Dummy-Strukturen · 538
 - Dump-Kommando · 531
 - duplizieren · 918
 - Durchlichthologramme · 36
 - dynamische asymmetrische Authentisierung · 227
 - dynamische Authentisierung · 219
 - dynamische Schlüssel · 205
 - dynamische Testverfahren · 596
 - dynamischer Test · 601
- E**
- EC · 199
 - ECB-Modus · 188
 - ECBS · 918
 - ECC · 169; 199; 918
 - Schlüssellänge · 200
 - Echtschlüssel · 601
 - Echtzeituhr · 671
 - E-Commerce · 918
 - ec-System in Deutschland · 722
 - EDC · 169; 918
 - EDGE · 733; 745; 918
 - EEPROM · 74; 918; 922
 - dynamische Programmierung · 641
 - Fehlererkennung · 89
 - Fehlerkorrektur · 89
 - Reduzierung der Schreibzeit · 641
 - EF · 260; 919
 - Eigenschaften von elektronischem Geld · 687
 - Einbenutzersysteme · 491
 - Einfachanmeldung · 945
 - Einlagenkarte · 919
 - Einschubkarte · 31; 937
 - einseitige Authentisierung · 221
 - Einwegfunktion · 919
 - Einzelbyteempfang · 414
 - Einzelkartendruckmaschine · 623
 - EIR · 749; 751
 - electronic code book · 188
 - electronic purse · 919
 - Elektrische Eigenschaften · 53
 - Elektronenstrahlschreiber · 613
 - elektronische Geldbörse · 693; 919
 - elektronische Mautsysteme · 827
 - elektronische Unterschrift · 229
 - elektronischer Scheck · 919
 - elektronischer Zahlungsverkehr · 682
 - elektronisches Geld · 687
 - Elementary File · 260
 - elementary time unit · 381
 - elliptic curve cryptosystem · 199; 918
 - elliptic curves · 199
 - Elliptische Kurven · 199
 - Embossing · 37; 919; 924
 - Empfangsfolgezähler bei $T = 1$ · 420
 - Emulator · 919
 - EMV · 919
 - EMV-Anwendung · 716
 - EMV-Spezifikation · 716; 919
 - EN · 1546
 - Datenelemente · 698
 - ENABLE CHV · 464
 - ENABLE VERIFICATION REQUIREMENT · 464
 - ENCIPHER · 471
 - ENCRYPT · 470
 - Ende-zu-Ende-Kommunikation · 747; 784
 - Ende-zu-Ende-Verbindung · 919
 - Endianness · 920
 - E-Netz · 743
 - enhanced data rates for GSM and TDMA evolution · 734
 - enrollment · 920
 - Entfärbung · 579
 - Entladen einer EEPROM-Zelle · 77
 - Entscheidungsabdeckung · 599
 - Entwertungszyklus · 692
 - ENVELOPE · 490; 781
 - EP SCP · 744; 920
 - Epilogfeld bei $T = 1$ · 419
 - EPROM · 74; 920
 - e-purse · 919
 - equipment identity register · 749
 - Ermittlung der Übertragungsgeschwindigkeit · 1020
 - error correction code · 169; 918

error counter · 921
 error detection code · 169; 918
 error recovery · 293; 571
 Erweiterung der Chiphardware · 90; 91
 Erzeugung von Geheimnissen · 645
 Erzeugung von Zufallszahlen · 213
 ESD-Festigkeit · 583
 ESD-Schäden · 102
 ETS · 920
 ETSI · 744; 920
 ETSI project smart card platform · 744
 etu · 381; 920
 European Committee for Banking Standards · 918
 Eurosmart · 920
 Evaluationsinstanz · 592
 Evaluierung · 920
 ZKA-Kriterien · 591
 Evaluierung von Software · 585
 Evaluierungsniveau · 590
 Evolutionäres-Modell · 888
 Exception · 310
 Executable Native-Code · 302
 execute · 270
 EXECUTE · 303
 explizite Selektion eines EF · 266
 EXTERNAL AUTHENTICATE · 467

F

f1; f2; f3; f4; f5 · 804; 920
 Fab · 920
 face · 921
 Falltür · 921; 949
 false acceptance rate · 514
 false rejection rate · 514
 FAR · 514
 FAT · 330; 921
 fault tree analysis · 921
 FCOS · 53
 FD/CDMA · 738; 921
 FDMA · 736; 921
 FDN · 752
 Fehlbedienungszähler · 921
 Fehlerbehandlung bei $T = 1$ · 425
 Fehlerbehebungsfunktion · 570; 571
 Fehlerbehebungsverfahren · 293
 Fehlererkennungscode · 169
 Fehlerkorrekturcode · 169
 Fehlerkosten vs. Lebensabschnitt · 880
 FeRAM · 922
 Fernsprechbandbreite · 742
 Fertigstellungsgrad einer Software · 893
 Fertigungsdaten
 typische · 610
 Feststation · 748
 Feststationsteilsystem · 748
 FETCH · 781
 FIB · 921
 FID · 262; 921
 Eindeutigkeit · 263
 FIFO-Speicherverwaltung · 282
 file body · 915

File Identifier · 262
 file management system · 657
 File Manager · 346
 file type · 915
 FINEID · 843; 848
 FIPS · 921
 Firewall · 85; 325; 921
 Firmenadressen · 1006
 firmenspezifische Kommandos · 430
 Flash · 921
 Flash-EEPROM · 79; 921
 Flip-Chip · 53; 632
 float · 684
 Floating Gate · 76
 Floorlimit · 922
 flüchtiger Speicher · 922
 FMS · 657
 focused ion beam · 547; 553; 921
 fokussierter Ionenstrahl · 547; 553
 Footprint · 922
 Format Character · 387
 Formelsammlung · 859
 Fotoresist · 614
 Foundry · 922
 Fowler-Nordheim-Effekt · 76
 Foyerautomat · 725
 FPLMTS · 733; 922
 FRAM · 80
 Frame · 922
 freischwinger Oszillator · 84
 frequency hopping · 737
 frequency reuse · 739
 Frequency Shift Keying · 97
 Frequenzspektrum · 735
 Frequenzsprungverfahren · 737
 Frequenzüberwachung · 543
 Frequenzvielfachzugriff · 736
 Frequenzwiederverwendung · 739
 FRR · 514
 full duplex · 952
 Funktion der Kontakte · 56
 Funktionalität von Mikrocontrollern · 66
 future public land mobile telecommunication service · 733

