

**Ergänzungen und Korrekturen
für das
Handbuch der Chipkarten
von
Wolfgang Rankl und Wolfgang Effing**

Autor:	Wolfgang Rankl (Rankl@gmx.net)	Datei:	EuK Liste, HdC 4. dt., V 9.doc ekhdc4_9.pdf
Ausgabe:	3. Dezember 2004	Version:	9
Bemerkungen:	Ergänzungen und Korrekturen für das Handbuch der Chipkarten, 4. deutsche Auflage 2002, Carl Hanser Verlag, München Wien, ISBN 3-446-22036-4 Die Liste beinhaltet i.d.R. keine erkannten Rächtcheipfähler.		

Wir möchten uns an dieser Stelle nochmals bei allen aufmerksamen Lesern herzlich für die Hinweise zu Ergänzungen und Korrekturen am Handbuch der Chipkarten bedanken.

Wolfgang Rankl

Wolfgang Effing

Seite	aufgenommen	Position auf der Seite	unklar / falsch	richtig
Beihefter 1/4	3.12.04	Kommando-APDU	Der Header bei der Kommando-APDU erstreckt sich über das Lc-Feld.	Der Header bei der Kommando-APDU darf sich nur über CLA, INS, P1 und P2 erstrecken.
div.	2.2.03	---	„Select-Kommando“	„SELECT-Kommando“
div.	9.4.03	---	„Mastercard“	„MasterCard“
XXII	4.12.02	32. Zeile von oben	„EFTPOS – electronic found transfer at point of sale“	„EFTPOS – electronic fund transfer at point of sale“
XVIII	17.9.03	9. Zeile von oben	„=, <, >, <>, <=, >=“	„=, !=, <, <=, >, >=“
XXIII	4.12.02	13. Zeile von oben	„FIFO – first in last out“	„FIFO – first in first out“
15	24.2.03	Fußzeile	„Siehe auch Abschnitt 15.4 ...“	„Siehe auch Abschnitt 16.4 ...“
94 - 152	19.9.02	Seitenüberschrift am oberen Rand	„3.5 Kontaktbehafete Karten“	„3.6 Kontaktlose Karten“
121	24.2.03	Tabelle 3.11, Zeile 8 in Tabelle (d.h. letzte Zeile mit Byte count)	„... Byte count = 4“	„... Byte count = 8“
122	2.1.03	Bildunterschrift zu Bild 3.102	„Die Zahlen in den ... des Algorithmus.“	„Die aufgeführten Schritte sind in Tabelle 3.13 im Detail erläutert.“
128	22.4.03	Bild 3.108	falsches Bild	siehe Anhang 4
129	24.2.03	Vorletzte Zeile	“... Ta'05', gefolgt von dem AFI-Byte, ...“	“... '05', gefolgt von dem AFI-Byte, ...“
133	24.2.03	Tabelle 3.20, Zeile 3 in Tabelle (d.h. letzte Zeile)	„Applikation ist codiert wie oben beschrieben“	„Applikation ist codiert wie im Text beschrieben“
134	2.1.03	7. Absatz von unten	„... REQB/WUPB. ATTRIB und HLTB.“	„... REQB/WUPB, ATTRIB und HLTB.“
134	2.1.03	5. Absatz von unten	„... ATRIB-Kommando ...“	„... ATTRIB-Kommando ...“
134	2.1.03	4. Absatz von unten	„... HALTB-Kommando ...“	„... HLTB-Kommando ...“
134	2.1.03	3. Absatz von unten	„... ATTRIB-Kommando ...“	„... ATTRIB-Kommando ...“
135	2.1.03	Bild 3.116	„B7“	„b7“
136	24.2.03	Vorletzter Absatz	„Die Codierung entspricht der Tabelle 3.28.“	„Die Codierung entspricht der Tabelle 3.21.“
137	24.2.03	Absatz nach Bild 3.118	„Die Karte antwortet auf ein gültiges HALT-Kommando folgendermaßen.“	„Die Karte antwortet auf ein gültiges HLTB-Kommando folgendermaßen.“

