[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.eracom.com.au/

[ETSI] **ETSI**
Normen
http://www.etsi.fr/

[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 Manufactorers 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 (*Movement for the Use of Smart Cards in a Linux Environment*)**
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.wrankl.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.technodata-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
http://www.unicode.org/

[USB] **USB**
http://www.usb.org/

[Utimaco] **Utimaco AG, Deutschland**
Terminalhersteller
http://www.utimaco.com/

[Verifone] **Verifone Inc., USA**
Terminalhersteller
http://www.verifone.com/

[Visa] **Visa International, USA**
Kartenherausgeber
http://www.visa.com/
http://www.visa.de/

[WAP] **WAP Forum**
Informationen über WAP
http://www.wapforum.org/

[Wiley] **John Wiley & Sons, Inc., Großbritannien**
Smart Card Handbook
http://www.wiley.co.uk/

[Zeitcontrol] **Zeitcontrol Cardsystems GmbH, Deutschland**
Chipkartenhersteller
http://www.zeitcontrol.de/

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	13334,479 msec
8	256011 etu	6 666,953 msec	13 333,906 msec	26667,813 msec
9	512011 etu	13 333,620 msec	26 667,240 msec	53334,479 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
	416,667 µs	447,917 µs	468,750 µs	489,583 µs	520,833 µs
Datenbit 5/4	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
Datenbit 7/2	2 604 Takte	2 716 Takte	2 790 Takte	2 864 Takte	2 976 Takte
	729,167 µs	760,417 µs	781,250 µs	802,083 µs	833,333 µs
Datenbit 8/1	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
Guardtime/ Stopbit 1	3 720 Takte	3 832 Takte	3 906 Takte	3 980 Takte	4 092 Takte
	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 der INS	Norm
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 Benutzer-identifizierung (z. B. PIN).	'24'	ISO/IEC 7816-8
CLOSE APPLICATION	Rücksetzen aller erreichten Zugriffs-bedingungen.	'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 AUTHORISATION 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, Anwen-dung 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 Fehlbedienungszählers.	'2C'	ISO/IEC 7816-8

Tabelle 16.14 *(Fortsetzung)*

Kommando	Funktion	Codierung der INS	Norm
RUN GSM ALGORITHM	Ausführen des GSM-spezifischen Kryptoalgorithmus.	'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-Fehlbedienungszählers.	'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					OP		OP									
Fy	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		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.	
Le	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 (*first*) Record mit dem Record Identifier, übergeben in P1

Tabelle 16.21 *(Fortsetzung)*

Datenelement	Codierung	Bemerkung	
		P2.b3 ... P2.b1 = °001°	Lese den letzten (*last*) Record mit dem Record Identifier, übergeben in P1
		P2.b3 ... P2.b1 = °010°	Lese den nächsten (*next*) Record mit dem Record Identifier, übergeben in P1
		P2.b3 ... P2.b1 = °011°	Lese den vorherigen (*previous*) Record mit dem Record Identifier, übergeben in P1
		P2.b3 ... P2.b1 = °100° ∧ P1 = 0	Lese den aktuellen Record
		P2.b3 ... P2.b1 = °100° ∧ P1 ≠ 0	Lese den Record mit der Recordnummer, übergeben in P1.
		P2.b3 ... P2.b1 = °101°	Lese alle Records ab der in P1 übergebenen Recordnummer bis zum Ende der Datei.
		P2.b3 ... P2.b1 = °110°	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 ≠ 0	Schreibe den Record mit der in P1 übergebenen Recordnummer.
P2	...	P2.b8 ... P2.b4 = °00000°	Schreibe Daten in die aktuell selektierte Datei
		P2.b8 ... P2.b4 ≠ °00000°	Schreibe Daten nach impliziter Dateiselektion durch Short-FID Short-FID = (P1.b8 ... P1.b4)
		P2.b3 ... P2.b1 = °000°	Schreibe den ersten (first) Record
		P2.b3 ... P2.b1 = °001°	Schreibe den letzten (last) Record
		P2.b3 ...P2.b1 = °010°	Schreibe den nächsten (next) Record
		P2.b3 ... P2.b1 = °011°	Schreibe den vorherigen (previous) Record
		P2.b3 ... P2.b1 = °100°	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 Referenzdaten verwendet (global reference data).
		P2.b8 = °1°	Es werden für eine oder mehrere Anwendungen gültige 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 processing*)
WP	Prozess ausgeführt, Warnung	(*process completed, warning processing*)
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 (*invalidated*)	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 veraltern. 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	ROM:	16 Bit	Vcc:	5 V
SLE 4404	PROM:	144 Bit	Strom:	3 mA
	EEPROM:	256 Bit	W/E-Zykl.:	100 000
			Dauer W/E:	5 ms
			HW:	---
Infineon	ROM:	24 Bit	Vcc:	5 V
SLE 4406S	PROM:	72 Bit	Strom:	1 mA
	EEPROM:	32 Bit	W/E-Zykl.:	100 000
			Dauer W/E:	3 ms
			HW:	Zähler für ≈ 20 000 Einheiten
Infineon	ROM:	---	Vcc:	5 V
SLE 44R35	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	ROM:	24 Bit	Vcc:	5 V
SLE 5536	PROM:	177 Bit	Strom:	2,5 mA
	EEPROM:	36 Bit	W/E-Zykl.:	100 000
			Dauer W/E:	3 ms
			HW:	Zähler für ≈ 20 000 Einheiten einseitige Authentisierung
Infineon	ROM:	---	Vcc:	5 V
SLE 4442	PROM:	32 Bit	Strom:	10 mA
	EEPROM:	256 Byte	W/E-Zykl.:	100 000
			Dauer W/E:	2,5 ms
			HW:	---
Infineon	ROM:	24 Bit	Vcc:	3 – 5 V
SLE 7736	PROM:	177 Bit	Strom:	1 mA
	EEPROM:	36 Byte	W/E-Zykl.:	100 000
			Dauer W/E:	3 ms
			HW:	Zähler für ≈ 20 000 Einheiten
Philips	ROM:	---	Vcc:	☹
MF1 S70	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	ROM:	---	Vcc:	☹
I-Code SLI ICPCB 7960	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	ROM:	---	W/E-Zykl.:	100 000
LRI512	PROM:	---	Dauer W/E:	5 ms
	EEPROM:	512 Bit	HW:	ISO/IEC 15 693
ST Micro-electronics	ROM:	---	W/E-Zykl.:	100 000
M35101	PROM:	---	Dauer W/E:	5 ms
	EEPROM:	2048 Bit	HW:	ISO/IEC 14 443 B
ST Micro-electronics	ROM:	16 Bit	Vcc:	5 V
ST1335D	PROM:	---	Strom:	500 µA
	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 veraltern. 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 (*universal asynchronous receiver transmitter*)
Timer:	Zähler zum Messen von Takten
CRC:	Recheneinheit für CRC
PLL: i	nterne Taktvervielfachung (*phase locked loop*)
MMU:	Speicherverwaltungshardware (*memory management unit*)
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	Flash:	64 kByte	CPU:	AVR
SC6464C	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:	☹, ☹
			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 Microlectronics 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 Microlectronics 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 Microelectronics 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

B

C

E

F

G

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

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.

CHIPKARTEN

4., überarbeitete und aktualisierte Auflage

ISBN 3-446-22036-4

9 783446 220362

HANSER www.hanser.de