G

Gap Test · 217
 Garbage Collection · 282; 922
 Gateway-Server · 807
 geätzte Spule · 633
 Geburtstags-Paradoxon · 211
 gedruckte Spule · 635
 gegenseitige Authentisierung · 223
 Geheimzahl · 503
 Geldkarte · 922
 general packet radio service · 794
 general packet radio system · 733
 GENERATE APPLICATION CRYPTOGRAM · 498
 Generatorpolynome für CRC · 172
 gerade Parität · 170
 Gerätekennzeichnungsregister · 749
 Geregelte Stufe · 892

geschichtetes Betriebssystem · 236
 geschlossene Systemarchitektur · 684
 GET CHANNEL STATUS · 780
 GET CHIP NUMBER · 466
 GET INKEY · 779
 GET INPUT · 779
 GET PROCESSING OPTIONS · 497
 GET READER STATUS · 780
 GET RESPONSE · 489
 gewickelte Spule · 633
 Glitch · 562; 923
 Global Platform · XXIII; 295; 923; 935
 global positioning system · 829
 GPRS · 733; 743; 745; 794; 923
 GPS · 829
 Granularität · 923
 Graphentheorie · 166
 Greybox Test · 601; 923
 Greylist · 923
 Größe der Kontakte · 92
 Großzelle · 741
 Grötrupp, Helmut · 3
 GSM · 923
 GSM 900 · 745
 GSM 1800 · 745
 GSM 1900 · 745
 GSM Association · 744; 923; 932
 GSM Komponenten · 748
 GSM Permanent Nucleus · 743
 GSM Systemarchitektur · 748
 GSM-System · 743
 Guillochen · 35; 923
 Gutfall · 923

H

HAL · 923
 Halbbyte · 924; 933
 halbduplex · 924
 Halbleiterproduktion
 Durchlaufzeit · 615
 Maske · 613
 Prozesszeit · 615
 Halbleitertechnologie · 537; 906
 handover · 749; 924
 Happy-Day-Szenario · 924
 hard mask · 924
 Hardmaske · 251; 924
 Hardware
 Initialisierung · 346
 hardware abstraction layer · 923; 942
 hardware security module · 925
 Hardware-unterstützte Speicherverwaltung · 83; 85
 HASH · 472
 Hash-Funktion · 210; 924
 HBCI · 924
 Header · 257; 915
 Heimatnetz · 924
 Heimatregister · 749
 Heißsiegeln · 36
 Henry, Edward Richard · 517
 high update aktivität · 775
 High-Order Differenzial Power Analysis · 549

Hintergrundsystem · 690; 924
 Historical Characters · 393
 HLR · 749; 751
 hochgeprägte Karten · 17
 Hochprägung · 37; 924
 Hologramm · 36; 924
 home location register · 749
 Homezone · 790; 925
 horizontaler Prototyp · 925; 938
 host security module · 925
 Hot-Electron-Injection · 79; 918; 921
 Hotlist · 925
 Hot-Stamp-Verfahren · 36; 624; 629
 HSCSD · 743; 745; 923; 925
 HSM · 925
 HTML · 925
 Huffman-Algorithmus · 176
 Hybridkarte · 925
 Hypertext · 925

I

I/O-Manager · 346
 I2C-Bus · 407
 ICC · 925
 ICCID · 752
 ID-00 · 33
 ID-000 · 32
 ID-1 · 32
 ID-1 Karte · 925
 IDEA · 185
 Berechnungszeiten · 186; 187
 IDEA-Algorithmus · 185
 identifizierendes Nummernsystem · 855
 Identifizierung · 925
 Identifizierungskommandos · 461
 IEC · 925
 IFD · 661; 926
 IFSC · 419
 IFSD · 419
 IMEI · 752
 Implanter · 638; 926
 Implantierung · 636
 Implementierung · 926
 implizite Selektion eines EF · 266
 IMSI · 753; 771
 IMSI-Catcher · 771; 926
 IMT-2000 · 733; 926
 in vehicle unit · 828
 INCREASE · 459
 Individualisierung · 926
 Induktionstelegrafen · 731
 induktive Kopplung · 94
 information field size for the card · 419
 information field size for the interface device · 419
 Informationsfeld bei T = 1 · 419
 Initial Character · 386
 initial level · 891
 initial waiting time · 384
 Initiale Stufe · 891
 Initialisierer · 926
 Initialisierung · 643; 926
 kryptografische Absicherung · 651; 653

Initialisierungsvektor · 189
 Inkrementelles Modell · 888
 Inlettfolie · 926
 Inmarsat · 756
 In-Mold-Labeling · 623
 input commands · 786
 Instrumentierung · 599; 926
 integrated chip card · 925
 Intel · 4004 · 68
 Interface Characters · 388
 Interface Device · 661
 INTERNAL AUTHENTICATE · 466
 Internal EF · 258
 Internal Elementary File · 260
 international mobile subscriber identity · 771
 international mobile telecommunication at · 2000 MHz · 733
 International Telecommunications Union · 733
 interoperabel · 926
 Interpreter · 300; 926
 INVALIDATE · 479
 inverse convention · 379
 IPES · 186
 IrDA · 795
 Iridium · 756
 IS-54 · 734
 IS-95 · 735
 ISDN · 690; 926
 ISO · 11; 927
 ISO-Position · 666
 Iteratives Prozeßmodell · 889
 ITSEC · 588; 927
 generische Oberbegriffe · 589
 Grundbedrohungen · 588
 Mechanismenstärke · 590
 sicherheitsrelevante Grundfunktionen · 589
 ITU · 733; 927
 IuKDG · 832
 IV · 189
 IVU · 828

J

Java · 308; 927
 API · 313
 Class-Datei · 314
 Eigenschaften · 310
 Programmiersprache · 309
 Softwareentwicklung · 322
 Zukunft · 327
 Java Card · 308; 309; 927
 Algorithmen · 326
 Anwendungslektion · 324
 Anwendungstrennung · 325
 Atomare Abläufe · 325
 Ausführungsgeschwindigkeit · 324
 Dateisystem · 325
 Export · 326
 Firewall · 325
 Kryptografie · 326
 Löschen von Applets · 326
 Löschen von Objekten · 325
 Persistente Objekte · 325
 Speicherplatzminimierung · 326