145	24.2.03	Absatz „Start Byte“	„Das höherwertige Halbbyte b8 bis b5 ist auf 'D' gesetzt ...“	„Das höherwertige Halbbyte b8 bis b5 ist auf 'D' = °1101° gesetzt ...“
148	9.4.03	Tabelle 3.38, bei b8 und b7	...	Die 1 muss in der Mitte zwischen DESELECT und WTX stehen.
148	9.4.03	Tabelle 3.38	„b6 0 1 b5 0 1“	„b6 0 (DESELECT) / 1 (WTX) b5 0 (DESELECT) / 1 (WTX)“
151	2.1.03	Absatz unter 3.6.5	„Die ISO/IEC 10 373 besteht aus 6 Teilen.“	„Die ISO/IEC 10 373 besteht aus 7 Teilen.“
154	24.2.03	Absatz vor „4.1 Strukturierung von Daten“	„... [GMD, Semper] ... [Ascom, Certicom, ...] ... [Gutmann, Tatu] ...“	„... [GMD] ... [Certicom, ...] ... [Gutmann] ...“
155	24.2.03	Tabelle 4.1	„OCTED STRING“	„OCTET STRING“
158	29.12.03	Tabelle 4.6	„Aufbau der DER-basierten Längenangabe ...“	„Aufbau der BER-basierten Längenangabe ...“
166	8.4.03	4. Absatz	„... dann erzeugt der Mikrozustandsautomat eine ...“	„... dann erzeugt der Zustandsautomat eine ...“
181	8.10.02	Bild 4.22, Unterpunkt „Kryptoalgorithmen symmetrisch“	...	„AES“ muß in der Zeichnung ergänzt werden
184	8.10.02	3. Zeile von oben	„... Computer gilt ein Schlüsselraum ...“	„... Computer gilt dieser Schlüsselraum ...“
186	8.10.02	Zeile 5 und 6	„Allerdings unterliegt er, ähnlich wie der RSA-Algorithmus, patentrechtlichen Beschränkungen.“	„Allerdings unterliegt er, ähnlich wie früher der RSA-Algorithmus, patentrechtlichen Beschränkungen.“
192	8.10.02	Bild 4.31	„Entschlüsseln: $x = y^e \text{ mod } n$ “	„Entschlüsseln: $x = y^d \text{ mod } n$ “
194	8.4.03	vorletzter Absatz	„... Rechenleistungen zur Faktorisierung und auch zum Brechen von symmetrischen Kryptoalgorithmen findet sich ...“	„... Rechenleistungen zur Faktorisierung findet sich ...“
194	8.4.03	Fußnote 10	...	letzten Satz ersatzlos streichen
195	8.4.03	Tabelle 4.16, Zeile „Chipkarte mit NPU und 4,9 MHz bei 1024 Bit“	...	„65 ms“ ersatzlos streichen
227	8.4.03	letzter Absatz	„... so ist das unter 4.10.3 beschriebene Verfahren ...“	„... so ist das unter 4.11.3 beschriebene Verfahren ...“
232	8.4.03	erster Absatz	„... muss ein Verfahren wie in 4.10.3 beschrieben ...“	„... muss ein Verfahren wie in 4.11.3 beschrieben ...“
239	8.1.03	Tabelle 5.2	...	In der Spalte „Betriebssystem für GSM um 2002, ...“ sind die Inhalte der Zeilen „Funktionalität“ und „Mikrocontroller“ zu vertauschen.
239	8.4.03	Tabelle 5.2, Spalte „Betriebssystem für GSM um 2002, ...“	„... 3 * Mikrobrowser ...“	„... 3 verschiedene Mikrobrowser ...“
241	8.4.03	Absatz unter „Kommando-Abarbeitung“	„... nachladbaren Programmcode, das keinen nachladbaren Programmcode unterstützt, läuft wie folgt ab: ...“	„... nachladbaren Programmcode läuft wie folgt ab: ...“
263	8.4.03	Tabelle 5.7, Zeile „Datei“	„... Dateigröße: n Bytes Zugriffe: READ: ...“	„... Dateigröße: n Bytes; Zugriffe: READ: ...“
264	8.4.03	letzte Zeile	„... finden sich im Anhang unter „15.7 Registrierungsstellen ...“	„... finden sich im Anhang unter „16.7 Registrierungsstellen ...“
281	8.4.03	2. Absatz	„Bei der Dateiverwaltung und im übrigen auch bei Speicherverwaltungen aller Art mit ...“	„Bei der Speicherverwaltung und im übrigen auch bei Dateiverwaltungen aller Art mit ...“

281	8.4.03	2. Absatz	„Anhand der Dateiverwaltung einer Chipkarte wird dies im Folgenden dargestellt.“	„Anhand der Speicherverwaltung einer Chipkarte wird dies im Folgenden dargestellt.“
282	8.4.03	2. Zeile	„... nach dem FIFO (first in first out)-Prinzip.“	„... nach dem LIFO (last in first out)-Prinzip.“
286	8.4.03	2. Absatz	“Die ISO/IEC 7819-9 definiert ...”	“Die ISO/IEC 7816-9 definiert ...”
289	8.4.03	Tabelle 5.12	„EXTERNAL AUTHENTICATION“	„externe Authentisierung“
290	8.4.03	Tabelle 5.14	„EXTERNAL AUTHENTICATION oder ...“	„externe Authentisierung oder ...“
290	8.4.03	Tabelle 5.15	„INTERNAL AUTHENTICATION“	„interne Authentisierung“
292	8.4.03	Tabelle 5.20, 4. gerahmte Zeile	„Als Sicherheitsbedingung für die folgenden ...“	„Die folgenden ...“
299	8.4.03	Bild 5.40	„INSTALL mit Parameter Laden einer Anwendung“	„INSTALL mit Parameter „Laden einer Anwendung““
308	8.4.03	3. Absatz	„... proprietäre Plattformen, welche in häufig abwertender Form ...“	„... proprietäre Plattformen. Der Begriff wird häufig in abwertender Form ...“
321	8.4.03	Tabelle 5.30	...	doppelte Zeile „javacard.security.MessageDigest ...“ ersatzlos streichen
372	8.4.03	2. Absatz	„In Tabelle 5.64 ist aufgeführt, wie die ...“	„In Tabelle 5.72 ist aufgeführt, wie die ...“
372	8.4.03	2. Absatz	„... wurde der in Bild 5.50 gezeigte ...“	„... wurde der in Bild 5.66 gezeigte ...“
378	8.4.03	Bild 6.2	...	ersetze „PTS“ durch „PPS“
389	8.4.03	Tabelle 6.6, letzte Spalte in erstem Kasten	...	bei FI = 0111 ist fmax ----
397	26.6.03	Tabelle 6.24, bei TB2	„TB2“	„TB3“
397	3.9.03	Tabelle 6.24, bei TB2/TB3	„CWI=3 BWI=4“	„BWI=3 CWI=4“
398	26.6.03	Tabelle 6.25 (Fortsetzung), bei TB2	„TB2“	„TB3“
398	8.4.03	Tabelle 6.25 (Fortsetzung)	„T1 . . . T15 '53' '54' '41' '52' '43' '4F' '53' '32' '31' '20' '43' "STARCOS 21 C"“	„T1 . . . T15 '53' '54' '41' '52' '43' '4F' '53' '20' '32' '31' '43' "STARCOS 21C"“
398	3.9.03	Tabelle 6.25 (Fortsetzung), bei TB2/TB3	„CWI=3 BWI=4“	„BWI=3 CWI=4“
398	3.9.03	Tabelle 6.28 (Fortsetzung), bei TB3	„CWI=4 BWI=5“	„BWI=4 CWI=5“
399	8.4.03	Tabelle 6.29	„PPS1, PPS2, PPS3 The Format Characters“	„PPS1, PPS2, PPS3 The Parameter Characters“
396 – 397	8.4.03	Tabelle 6.23 – Tabelle 6.25	...	Bitwerte sind nicht immer als solche explizit mit „°“ gekennzeichnet
412	8.4.03	letzter Satz	“Die wird work waiting ist im ATR ...”	“Sie ist im ATR ...”
426	8.4.03	6.4.3.4 Beispiel für die Datenübertragung mit T = 1	„6.4.3.4 Beispiel für die ...“	„6.4.3.5 Beispiel für die ...“
427	8.4.03	6.4.3.5 Unterschiede zwischen T = 1 nach ISO/IEC und T = 1 nach EMV	„6.4.3.5 Unterschiede zwischen ...“	„6.4.3.6 Unterschiede zwischen ...“