 Transaktionsintegrität · 325
 Transistente Objekte · 325
 Java Card Forum · 309; 927
 Java Card Runtime Environment · 927
 Java Card Virtual Machine · XXIV; 927
 Java Development Kit · XXIV; 927
 Java Virtual Machine · 310; 314
 Java VM
 Loader · 316
 Java VM · 310
 Bytecode Verifier · 316
 Evaluierung · 315
 Heap · 316
 Interpreter · 316
 Security Manager · 316
 Stack · 316
 Java-Beschleuniger · 88
 JCRE · 927
 JCVM · 927
 JDK · 927
 JIT-Compiler · 311
 Just-In-Time-Compiler · 311
 Just-In-Time-Personalisierung · 655
 JVM · 310; 314

K

Kaltreset · 63; 402; 927
 kapazitive Kopplung · 94
 Kapselung von Anwendungen · 566
 Karte · 927
 Kartenakzeptant · 928
 Kartenauswurf · 669
 Kartenbenutzer · 928
 Kartenbesitzer · 928
 Karteneigentümer · 928
 Kartenelement · 34; 928
 Kartenemittent · 928
 Kartenformate · 30
 Kartenherausgeber · 928
 Kartenhersteller · 928
 Karteninhaber · 928
 Kartenkörper · 40; 928
 Einlagenaufbau · 622
 Kartenkörper mit Spule · 630
 Mehrlagenaufbau · 622
 Spritzguss · 623
 Kartenleser · 928
 Kartenmanagementsysteme · 657
 Kartenmaterialien · 42
 Kavität · 627; 928
 Kc · 753
 Kerckhoff, August · 179
 Kerckhoff-Prinzip · 179
 Kerckhoffs Prinzip · 527
 Kern · 928
 Kernel · 928
 Kernfolie · 622; 928
 Kernspannung · 928
 key · 942
 key management · 942
 Ki · 753
 Kilo · XVII

Kinegramm · 36; 929
 Kippbild · 36; 929
 Klartext · 178
 Klasse · 929
 klassifizierendes Nummernsystem · 855
 Klassifizierungsbaum
 Dateistrukturen · 267
 Klon · 929
 klonen · 929
 Knotenadresse · 418
 known plaintext attack · 182
 Kollision · 929
 Kommando · 929
 case · 431
 private use · 430
 undokumentiert · 557
 Kommando Codierungen · 1028
 Kommandoabarbeitung · 242
 Kommando-APDU · 429; 430; 929
 Kommandointerpreter · 347
 Kommandos · 443
 Kommandos für Datenbanken · 491
 Kommandos für Debitkarten · 497
 Kommandos für elektronische Geldbörsen · 494
 Kommandos für Kreditkarten · 497
 Kommandos Klassifizierungsbaum · 446; 447
 Kommandos zum Test der Hardware · 486
 Kommandos zur Auswahl von Dateien · 447
 Kommandos zur Verwaltung von Dateien · 475; 482
 Kommandos für Komplettierung · 482
 komplettieren · 929
 Komplettierung · 248; 482; 642
 Komplettierungsablauf · 485
 Konfusion · 183
 Kontaktbehaftete Karte · 91
 Kontaktfläche · 929
 Kontaktiereinheit · 667
 Kontaktierung · 666
 Kontaktlose Chipkarte · 23
 kontaktlose Karte · 929
 Kontaktlose Karte · 9
 Answer to Reset · 105
 Antikollision · 99
 Datenübertragung · 97
 Energieübertragung · 96; 103
 Induktive Datenübertragung · 103
 Induktive Kopplung · 95
 Kapazitive Datenübertragung · 105
 kapazitive Kopplung · 98
 Koppelemente · 102
 Stand der Normung · 100
 Konzept · 595
 Konzeption · 857
 Kosten für die Fehlersuche · 602
 Kosten für Fehlerbehebung · 596
 Krankenversichertenkarte · 822
 Systemaufbau · 826
 Kreditkarte · 683; 929
 Kreditkarte mit Chip · 716
 Kryptoalgorithmen
 Überblick · 191
 Kryptoalgorithmus · 929
 rauschfrei · 560
 Kryptoanalyse · 178

Kryptobibliothek · 243
 Kryptocoprozessor · 930
 Kryptografie · 178
 kryptografische Funktionen · XVII
 kryptografisches Token · 841
 Kryptokarte · 930
 Kryptologie · 177
 Kurzmitteilungsdienst · 946
 Kurznachrichten · 753
 Kurzschlussfestigkeit · 670
 kuvertieren · 655; 930
 Kuvertiermaschine · 655
 KVK · 822

L

Ladebeauftragter · 930
 Laden einer EEPROM-Zelle · 77
 Ladezentralen · 725
 Laminierung · 622; 930
 LANGUAGE NOTIFICATION · 779
 Lasercutter · 930
 Lasergravur · 37; 930
 Lasern · 37
 Lastenheft · 880
 Lastmodulation · 97
 Lauflängencodierung · 176
 LAUNCH BROWSER · 781
 Lc-Feld · 431
 Lead-Frame Modul · 930
 Lead-Frame-Modul · 50
 Leadtime · 930
 Lebensdauer · 852
 Lebenszyklus · 930
 Le-Feld · 431
 Leistungsanbieter · 695; 930
 leistungsorientiert · 930
 LEN-Feld · 419
 Lesekommandos · 450
 Lettershop · 655
 LFSR · 213
 Lichtangriff · 563
 life cycle · 930
 life cycle management · 658
 life cycle models · 883
 Lifekey · 601
 light attack · 563
 linear fixed · 268
 linear rückgekoppeltes Schieberegister · 213
 linear variable · 269
 Linker · 930
 Linux · 679
 little Endian · 931
 load agent · 696; 930
 Loader · 931
 Location based Service · 931
 LOCK · 481
 logical channels · 441; 931
 logische Funktionen · XVII
 logische Kanäle · 931
 Logische Kanäle · 441
 Longitudinal Redundancy Check · 170
 LRC · 170
 Lufthansakarte · 819

M

- M/Chip · 931
- MAC · 170; 202; 931
- Mächtigkeit des Schlüsselraums · 180
- Magnetkarte · 931
- Magnetstreifenkarte · 18; 931
- Makrozelle · 741
- MANAGE ATTRIBUTES · 477
- MANAGE CHANNEL · 490
- MANAGE SECURITY ENVIRONMENT · 470
- managed level · 892
- Maosco · 931
- Maske · 613; 931
- Maßnahmenkataloge · 833
- Master File · 259
- Master Key · 204
- Master-Slave-Beziehung · 781
- Master-Slave-Verhalten · 377
- Matching-On-Chip · 514
- M-Commerce · 931
- MCOS · 236
- MD4 · 212
- MD5 · 212
- meet-in-the-middle-attack · 189
- Mega · XVII
- Mehrbenutzersysteme · 491
- Mehrfachverschlüsselung · 189
- Mehrlagenkarte · 931
- Mehrwertdienste · 779
- MEL · 300; 712
- Memorandum of Understanding · 744
- memory card · 946
- Memory Footprint · 922; 931
- memory management unit · 85; 86; 303; 566
- message authentication code · 170; 202
- Metallisierungsebenen · 539; 540
- Methode · 931
- MEtX · 796; 931
- MF · 259; 932
- MFC · 723
- Micardo · 236
- Microbrowser · 932
- Mikrobrowser · 805
- Mikrocontroller · 932
 - Chipfläche von · 67
 - Herstellungskosten von · 65
 - Selbstzerstörung · 533
 - Verfügbarkeit von · 67
- Mikrocontroller für Chipkarten · 64
- Mikrocontroller für Mikroprozessorkarten · 1035
- Mikroprobennadel · 547
- Mikroprozessor · 932
- Mikroprozessorkarte · 7; 22; 932
- Mikroschrift · 35
- Mikrozelle · 741
- MILENAGE-Algorithmus · 805; 932
- Miller-Rabin-Test · 196
- Mini-Karte · 31
- Minutien · 517
- Mischnummern · 855
- MKT · 678; 932
- MKT-Spezifikation · 674; 678
- MLI · 36
- MMU · 85; 86; 303; 566
- MM-Verfahren · 38
- Mobile Equipment · 748
- Mobile Station · 748
- Mobile Switching Center · 749
- Mobilfunksysteme · 735
- Mobilvermittlungsstelle · 741; 749
- MOC · 514
- Modul · 932
- Modul mit integrierter Spule · 630
- modulare Exponentiation · 192
- Modularten · 44
- Moduleinbau
 - schwimmend · 627
- Modulhersteller · 932
- Modul-Schnittstellen-Konzept · 245
- Möglichkeiten der Systemstruktur · 689
- Moldkörper · 50; 930
- Mondex · 932
- Mondex-System · 711
- Monoapplication-Chipkarte · 932
- Monofolie · 622
- monofunktionale-Chipkarte · 932
- MORE TIME · 780
- Moreno, Roland · 4
- Morse-Alphabet · 731
- MOSAIC-Technologie · 51
- MOSFET · 76
- MoU · 744; 932
- MPCOS · 236
- MSC · 749
- MSISDN · 753
- multi lane · 827
- Multi User System · 491
- Multiapplication-Chipkarte · 922; 932; 953
- Multiflex · 236
- multifunktionale Chipkarte · 933
- multifunktionalen Chipkarte · 723
- Multifunktionales Kartenterminal · 932
- multiple access · 735; 952
- Multiple Laser Image · 36
- Multiple-Sourcing · 318
- Multitasking · 933
- Multithreading · 933
- Multos · 236; 328; 712; 933
- MUSCLE · 679
- MUTUAL AUTHENTICATE · 468
- Mutual Authentication · 223

N

- Nachvollziehbarkeit · 609
- NAD · 418
- Namensraum · 933
- Nativcode · 933
- nativer Programmcode · 299
- NBS · 933
- NCSC · 933
- negative file · 933
- negotiable mode · 399
- Nibble · 933
- Nichtabstreitbarkeit · 178; 933
- nichtflüchtige Speicher · 933

niederwertigstes Bit · XVII
 NIST · 933
 non-repudiation · 933
 non-volatile memory · 933
 Norm · 934
 Definition · 11
 Entstehung einer · 10; 12
 Normenkonformität · 858
 Normenverzeichnis · 977
 Normung · 10
 Chipkarten · 13
 Notationen · XVII
 NPU · 934
 NRZ-Codierung · 103
 NSA · 934
 Null-PIN · 934
 Nullpin-Verfahren · 462; 503
 Nutzdaten · 934
 Nutzen · 623; 934

O

Objekt · 934
 objektorientierte Programmierung · 934
 OBU · 828
 OCF · 678; 934
 offcard Applikation · 934; 935
 Offcard-VM · 322
 Offene Plattformen · 308
 offene Systemarchitektur · 684
 offenes Chipkarten-Betriebssystem · 934
 Öffentliches · 814
 offline-Inhalte · 808
 Offsetdruck · 624
 Oktett · XVII
 OMC · 749
 on board unit · 828
 oncard Applikation · 935
 oncard Matching · 514; 935
 Oncard-VM · 322
 one-way function · 919
 online-Inhalt · 808
 Online-Verhalten · 571
 OP · 295; 935
 OP API · 297
 open card framework · 678; 934
 Open Card Initiative · 678
 OPEN CHANNEL · 780
 Open Platform · 295; 297; 935
 open terminal architecture · 308
 operating system · 910
 operation and maintenance centre · 749
 Operationen auf Dateien · 459
 Optical Fault Induction Attack · 563
 Optimierende Stufe · 892
 optimizing level · 892
 Optische Speicherkarte · 26; 935
 Orange Book · 587
 OSI-Modell der Kommunikation · 379
 OSI-Schicht · 1; 2; 7; 378; 379
 OTA · 308; 747; 784; 935
 output commands · 786
 over the air · 747; 935

overlay foils · 622
 Overlayfolien · 626

P

PA · 548
 Package · 935
 Padding · 201; 935
 pads · 47
 paketerorientiert · 935
 parallele Datenübertragung · 935
 Paritätsbit · 935
 Passivierung · 936
 Passivierungsüberwachung · 542
 Patch · 936
 Patent · 936
 pay before · 683; 936
 pay later · 682; 936
 pay never · 683
 pay now · 683; 936
 Payflex · 236
 PC · 43
 PC/SC · 674; 936
 Crypto Service Provider · 676
 ICC · 678
 ICC Resource Manager · 676
 ICC Service Provider · 676
 ICC-Aware Application · 676
 IFD · 677
 IFD Handler · 677
 service provider · 676
 PC/SC Spezifikation · 674
 PCB-Feld · 418
 PC-Card · 664
 PC-Card Terminal · 664
 PCD · 936
 PCK · 401
 PCMCIA · 664
 PCMCIA-Terminal · 664
 PCOS · 236
 PCS · 745
 PDA · 795
 PEM · 234
 Pentium
 Rechenfehler · 299
 PERFORM CARD APDU · 780
 PERFORM SCQL OPERATION · 492
 PERFORM SECURITY OPERATION · 470
 PERFORM TRANSACTION OPERATION · 493
 PERFORM USER OPERATION · 493
 persistenz · 936
 personal communication system · 745
 personal identification number · 503
 personal unblocking key · 503
 Personalisierer · 936
 Personalisierung · 649; 937
 Durchsatzdiagramm · 653
 kryptografische Absicherung · 651; 653
 Personalisierungstests · 654
 PES · 186
 PET · 44
 PETP · 44
 Pferd
 trojanisches · 949