429	10.4.03	Absatz nach 6.5 Struktur der Nachrichten-APDUS	„Bei Chipkarten ist diese Schicht direkt oberhalb der Übertragungsprotokolle amgesiedelt. Die protokollabhängigen TPDU (transport protocol data unit) hingegen ...“	„Bei Chipkarten ist diese Schicht direkt oberhalb der Übertragungsprotokolle amgesiedelt, deren protokollabhängige Dateneinheiten den Namen TPDU (transmission protocol data unit) haben.“
432	8.4.03	Absatz nach Bild 6.43	„... ist in Bild 6.51 dargestellt.“	„... ist in Bild 6.44 dargestellt.“
455	9.4.03	Tabelle 7.8, Tabelle 7.9, Tabelle 7.10	„... Modus (erster, letzter, nächster, vorheriger Record) ...“	„... Modus (aktueller, erster, letzter, nächster, vorheriger Record) ...“
455	9.4.03	Tabelle 7.9	„... zu schreibender Record Nummer des zu schreibenden Record ...“	„... zu schreibender Record <neue Zeile> Nummer des zu schreibenden Record ...“
466	9.4.03	Tabelle 7.28	„ASK RANDOM / GET CHALLENGE“	„GET CHALLENGE“
479	9.4.03	Tabelle 7.46	„... nach EN 726-3“	„... nach GSM 11.11“
494	9.4.03	3. Absatz	„... auch in das Unterkapitel „7.14 Anwendungsspezifische Kommando“ passen, ...“	„... auch in das Unterkapitel „7.16 Anwendungsspezifische Kommando“ passen, ...“
496	9.4.03	Tabelle 7.72	„Die Funktionalität von DEBIT nach EN 1546-3“	„Die Funktionalität von DEBIT IEP nach EN 1546-3“
508	9.4.03	Fußnote 3	„... ist im Abschnitt 14.7.3 „Prüfung auf ...“	„... ist im Abschnitt 15.9.3 „Prüfung auf ...“
519	9.4.03	2. Absatz	„Im Bild 8.9 ist beispielhaft ...“	„Im Bild 8.10 ist beispielhaft ...“
526	9.4.03	letzter Absatz	„Alle vier können gleichermaßen ...“	„Alle können gleichermaßen ...“
531	9.4.03	letzter Absatz	„... befindet sich dann beim Chiphersteller, ...“	„... befindet sich dann nicht beim Chiphersteller, ...“
532	9.4.03	Fußnote 8	„Siehe auch Abschnitt 13.6 „Digitale Signatur ...“	„Siehe auch Abschnitt 14.4 „Digitale Signatur ...“
535	9.4.03	Tabelle 8.6 (Fortsetzung), bei COMP 128	„... des von einigen Netzbetreibern verwendeten ...“	„... des von einigen GSM Netzbetreibern verwendeten ...“
535	9.4.03	Tabelle 8.6 (Fortsetzung), bei Störung des Prozessors	„Durch Störung des Prozessors (z. B. durch Lichtblitze) durch ...“	„Durch Störung des Prozessors durch ...“
566	9.4.03	3. Absatz	„... durch unberechtigt falsche Daten aus dem ...“	„... durch unberechtigt Daten aus dem ...“
592	9.4.03	1. Absatz	„Die Tabellen 9.4 und 9.5 zeigen die...“	„Die Tabellen 9.3 und 9.4 zeigen die...“
593	4.10.02	1. Absatz	„... bei den niedrigen Funktionalitätsklassen erheblich.“	„... bei den niedrigen Evaluationsstufen erheblich.“
596	9.4.03	2. Absatz	„... werden die Schritte Spezifikation, Codierung, Test, ...“	„... werden die Schritte Design, Realisierung, Test, ...“
600	9.4.03	2. Absatz	„Tabelle 9.6 zeigt dazu einen kurzen ...“	„Tabelle 9.5 zeigt dazu einen kurzen ...“
606	9.4.03	3. Absatz	„... ist in Bild 9.15 dargestellt.“	„... ist in Bild 9.17 dargestellt.“
627	9.4.03	letzter Absatz	„... in der Größe der Kontaktflächen und einer ...“	„... in der Größe der Kontaktfelder und einer ...“
644	9.4.03	2. Absatz	„... aus Abschnitt 14.2 (Formelsammlung zur ...“	„... aus Abschnitt 15.2 (Formelsammlung zur ...“
646	9.4.03	Bild 10.58	„... einer Chipkarte durch logische Kommandos wie ...“	„... einer Chipkarte durch Dateiverwaltungskommandos wie ...“
647	9.4.03	Bild 10.59, Zeichnung zu	...	Das Quadrat mit der Bezeichnung „Body“ muss diagonal in weiß sein.