- Pflichtenheft · 881
 - Phase · 1 · 744
 - Phase · 1; Phase · 2; Phase · 2+ · 937
 - Phase Shift Keying · 97
 - Physikalische Eigenschaften · 29
 - Physikalische Übertragungsschicht · 379
 - Physiologische Merkmale · 515
 - PICC · 937
 - Pick-and-Place-Automat · 49
 - Pikozelle · 741
 - PIN · 503; 937
 - änderbar · 503
 - statisch · 503
 - PIN-Brief · 655
 - PIN-Pad · 503; 937
 - PIN-Vergleich
 - Stromanalyse · 559
 - Zeitanalyse · 560
 - PKCS #1 ... · 15 · 937
 - PKCS #15 · 841
 - PKI · 937
 - plaintext · 178
 - plattformfreie Implementierung · 245; 332
 - plattformunabhängigkeit · 313
 - PLAY TONE · 779
 - PLL-Schaltung · 83
 - PLMN · 732; 937
 - Plug-In · 31; 937
 - Poker Test · 217
 - POLL INTERVAL · 780
 - polling · 781; 937
 - POLLING OFF · 780
 - Polycarbonat · 43
 - Polyethylenterephthalat · 44
 - Polyvinylchlorid · 42
 - portables Terminal · 661
 - POS · 937
 - Position der Kontakte · 92
 - Postoptimierung · 656
 - postpaid · 829; 938
 - Power Analysis · 548
 - POWER OFF CARD · 780
 - POWER ON CARD · 780
 - Power-On-Reset · 938
 - POZ · 723
 - PP · 938
 - PPS · 399
 - PPS-System · 639
 - Prägehologramm · 36
 - Prägekarten · 17
 - prepaid · 829; 938
 - prepaid SIM · 791; 938
 - Primary Flat · 615
 - Primzahlentest
 - probabilistische · 196
 - Prinzip der Wissensteilung · 531
 - Prinzip von Kerckhoff · 179; 527
 - private-use command · 430
 - PRNG · 213
 - proaktivität · 938
 - probabilistisch · 938
 - Profile von Chipkarten · 243
 - Programmcode · XVIII; 938
 - binärkompatibler · 910
 - Prologfeld bei T = 1 · 418
 - PROM · 73
 - proprietär · 938
 - Proprietary Application Identifier Extension · 265
 - Protection Profil · XXVII; 938
 - protocol control byte · 418
 - Protocol Parameter Selection · 399
 - Protocol Type Selection · 399
 - Proton · 710; 938
 - Prototyp · 938
 - Prototypen-Modell · 886; 887
 - PROVIDE LOCAL INFORMATION · 780
 - Proximity Coupling Device · 936
 - Proximity Integrated Circuit Card · 937
 - Proximity Integrated Circuit(s) Cards · 107
 - proximity Karten · 107
 - prozedurale Programmierung · 939
 - Prozessmodell · 939
 - Prozessor · 939
 - Prozessorkarte · 939
 - Prozessortypen · 67
 - Prozessqualität · 893
 - Prozefbreifegrad · 890
 - Prüfebenen · 569
 - Prüfmethode für kontaktlose Chipkarten · 151
 - Prüfung auf Dateizugriff · 288
 - Prüfung auf Echtheit des Terminals · 508
 - Prüfung von Zufallszahlen · 216
 - Pseudonymisierung · 939
 - Pseudozufallszahlen · 213
 - Pseudozufallszahlengenerator · 214
 - Initialwert · 568
 - seed number · 568
 - PSTN · 732; 939
 - PTS · 399
 - PTS0 · 400; 401
 - PTS1 · 401
 - PTS-Ablauf · 401
 - PTS-Anfrage · 399
 - PTS-Request · 399
 - PTSS · 400
 - public land mobile network · 732
 - public switched telephone network · 732
 - Public-Key-Algorithmus · 939
 - PUK · 463; 503; 939
 - Pull-Technologie · 939
 - Pull-Up-Widerstand · 62
 - Purse Holder · 911
 - purse provider · 695; 911
 - Purse-to-Purse Transaction · 688
 - Purse-to-Purse-Transaktion · 939
 - Push-Technologie · 939
 - PVC · 42; 44
- Q**
- Qualitätssicherung und Test · 577
 - Quick · 694; 939
- R**
- RA · 940
 - Radicchio · 939
 - radierfest · 35

RAM · 81; 939
RATS · 141
Raumvielfachzugriff · 738; 942
Rauschfreiheit · 181; 939
RC-Oszillator · 83
REACTIVATE FILE · 480
READ BINARY · 450
reale Händlerkarte · 726
RECEIVE DATA · 780
Record · 940
Recovery Tests · 598
Recycling · 659
Redlist · 940
Redlists · 572
Reed-Solomon-Codes · 173; 282
Reed-Solomon-Fehlerkorrektur · 174
refactoring · 882
REFRESH · 781
regelbasierte Programmierung · 940
REGISTER · 476
Registered Identifier · 264
registration authority · 940
Registrierungsinstanz · 940
Registrierungsstellen für RID · 1004
REHABILITATE · 480
Reifegradstufen von CMM · 891
remote applet management · 747; 788; 940
remote file management · 657; 747; 786; 940
Remote-Coupling-Karten · 106
removable user identity module · 941
repeatable level · 891
Reset · 940
response · 908
response data · 646
response-APDU · 908
Ressource und Sicherheitsattribute · 286
Ressource und Zugriffsregeln · 286; 287
Retikel · 940
Returncode Manager · 242; 347
Returncodes
 Systematik · 432
Review · 597
RFID-System · 94
RFM · 657; 747; 786
RID · 264
RID-Registrierungsstelle · 1004
RISC · 69
RNG · 87
road pricing · 827
roaming · 940
roll back · 571; 940
roll forward · 940
Roll-On-Verfahren · 36; 630
ROM · 73; 941
ROMable Applet · 323
romed application · 941
ROM-Maske · 941
Root-CA · 954
Round-trip Engineering · 941
RSA · 191; 941
 Berechnungszeiten · 195
 geheimer Schlüssel · 193
 öffentlicher Schlüssel · 193
 Schlüsselgenerierung · 195; 197

RSA-Algorithmus · 191
R-UIM · 756; 941
RUN AT COMMAND · 780
RUN GSM ALGORITHM · 498

S

salt · 575; 941
SAM · 696; 941
Sammelbeauftragter · 696; 907; 941
Sandbox · 311; 941
SAT · 779; 944
Satz von Bernoulli · 216
Schachbrettmuster · 641
Schattenkonto · 726
Schicht-7-Chaining · 473
Schirmzelle · 741
Schlechtfall · 942
Schleifkontakte · 667
Schlüssel · 942
Schlüsseldiversifizierung · 204
Schlüsselinformationen · 207
Schlüsselmanagement · 203; 855; 942
Schlüsselversionen · 204
Schreibkommandos · 450
Schutzschichten · 539
SCQL · 491
 Object Description Table · 491
 Privilege Description Table · 491
 User Description Table · 491
Scrambling · 942
 Speicher · 540
Scrambling der Bus · 544
Scratch-Karte · 942
SDL-Symbolik · 163
SDMA · 738; 942
SE · 942
SECCOS · 727; 942
Secret-Key-Algorithmus · 942
secure application module · 696
secure electronic transaction standard · 943
Secure Messaging · 433; 942
security domains · 296
security environment · 942
security functions · 805
security target · 588; 943
Seed · 943
seed number · 213; 568
SEEK · 458
SEIS-Spezifikationen · 841
Seitenorientierung · 943
Selbstzerstörung · 533
SELECT FILE · 448
SELECT ITEM · 779
Selektion
 explizit · 266
 implizit · 266
 Selektion durch Pfadangabe · 267
 Selektion von Dateien · 265
selektivem Ätzen · 539
Selektivzelle · 741
semiformale Beschreibung
 Beispiel dafür · 333
SEND DATA · 780

- SEND DTMF · 780
- send sequence counter · 440
- SEND SHORT MESSAGE · 780
- SEND SS · 780
- SEND USSD · 780
- Sendefolgenummer · 420
- Sendefolgezähler · 440
- Sendefolgezähler bei T = 1 · 420
- Separierung von DFs · 280
- Serial Test · 217
- serielle Datenübertragung · 943
- service provider · 695; 917; 930
- session · 945
- Session Key · 205
- SET · 234; 943
- SET UP CALL · 780
- SET UP EVENT LIST · 781
- SET UP IDLE MODE TEXT · 779
- SET UP MENU · 779
- SHA · 212
- SHA-1 · 212
- shared secrets · 531
- Shared-Batch · 615
- Short File Identifier · 264
- Short-FID · 264; 943
- Shrink · 943
- Shrink-Prozess · 64
- Shutter · 674; 943
- sicheren Zustand · 77
- Sicherheit · 521
- Sicherheit durch Verschleiern · 179
- Sicherheit von Mikrocontrollern · 66
- Sicherheitsbetriebssystem · 241
- Sicherheitschips · 40
- Sicherheitsmerkmale · 34; 40; 570
- Sicherheitsmodul · 672; 943
- Sicherheitstechnik · 501; 671
- Sicherheitsvorgabe · 943
- Sicherheitsvorgaben · 588
- Sicherung · 545
- Sicherung der Datenübertragung · 433
- Sieb des Eratosthenes · 196
- Siebdruck · 624
- SigG · 833; 944
- SIGN DATA · 470
- Signalburst · 912; 943
- Signatur · 202
- Signaturanwendung · 841
- Signaturgesetz · 833; 944
- Signaturkarte · 835; 838; 944
 - Ausführungsbestimmungen · 833
 - DIN-Spezifikation · 834
 - gesetzeskonform · 833
 - Kommandos · 840
 - nicht gesetzeskonform · 833
 - Pseudonym · 832
 - Schlüsselgenerierung · 838
- Signaturverordnung · 833; 944
- SigV · 833; 944
- SIM · 743; 748; 754; 944
- SIM Alliance · 805; 944
- SIM Application Toolkit · XXVIII; 779; 918; 944; 945
- SIM Lock · 945
- SIM service table · 752
- SIM Sperre · 945
- SIM Toolkit · 945
- SIMEG · 744; 945
- SIM-Lock · 791
- Simple Power Analysis · 548
- Simulator · 945
- Simultaneous Engineering · 594
- single lane · 827
- Single User Systems · 491
- Single-Sign-On · 945
- Sitzung · 945
- Sitzungsschlüssel · 205
- skimming · 945
- Skript · 945
- Sleep-Modus · 61
- Small-OS · 332
- Smart Card · 945
- smart card application · 913
- Smart Card Reader · 661
- Smart Label · 945
- Smart Object · 945
- Smartcard · 946
- SMG9 · 744; 946
- SMIME · 234
- SMS · 742; 753; 946
- soft mask · 946
- Softmaske · 251; 946
- Software
 - Metriken für Qualität · 587
- Software-Lebenszyklus · 594
- Solaic · 51
- Solovay-Strassen-Test · 196
- Sonotrode · 634
- SPA · 548; 946
- SPA/DPA-resistent · 946
- space division multiple access · 942
- Space Manager · 729
- Spannungsüberwachung · 543
- specific mode · 399
- Speicherarten · 71
- Speicherdesign · 538
- Speicherinhalte
 - Prüfsummen · 566
- Speicherkapazität des Magnetstreifen · 18
- Speicherkarte · 7; 21; 946
 - Intelligente · 926
- Speicherorganisation · 253
- Speicherscrambling · 540
- Speicherseiten · 279
- Spektraltest · 217
- Spektralverteilung · 216
- Sperrliste · 946
- Sperrlisten · 572
- Spezifikation · 595; 881; 946
- Spiralmodell · 889; 890
- Spritzgusstechnik · 623
- Spule · 630
- SQL · 491
- SQUID · 552
- SRAM · 81; 946
- SSL · 234
- SSO · 945
- Stack · 947
- Standard · 947