656	9.4.03	letzter Absatz	„Im einfachsten Fall werden Daten in Dateien von bestimmten Chipkarten aktualisiert (RFM - remote file management).“	„Im einfachsten Fall werden Daten in Dateien von bestimmten Chipkarten aktualisiert. Die Verwaltung von Dateien über die Ferne bezeichnet man als remote file management (RFM)“
656	9.4.03	letzter Absatz	„... Chipkarten aktualisiert (RFM – remote file management).“	„... Chipkarten aktualisiert.“
662	23.4.03	vorletzte Zeile	„... mit dem Zusatz eines Displays. Die nächsthöhere Klasse 3 besitzt zusätzlich zu den Klasse-2-Elementen noch eine Tastatur.“	„... mit dem Zusatz einer Tastatur. Der Klasse 2 Leser benötigt keine eigene Tastaturreinheit er zwischen Kontaktierereinheit und PC eingeschleift ist. Die nächsthöhere Klasse 3 besitzt zusätzlich zu den Klasse-2-Elementen noch ein Display.“
663	23.4.03	Tabelle 11.1, bei Klasse 2	„Klasse 1 Funktionselemente + Display“	„Klasse 1 Funktionselemente + Tastatur“
663	23.4.03	Tabelle 11.1, bei Klasse 3	„Klasse 1 Funktionselemente + Tastatur“	„Klasse 1 Funktionselemente + Display“
674	9.4.03	3. Absatz	„... Industriestandards PC/SC SC (personal ...“	„... Industriestandards PC/SC (personal ...“
698	9.4.03	Tabelle 12.2	keine Tiefstellung bei: IKIEP, IKPSAM, IKPPSAM, MLDA, MPDA, MTOTIEP, MTOTPSAM, NTIEP, NTLSAM, NTPSAM, PPIEP, PPPSAM, PPPPSAM	IK _{IEP} , IK _{PSAM} , IK _{PPSAM} , M _{LDA} , M _{PD} , MTOT _{IEP} , MTOT _{PSAM} , NT _{IEP} , NT _{LSAM} , NT _{PSAM} , PP _{IEP} , PP _{PSAM} , PP _{PPSAM}
699	9.4.03	3. Absatz	„Tabelle 12.4 zeigt die Dateien ...“	„Tabelle 12.3 zeigt die Dateien ...“
700	9.4.03	3. Absatz	„Die drei Protokolldateien ...“	„Die Protokolldateien ...“
706	9.4.03	letzte Zeile	„... Transaktionszähler NT _{IEP} erhöht.“	„... Transaktionszähler NT _{PSAM} erhöht.“
718	9.4.03	2. Absatz	„... Version 2 lässt auch noch ...“	„... Version lässt auch noch ...“
735	9.4.03	Tabelle 13.1 (Fortsetzung)	„CDMA 2000“	„CDMA 2000“
744	9.4.03	letzter Absatz	„... erste GSM-Netzwerk in Großbritannien und das erste Roaming-Abkommen kam zustande.“	„... erste GSM-Netzwerk in Großbritannien.“
751	9.4.03	Tabelle 13.3, bei Besucherregister VLR	„Informationen über das Gerät des Teilnehmers Authentifizierungsdaten ...“	„Informationen über das Gerät des Teilnehmers <neue Zeile> Authentisierungsdaten ...“
758	9.4.03	Tabelle 13.5	„... für die Verwaltung von Anwendungen auf ...“	„... für die Verwaltung von Dateien auf ...“
761	17.9.03	erste Zeile	„... die meisten Anwendungsanbieter die Chipkarten ...“	„... die meisten Netzbetreiber die Chipkarten ...“
762	9.4.03	Tabelle 13.6 (Fortsetzung), bei DF _{GSM} .EF _{FPLMN}	„... siehe EF _{FPLMN} sel“	„... siehe EF _{FPLMN} sel“
762	17.9.03	Tabelle 13.6 (Fortsetzung), bei DF _{GSM} .EF _{FPLMN}	„'10' ⇒ MCC ...“	„'10' ⇒ MNC ...“
765	17.9.03	Tabelle 13.6 (Fortsetzung), bei DF _{GSM} .EF _{PUCT}	„'20' ⇒ MCC ...“	„'20' ⇒ MNC ...“
765	9.4.03	Tabelle 13.6 (Fortsetzung), bei DF _{GSM} .EF _{PUCT}	...	Text „Exponent-Teil EX.“ muß eine Zeile höher stehen
772	3.9.03	5. Zeile von unten	„... wurde, da er eine zu geringe Schlüssellänge hatte.“	„... wurde, da seine kryptografische Sicherheit nicht ausreichend genug war.“
772	31.1.03	3. Zeile von unten	„... Prinzip, da die zu kurze Schlüssellänge wohl für Kryptologen war.“	„... Prinzip, da das Problem mit diesem Algorithmus u.U. für einen größeren Kreis von Kryptologen erkennbar gewesen wäre.“
774	9.4.03	Bild 13.14	„... Station benutzt mittels des ...“	„... Station mittels des ...“