Standardzellen · 538
 standortbezogener Dienst · 931
 STARCOS · 236; 947
 Statement Coverage · 599
 stationäres Terminal · 661
 statische asymmetrische Authentisierung · 225
 statische Authentisierung · 219
 statische Testverfahren · 596
 Steganografie · 598; 947
 Stepper · 615
 stepping · 614
 Structured Card Query Language · 491
 Structured Query Language · 491
 Struktur der Nachrichten · 429
 Strukturformeln von Kartenmaterialien · 42
 Strukturierung von Daten · 154
 subscriber identity module · 743
 Subscriber Identity Module · 748
 Suchkommandos · 457
 Sun · 309
 Super Smart Card · 947
 Super-PIN · 503
 Symbole · XVII
 symmetrische Kryptoalgorithmen · 180; 183
 symmetrischer Kartenaufbau · 626
 symmetrischer Kryptoalgorithmus · 947
 synchrone Datenübertragung · 947
 Synchrone Datenübertragung · 404
 Systemintegration · 595
 System-on-Card · 947
 Systemstruktur von Zahlungsverkehrssystemen · 689

T

T = 0 · 410; 947
 T = 1 · 416; 947
 T = 1 nach EMV · 427
 T = 1 nach ISO/IEC · 427
 T = 14 · 427
 T = 2 · 404
 T = · 403
 T3 · 948
 TA1 · 388; 390
 TA2 · 393
 Tabelle der Chipkarten-Returncodes · 1031
 TAB-Technik · 47
 Tachosmart · 848
 Tag · 948
 TAi · 392
 Taktversorgung · 61
 TAN · 949
 Tape · 618
 tape automated bonding · 47
 tape out · 948
 Target of Evaluation · 920; 938; 948
 TB1 · 390
 TB2 · 391
 TBi · 392
 TC · 837
 TC1 · 390
 TC2 · 391
 TC-Anzeige · 38
 TCi · 392

TCOS · 236
 TCSEC · 587; 948
 TD/CDMA · 738; 948
 TDES · 190; 948
 TDMA · 736; 948
 Teiler · 948
 Telefonkarte
 Belegung der Kontakte · 816
 Telegraf · 731
 Telekommunikation · 731
 Temperaturüberwachung · 544
 temporäre Schlüssel · 205
 temporary mobile subscriber identity · 751; 771
 Terminal · 661; 948
 Anbindung · 685
 PC-Card · 664
 Prüfung auf Echtheit · 902
 TERMINAL RESPONSE · 781
 TERMINATE CARD USAGE · 482
 TERMINATE DF · 481
 Test
 Hardware von Mikrocontrollern · 584
 Kartenkörper · 578
 Produktion · 577
 Qualifikation · 577
 Software · 585
 TEST EEPROM · 488
 TEST RAM · 487
 test zone · 383
 Testanwendung · 603
 Testen · 593
 Testing · 948
 testkey · 601
 Testmethoden für Software · 593
 Testmodus · 616
 Umschaltung · 545
 Testpad · 546
 Testschlüssel · 601
 Testspezifikation · 593
 Teststrategien · 596
 Testverfahren · 596
 Testverfahren für Close-coupling-Chipkarten · 152
 Testverfahren für Proximity-coupling-Chipkarten · 152
 Testverfahren für Vicinity-coupling-Chipkarten · 152
 TETRA · 756; 948
 TETRA-SIM · 948
 Thermochrome-Anzeige · 38
 Thermosublimationsdruck · 626
 Thermotransferdruck · 625
 third generation partnership project · XIX; 756; 796; 906
 Thread · 948
 time division/code division multiple access · 921; 948
 TIMER MANAGEMENT · 781
 Timing Analysis · 561
 Timing Attack · 561
 TLV
 Length · 156
 Tag · 156
 Value · 156
 TLV-Format · 949
 TLV-Struktur · 156
 TMSI · 753; 771
 TOE · 948
 Top-down-Entwurf · 896

Top-Level-CA · 954
 TPDU · 404; 429; 949
 Träger · 910
 Trägerdienste · 741
 Transaktion · 949
 Transaktionsnummer · 949
 Transaktionsprimitiven · 677
 Transferkarte · 949
 Transferkarten · 690
 transistenz · 936; 949
 transition zone · 383
 transmission protocol data unit · 404
 transparent · 267
 transport protocol · 950
 transport protocol data unit · 429
 Transport-PIN · 503
 Transportprotokoll · 949
 trap door · 921
 trapdoor · 949
 Triple-Band-Mobiltelefon · 949
 Triple-DES · 190; 949
 Tri-State · 408
 Trivial-PIN · 504; 949
 TRNG · 213
 trojanisches Pferd · 531; 572
 Trustcenter · 233; 832; 835; 837; 937; 949
 Trusted-Third-Party · XXIX; 949
 try-and-error · 367
 TTP · 949
 Tunnel-Effekt · 76
 tunneling · 950
 Tunnel-Oxidschicht · 76

U

UART · 950
 UART-Baustein · 82
 UATK · 756; 784
 Übergangszonen · 383
 Übersetzung von Fachwörtern · 955
 Übersicht über Instruction-Bytes · 1027
 Übertragungsfehler bei T = 0 · 411
 Übertragungsprotokoll · 950
 Übertragungsprotokoll T = 0 · 410
 Übertragungsprotokoll T = 1 · 416
 Übertragungsprotokoll T = 14 · 427
 Übertragungsprotokoll USB · 428
 Übertragungsprotokolle · 403
 Vergleich der · 429
 Übertragungsprotokolle im Überblick · 403
 UCS · 162; 752; 950
 UCS transformation format · 162
 UCS-2 · 752
 UCS-4 · 162
 UICC · 747; 950
 UIM · 950
 UIM application toolkit · 784
 UML · 950
 Umrechnungstabelle für BWT · 1020
 UMTS · 796; 950
 UMTS-System · 796
 Unabhängigkeit von Ereignissen · 216
 UNBLOCK CHV · 463

ungerade Parität · 170
 Unicode · 161; 951
 universal character set · 162
 universal integrated circuit card · 747
 Universal Mobile Telecommunication System · 796
 universal subscriber identity module · 798; 951
 Unterschriftstreifen · 35
 UPDATE BINARY · 450
 Uplink · 951
 Upload · 951
 URL · 951
 USAT · 784; 951
 USAT-Interpreter · 805; 807
 USB · 428
 USB-Protokoll · 82
 USB-Token · 515
 user requirement specification · 880
 Usermodus · 620
 USIM · 798; 951
 USIM Application Toolkit · XXX; 951
 USIM application toolkit · 784
 USSD · 742
 UTF · 162
 UTF-16 · 162
 UTF-32 · 162
 UTF-8 · 162
 UV-Schrift · 35; 36