780	9.4.03	Tabelle 13.7 (Fortsetzung)	„Tabelle 13.7 (Fortsetzung)“	„Tabelle 13.8 (Fortsetzung)“
783	9.4.03	Bild 13.18	„Information der SIM über die ...“	„Informieren der SIM über die ...“
788	8.10.02	Bild 13.20	fehlende Verbindungslinien im Flussdiagramm	Die mit „Ja“ gekennzeichnete Abfrage muß mit „in SMS enthaltenes Kommando ausführen“ verbunden werden. Die mit „Nein“ gekennzeichnete Abfrage muß mit „Ende“ verbunden werden.
794	9.4.03	13.2.5 GPRS (General Paket Radio Service)	„13.2.5 GPRS (General Paket Radio Service)“	„13.2.5 GPRS (General Paket Radio System)“
794	9.4.03	1. Absatz	„GPRS (General Paket Radio Service) ist eine von ...“	„GPRS (General Paket Radio System ist eine von ...“
795	9.4.03	1. Absatz	„... ist ein Gateway Support Node GGSN, ...“	„... ist ein Gateway GPRS Support Node GGSN, ...“
797	9.4.03	letzte Zeile	„... wird gemäß IMTS-2000 der ...“	„... wird gemäß IMT-2000 der ...“
799	9.4.03	Tabelle 13.12	„... einer USIM basierend auf der UICC“	„... einer USIM die auf den Spezifikationen für UICC basiert.“
801	9.4.03	Tabelle 13.13	„Kategorie SIM Application Toolkit“	„Kategorie USIM Application Toolkit“
801	9.4.03	Tabelle 13.14, bei MF.EF _{DIR}	„Erweiterung für bevorzugte Sprache (ELP – extended language preference)“	„Anwendungsverzeichnis (DIR – directory)“
802	9.4.03	Tabelle 13.15, bei ADF _{USIM}	„RID = RID = 'A0 00 00 00 87'“	„AID = RID = 'A0 00 00 00 87'“
803	9.4.03	Tabelle 13.15 (Fortsetzung), bei ADF _{USIM} .EF _{KeysPS}	„... für Integritätsprüfung IK (integrity key ...“	„... für Integritätsprüfung IKPS (integrity key ...“
804	9.4.03	Tabelle 13.15 (Fortsetzung), bei ADF _{USIM} .EF _{ECC}	„Verwaltungsdaten (AD – administrative data)“	„Notrufnummern (ECC – emergency call codes)“
806	9.4.03	Absatz nach Bild 13.26	„... auch ohne Abstriche an Sicherheit eine Ende-zu-Ende-Sicherheit auf Anwendungsebene ...“	„... auch ohne Abstriche eine sichere Ende-zu-Ende-Verbindung auf Anwendungsebene ...“
806	9.4.03	Tabelle 14.16	„Tabelle 14.16“	„Tabelle 13.16“
812	9.4.03	Tabelle 13.21	„... Dateien einer WIM19“	„... Dateien einer WIM ¹⁹ “
812	9.4.03	Tabelle 13.21, bei EF _{TokenInfo}	...	EF _{TokenInfo} Allgemeine Informationen Diese Datei enthält eine Reihe grundlegender Informationen über die WIM und die von ihr unterstützten Funktionen.
812	9.4.03	Tabelle 13.21, bei EF _{CDF_1}	„... auf diese Schlüssel ...“	„... auf diese Zertifikate ...“
817	9.4.03	1. Absatz	„... gemessen in Pfennigen aufweist.“	„... gemessen in Eurocent aufweist.“
834	9.4.03	vorletzte Zeile	„... und Protocol Type Selection (PTS)“	„... und Protocol Parameter Selection (PPS)“
840	9.4.03	Tabelle 14.4	mehrmalige fehlende Tiefstellung des „G“ bei „DF _{SigG} “	„DF _{SigG} “
843	17.9.03	erste Zeile des letzter Absatz	„Die Verzeichnisdateien EF _{PrKDF} , EF _{PrKDF} , ...“	„Die Verzeichnisdateien EF _{PrKDF} , EF _{PuKDF} , ...“
845	17.8.03	EF _{TokenInfo}	falscher Beschreibungstext zu EF _{TokenInfo}	EF _{TokenInfo} Allgemeine Informationen Diese Datei enthält eine Reihe grundlegender Informationen über die Anwendung und die von ihr unterstützten Funktionen.
877	9.4.03	letzte Zeile	„... Inhalt EF _{DIR} “	„... Inhalt EF _{DIR} “

906 - 955	9.4.03	diverse Stellen	„siehe auch“	„→“
914	9.4.03	CDMA 2000	„CDMA 2000“	„CDMA 2000“
920	9.4.03	bei enrollment	„... eines → Chipkartenbenutzers und die ...“	„... eines → Kartenbesitzers und die ...“
920	9.4.03	bei Evaluierung	„... und Common Criteria (→ CC).“	„... und → Common Criteria (CC).“
925	9.4.03	bei Hotlist	„... (→ Sperrliste, Redlist, Greylist ...“	„... (→ Sperrliste, Greylist ...“
928	9.4.03	bei Kernspannung	„Niedrige Kernspannungen sind wegen der notwendigen Spannungsfestigkeit bei zunehmend geringeren Strukturbreiten und zur Reduktion der chipinternen Kapazitäten bei den immer höher werdenden Taktfrequenzen notwendig.“	„Niedrige Kernspannungen sind notwendig um die geringere Spannungsfestigkeit des Halbleiters bei kleinen Strukturbreiten zu kompensieren und um die Lade- und Entladeströme der chipinternen Kapazitäten zu reduzieren.“
928	10.4.03	bei Karte	„... einen Halbleiterchip (→ Chipkarte) besitzen. Der englische Begriff card hat im WMLUmfeld eine völlig andere Bedeutung (→ Card).“	„... einen Halbleiterchip (→ Chipkarte) besitzen.“
932	9.4.03	bei MF	„MF“	„MF (master file)“
937	9.4.03	bei Personalisierung	„... bei anonymen (→ vorbezahlten SIMs.“	„... bei anonymen (→ prepaid SIMs.“
937	9.4.03	bei Plug-In	„... Breite von ≈ 25 mm, eine Höhe von ≈ 15 mm und eine Dicke $\approx 0,76$ mm ...“	„... Breite von ≈ 25 mm, eine Höhe von ≈ 15 mm und eine Dicke $\approx 0,76$ mm ...“
937	9.4.03	bei polling	„... mittels Interrupt bevorzugt.“	„... mittels Interrupt bevorzugt. Polling wird beispielsweise bei Mobiltelefonen im Rahmen des → SIM Application Toolkit benutzt damit die → SIM proaktive Kommandos (→ Proaktivität) an das Mobiltelefon senden kann.“
939	9.4.03	bei PSTN	„PSTN (public switched mobile network)“	„PSTN (public switched telephone network)“
941	9.4.03	bei Round-trip Engineering	„... des Software-Entwicklungsprozesses sequentiell an Design und ...“	„... des Software-Entwicklungsprozesses parallel an Design und ...“
941	9.4.03	bei R-UIM	„... für die GSM-spezifische Chipkarte.“	„... für die CDMA-spezifische Chipkarte.“
946	9.4.03	bei Softmaske	„Softmasken werden üblicherweise nicht für große Stückzahlen (z. B. für Feldversuche) bei → rapid prototyping oder für Erweiterungen verwendet.“	„Typischerweise werden Softmasken für Feldversuche eingesetzt.“
950	9.4.03	bei IM	„IM (user identity module)“	„UIM (user identity module)“
951	9.4.03	Fußnote 64	„Siehe auch Abschnitt 13.2 „Das GSM-System“.“	„Siehe auch Abschnitt 13.3 „Das UMTS-System“.“
953	9.4.03	bei Whitelist	„... dürfen (→ Sperrliste, White List).“	„... dürfen (→ Sperrliste, Hotlist, Greylist).“
971	9.4.03	bei [Boneh 96]	...	Eintrag ersatzlos streichen.
977	9.4.03	bei Java Card Forum	...	[JCF] in Spalte Web-Server ergänzen
982	9.4.03	bei prEN 13 344	...	Referenz auf Norm ersatzlos streichen.
982	9.4.03	bei prEN 13 345	...	Referenz auf Norm ersatzlos streichen.
988	9.4.03	bei –3 : 1997	„... von ATR und PTS definiert.“	„... von ATR und PPS definiert.“

989	9.4.03	ISO 8583	...	Referenz auf Norm ersatzlos streichen.
993	9.4.03	ISO/IEC 10 373-3	„... bei ATR, PTS und den ...“	„... bei ATR, PPS und den ...“
993	9.4.03	ISO/IEC 10 536-4	„... von ATR und PTS für ...“	„... von ATR und PPS für ...“
996	9.4.03	vor PKCS	...	Eintrag zu PC/SC von Seite 982 einfügen.
1001	9.4.03	TS 102.241	„TS 102.241“	„TS 123.002“
1003	8.10.02	Tabelle 16.3	Datenelement „Geburtsdatum“ doppelt vorhanden	ein Datenelement „Geburtsdatum“ ersatzlos streichen
1007	12.9.02	bei „[a la Card]“	der gesamte Eintrag ist ersatzlos zu streichen	...
1008	10.9.02	bei „[AC]“	„Austria Card, Deutschland“	„Austria Card, Österreich“
1010	8.1.03	bei „[ETSI]“	„http://www.etsi.fr“	„http://www.etsi.org“
1014	10.9.02	bei „[OCF]“	„www.opencard.com“	„www.opencard.org“
1019	30.1.03	Tabelle 16.10	Die Tabelle ist unvollständig	siehe Anhang 1
1020	8.1.03	Tabelle 16.11	Einige Tabelleneinträge sind fehlerhaft.	siehe Anhang 2
1020	9.4.03	Tabelle 16.12	Einige Tabelleneinträge sind fehlerhaft.	siehe Anhang 3
1023	9.4.03	Tabelle 16.14 (Fortsetzung), 2. Eintrag zu DEACTIVATE FILE	„DEACTIVATE FILE“	„REACTIVATE FILE“
1030	9.4.03	zung)	„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.“	„P2.b3 . . . P2.b1 = °101° Lese ab den in P1 referenzierten Record vorwärts alle Records bis zum letzten Record. P2.b3 . . . P2.b1 = °110° Lese vom letzten Record rückwärts alle Records bis zu dem in P1 referenzierten Record.“

Anhang 1 – CWI/CWT-Tabelle mit D=1 und Takt = 3,5712 MHz (Ersatz von Tabelle 16.10)