V

value added service · 955
 VAS · 779; 955
 VEE · 952
 Veranstaltungen · 1005
 Verbindlichkeit · 178
 verbindungsorientiert · 951
 Verhaltensbasierte Merkmale · 517
 VERIFY · 461
 VERIFY CERTIFICATE · 474
 VERIFY CRYPTOGRAPHIC CHECKSUM · 471
 VERIFY DIGITAL SIGNATURE · 474
 VERIFY SIGNATURE · 470
 Verklemmungen · 164
 verlegte Spule · 634
 Verschlüsselung · 177
 versenden · 655
 Versorgungsspannung · 57
 Versorgungsstrom · 59
 vertical stack integration · 91
 vertikaler Prototyp · 938; 951
 Verwaltungsdaten · 951
 Verweise · XVII
 Verzeichnisdienst · 951
 Vicinity Integrated Circuits Cards · 151
 vicinity Karten · 107
 Vielfachzugriffsverfahren · 735; 952
 Vier-Augen-Prinzip · 531
 Virginalkarte · 952
 Virtual Machine · 310; 952
 virtual smart card · 952
 virtuelle Chipkarte · 952
 virtuelle Händlerkarte · 726; 952
 Visa Cash · 694

Visa Easy Entry · 952
 Visa Open Platform · 295
 Visacash · 952
 visitor location register · 749
 VLR · 749; 751
 VM · 310; 952
 V-Modell · 885
 volatile memory · 922
 vllduplex · 952
 VOP · 295; 952
 vorbezahlt · 938
 vorbezahlte SIM · 938
 vorbezahlte Speicherkarten · 692
 Vorgehensmodell · 879; 883; 952
 Vorgehensweise für Tests · 603
 Vorphonalisierung · 952
 VSI · 91

W

W3 · 954
 Wafer · 952
 waiting time extension · 423
 WAP · 808; 952
 WAP Forum · 953
 Warmreset · 63; 402; 953
 Wartezeiten bei $T = 1$ · 420
 Wartezeitverlängerung · 423
 Wasserfallmodell · 594
 Wasserfall-Modell · 884
 Watchdog · 83
 WCDMA · 738; 953
 weiße Karte · 953
 Weißlicht-Reflexionshologramm · 36
 white plastic · 953
 Whitebox Test · 599; 953
 Whitelist · 953
 Whitelists · 572
 wideband code division multiple access · 738; 953
 Wiedereinspielung · 222
 Wiederholbare Stufe · 891
 WIM · 808; 953
 Windows for Smart Card · 330; 332; 953
 Wire-Bonding · 45; 631
 Wireless Identification Module · 808
 wireless markup language · 953
 Wissensteilung · 531; 953
 WML · 953
 work around · 954
 Working EF · 258
 Working Elementary File · 260
 World-Wide-Web-Adressen · 1006
 WORM-Speicherverwaltung · 281
 WRITE BINARY · 450
 WRITE DATA · 484
 WSC · 330
 WWW · 954

X

X.25 · 690
 X.509 · 234; 831; 832; 954
 XML · 155; 954
 XOR-Prüfsumme · 170

Z

Zahlungsströme · 696
 Zahlungsverkehr · 681
 Zeichen- und Zahlendarstellung · XVII
 Zeitbedarf
 Datenübertragung · 862
 EEPROM-Operationen · 861
 Kommandoabarbeitung · 859
 Zeitbereich für den ATR · 1019
 Zeitstempel · 954
 Zeitvielfachzugriff · 736
 Zelle · 954
 Zelltypen · 741
 Zellulartechnik · 739; 954
 Zentrale Kreditausschuss · 723
 Zertifikatswiderrufsliste · 954
 Zertifikat · 232; 954
 Zertifikatsstruktur · 234
 Zertifizierung · 954
 Zertifizierungsinstanz · 232; 813; 937; 949; 954
 Zertifizierungsstelle · 832
 Ziehbarkeit · 669
 ziffern · 955
 ZKA · 723; 955
 ZKA-Kriterien · 591
 Zufallszahlen · 212
 Coupon Collector Test · 219
 Gap Test · 219
 Güte von · 216
 Long Run Test · 219
 Monobit Test · 219
 Pattern Test · 219
 Poker Test · 219
 Runs Test · 219
 Serial Test · 219
 Zufallszahlengenerator · 87; 214; 567
 Startwert · 213
 Zugangskontrolle · 899
 Zugriffsbedingungen · 285; 955
 objektorientiert · 567
 Zugriffsbedingungen auf Dateien · 271
 Zusammenhänge zwischen den Kartenformaten · 33
 Zusatzanwendung · 955
 Zusatzhardware · 81
 Zustandsautomat · 164
 für Komplettierung · 486
 für $T = 0$ · 413
 Realisierung des Lebenszyklus · 643
 Zwei-Chip-Lösung · 90

Handbuch der Chipkarten

Das »Handbuch der Chipkarten« ist das Standardwerk zur Chipkartentechnologie weltweit. Es bietet einen umfassenden Überblick über das gesamte Themengebiet. Als Grundlagen- und Nachschlagewerk ist es für alle unentbehrlich, die sich in der Praxis oder Ausbildung mit Chipkarten beschäftigen.

Die Autoren erklären zunächst die grundlegenden Themen wie Kartenaufbau, physikalische und elektrische Eigenschaften und informationstechnische Aspekte. Daran schließen sich zentrale Themen wie Chipkarten-Betriebssysteme, Datenübertragung zur Chipkarte, Befehlssätze und Sicherheitstechnik an. An zahlreichen Anwendungsbeispielen wie z.B. dem Einsatz im Zahlungsverkehr oder der Verwendung beim Mobiltelefon wird die praktische Umsetzung erläutert.

Das Buch berücksichtigt den aktuellen Stand der internationalen Normung. Die klare Sprache und zahlreiche Abbildungen erleichtern den Zugang zur komplexen Materie. Das Literatur- und Normenverzeichnis, das Glossar, die Übersetzungsliste für Fachbegriffe und die Tabellen der Kennwerte für Chipkarten runden das Handbuch ab.

Im Internet: Der Smart Card Simulator, das Glossar des Buches und weitere Informationen.

4., überarbeitete und
aktualisierte Auflage

HANSER

www.hanser.de

ISBN 3-446-22036-4



9 783446 220362