		CWT						
F		4	8	16	31	93	186	372
CWI	work etu	1,120 µs	2,240 µs	4,480 µs	8,681 µs	26,042 µs	52,083 µs	104,167 µs
	0	0,013 ms	0,027 ms	0,054 ms	0,104 ms	0,313 ms	0,625 ms	1,250 ms
	1	0,015 ms	0,029 ms	0,058 ms	0,113 ms	0,339 ms	0,677 ms	1,354 ms
	2	0,017 ms	0,034 ms	0,067 ms	0,130 ms	0,391 ms	0,781 ms	1,563 ms
	3	0,021 ms	0,043 ms	0,085 ms	0,165 ms	0,495 ms	0,990 ms	1,979 ms
	4	0,030 ms	0,060 ms	0,121 ms	0,234 ms	0,703 ms	1,406 ms	2,813 ms
	5	0,048 ms	0,096 ms	0,193 ms	0,373 ms	1,120 ms	2,240 ms	4,479 ms
	6	0,084 ms	0,168 ms	0,336 ms	0,651 ms	1,953 ms	3,906 ms	7,813 ms
	7	0,156 ms	0,311 ms	0,623 ms	1,207 ms	3,620 ms	7,240 ms	14,479 ms
	8	0,299 ms	0,598 ms	1,196 ms	2,318 ms	6,953 ms	13,906 ms	27,813 ms
	9	0,586 ms	1,172 ms	2,343 ms	4,540 ms	13,620 ms	27,240 ms	54,479 ms
	10	1,159 ms	2,319 ms	4,637 ms	8,984 ms	26,953 ms	53,906 ms	107,813 ms
	11	2,306 ms	4,612 ms	9,225 ms	17,873 ms	53,620 ms	107,240 ms	214,479 ms
	12	4,600 ms	9,200 ms	18,401 ms	35,651 ms	106,953 ms	213,906 ms	427,813 ms
	13	9,188 ms	18,376 ms	36,752 ms	71,207 ms	213,620 ms	427,240 ms	854,479 ms
	14	18,364 ms	36,727 ms	73,454 ms	142,318 ms	426,953 ms	853,906 ms	1 707,813 ms
15	36,715 ms	73,430 ms	146,859 ms	284,540 ms	853,620 ms	1 707,240 ms	3 414,479 ms	
	0	12 etu	12 etu	12 etu				
	1	13 etu	13 etu	13 etu				
	2	15 etu	15 etu	15 etu				
	3	19 etu	19 etu	19 etu				
	4	27 etu	27 etu	27 etu				
	5	43 etu	43 etu	43 etu				
	6	75 etu	75 etu	75 etu				
	7	139 etu	139 etu	139 etu				
	8	267 etu	267 etu	267 etu				
	9	523 etu	523 etu	523 etu				
	10	1 035 etu	1 035 etu	1 035 etu				
	11	2 059 etu	2 059 etu	2 059 etu				
	12	4 107 etu	4 107 etu	4 107 etu				
	13	8 203 etu	8 203 etu	8 203 etu				
	14	16 395 etu	16 395 etu	16 395 etu				
	15	32 779 etu	32 779 etu	32 779 etu				

Anhang 2 – BWI-BWT-Tabelle mit D=1 und Takt = 3,5712 MHz (Ersatz von Tabelle 16.11)

		BWT						
F		4	8	16	31	93	186	372
BWI	work	1,120 µs	2,240 µs	4,480 µs	8,681 µs	26,042 µs	52,083 µs	104,167 µs
	etu							
	0	100 ms	100 ms	100 ms	100 ms	100 ms	100 ms	100 ms
	1	200 ms	200 ms	200 ms	200 ms	200 ms	200 ms	200 ms
	2	400 ms	400 ms	400 ms	400 ms	400 ms	400 ms	400 ms
	3	800 ms	800 ms	800 ms	800 ms	800 ms	800 ms	800 ms
	4	1 600 ms	1 600 ms	1 600 ms	1 600 ms	1 600 ms	1 600 ms	1 600 ms
	5	3 200 ms	3 200 ms	3 200 ms	3 200 ms	3 200 ms	3 200 ms	3 200 ms
	6	6 400 ms	6 400 ms	6 400 ms	6 400 ms	6 400 ms	6 400 ms	6 400 ms
	7	12 800 ms	12 800 ms	12 800 ms	12 800 ms	12 800 ms	12 800 ms	12 800 ms
	8	25 600 ms	25 600 ms	25 600 ms	25 600 ms	25 600 ms	25 600 ms	25 600 ms
	9	51 200 ms	51 200 ms	51 200 ms	51 200 ms	51 200 ms	51 200 ms	51 200 ms
	0	89 291 etu	44 651 etu	22 331 etu	11 531 etu	3 851 etu	1 931 etu	971 etu
	1	178 645 etu	89 323 etu	44 661 etu	23 051 etu	7 684 etu	3 842 etu	1 921 etu
	2	357 131 etu	178 571 etu	89 291 etu	46 091 etu	15 371 etu	7 691 etu	3 851 etu
	3	714 251 etu	357 131 etu	178 571 etu	92 171 etu	30 731 etu	15 371 etu	7 691 etu
	4	1 428 491 etu	714 251 etu	357 131 etu	184 331 etu	61 451 etu	30 731 etu	15 371 etu
	5	2 856 971 etu	1 428 491 etu	714 251 etu	368 651 etu	122 891 etu	61 451 etu	30 731 etu
	6	5 714 005 etu	2 857 003 etu	1 428 501 etu	737 291 etu	245 764 etu	122 882 etu	61 441 etu
	7	11 427 925 etu	5 713 963 etu	2 856 981 etu	1 474 571 etu	491 524 etu	245 762 etu	122 881 etu
8	22 855 765 etu	11 427 883 etu	5 713 941 etu	2 949 131 etu	983 044 etu	491 522 etu	245 761 etu	
9	45 711 445 etu	22 855 723 etu	11 427 861 etu	5 898 251 etu	1 966 084 etu	983 042 etu	491 521 etu	

Anhang 3 – Übertragungsgeschwindigkeiten (Ersatz von Tabelle 16.12)

		clock rate conversion factor F							
		bit rate adjustment factor D							
		372							
		1	2	4	8	12	16	20	32
F/D		372,00	186,00	93,00	46,50	31,00	23,25	18,60	11,63
frequency f	1,0000 MHz	2 688 bit/s	5 376 bit/s	10 753 bit/s	21 505 bit/s	32 258 bit/s	43 011 bit/s	53 763 bit/s	86 022 bit/s
	2,0000 MHz	5 376 bit/s	10 753 bit/s	21 505 bit/s	43 011 bit/s	64 516 bit/s	86 022 bit/s	107 527 bit/s	172 043 bit/s
	3,0000 MHz	8 065 bit/s	16 129 bit/s	32 258 bit/s	64 516 bit/s	96 774 bit/s	129 032 bit/s	161 290 bit/s	258 065 bit/s
	3,5712 MHz	9 600 bit/s	19 200 bit/s	38 400 bit/s	76 800 bit/s	115 200 bit/s	153 600 bit/s	192 000 bit/s	307 200 bit/s
	4,0000 MHz	10 753 bit/s	21 505 bit/s	43 011 bit/s	86 022 bit/s	129 032 bit/s	172 043 bit/s	215 054 bit/s	344 086 bit/s
	5,0000 MHz	13 441 bit/s	26 882 bit/s	53 763 bit/s	107 527 bit/s	161 290 bit/s	215 054 bit/s	268 817 bit/s	430 108 bit/s
	6,0000 MHz	16 129 bit/s	32 258 bit/s	64 516 bit/s	129 032 bit/s	193 548 bit/s	258 065 bit/s	322 581 bit/s	516 129 bit/s
	7,0000 MHz	18 817 bit/s	37 634 bit/s	75 269 bit/s	150 538 bit/s	225 806 bit/s	301 075 bit/s	376 344 bit/s	602 151 bit/s
	8,0000 MHz	21 505 bit/s	43 011 bit/s	86 022 bit/s	172 043 bit/s	258 065 bit/s	344 086 bit/s	430 108 bit/s	688 172 bit/s
	9,0000 MHz	24 194 bit/s	48 387 bit/s	96 774 bit/s	193 548 bit/s	290 323 bit/s	387 097 bit/s	483 871 bit/s	774 194 bit/s
10,0000 MHz	26 882 bit/s	53 763 bit/s	107 527 bit/s	215 054 bit/s	322 581 bit/s	430 108 bit/s	537 634 bit/s	860 215 bit/s	

		clock rate conversion factor F							
		bit rate adjustment factor D							
		512							
		1	2	4	8	12	16	20	32
F/D		512,00	256,00	128,00	64,00	42,67	32,00	25,60	16,00
frequency f	1,0000 MHz	1 953 bit/s	3 906 bit/s	7 813 bit/s	15 625 bit/s	23 438 bit/s	31 250 bit/s	39 063 bit/s	62 500 bit/s
	2,0000 MHz	3 906 bit/s	7 813 bit/s	15 625 bit/s	31 250 bit/s	46 875 bit/s	62 500 bit/s	78 125 bit/s	125 000 bit/s
	3,0000 MHz	5 859 bit/s	11 719 bit/s	23 438 bit/s	46 875 bit/s	70 313 bit/s	93 750 bit/s	117 188 bit/s	187 500 bit/s
	3,5712 MHz	6 975 bit/s	13 950 bit/s	27 900 bit/s	55 800 bit/s	83 700 bit/s	111 600 bit/s	139 500 bit/s	223 200 bit/s
	4,0000 MHz	7 813 bit/s	15 625 bit/s	31 250 bit/s	62 500 bit/s	93 750 bit/s	125 000 bit/s	156 250 bit/s	250 000 bit/s
	5,0000 MHz	9 766 bit/s	19 531 bit/s	39 063 bit/s	78 125 bit/s	117 188 bit/s	156 250 bit/s	195 313 bit/s	312 500 bit/s
	6,0000 MHz	11 719 bit/s	23 438 bit/s	46 875 bit/s	93 750 bit/s	140 625 bit/s	187 500 bit/s	234 375 bit/s	375 000 bit/s
	7,0000 MHz	13 672 bit/s	27 344 bit/s	54 688 bit/s	109 375 bit/s	164 063 bit/s	218 750 bit/s	273 438 bit/s	437 500 bit/s
	8,0000 MHz	15 625 bit/s	31 250 bit/s	62 500 bit/s	125 000 bit/s	187 500 bit/s	250 000 bit/s	312 500 bit/s	500 000 bit/s
	9,0000 MHz	17 578 bit/s	35 156 bit/s	70 313 bit/s	140 625 bit/s	210 938 bit/s	281 250 bit/s	351 563 bit/s	562 500 bit/s
10,0000 MHz	19 531 bit/s	39 063 bit/s	78 125 bit/s	156 250 bit/s	234 375 bit/s	312 500 bit/s	390 625 bit/s	625 000 bit/s	

Anhang 4 – Übertragungsgeschwindigkeiten (Ersatz von Bild 3.108)

