

**Errata Liste für das
Handbuch der Chipkarten
von
Wolfgang Rankl und Wolfgang Effing**

Source:	Wolfgang Rankl	
File:	Errata Liste V 17x.doc (*.pdf)	No. of Pages: 5
State:	draft final	Print Date, Time: 29. Mai 2001, 11:24
Remarks:	Handbuch der Chipkarten 3. deutsche Auflage 1999, Erstdruck Carl Hanser Verlag, München ISBN 3-446-21115-2 • Dokument im Word 97 Format • e-Mail für Korrekturhinweise: WRankl@gmx.net	
Ausgaben:	1.7.3 28. Mai 2001	div. Fehler verbessert, erkannt durch Zuschriften von Lesern (DANKE!)
	1.7.2 1. Feb 2001	div. Fehler verbessert, erkannt durch Zuschriften von Lesern (DANKE!)
	1.6.912. April 2000	div. Fehler, erkannt durch die Übersetzung ins englische
	1.5.3 19. Jan. 2000	div. Fehler, erkannt durch die Übersetzung ins englische und e-Mails
	1.4.5 29./XII/1999	div. Fehler, erkannt durch die Übersetzung ins englische
	1.3.0 24.08.1999	Kapitel 6: TC1 -Fehler ergänzt, auf Word 97 umgestellt
	1.1.1 5.8.1999	---
	1.0.0 23.7.1999	erste Version

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

Wolfgang Rankl

Wolfgang Effing

Seite	Position auf der Seite	falsch	richtig
diverse	Bildunterschriften	Giesecke und Devrient	Giesecke & Devrient
7	7te Zeile von unten	„... die Referenz erkennen).“	„... die Reverenz erkennen).“
17	vorletzte Zeile	„verify ...“	„R := verify ...“
18	vor der 4ten Zeile von unten; zwischen „SE-ARCH“ und „LENGTH“ eine Zeile ergänzen	---	„STATUS (...) Abfrage des Ausführungsergebnisses bei einem vorangegangenen Funktionsaufruf“
154	3ter Abschnitt von unten	„... (= 2 • 8 Bit) ...“	„... (= 2 • 8 Byte) ...“
157	4te Zeile von oben	„... Der DES ist aber eine Gruppe, ...“	„... Der DES ist aber keine Gruppe, ...“
169	3ter Abschnitt von oben	„... Daten geradzahlig durch die Blocklänge ...“	„... Daten ganzzahlig durch die Blocklänge ...“

185	2ter Abschnitt von unten	„... Komprimierung korrespondiert nach Shannon direkt mit der ...“	„...Komprimierung ist nach Shannon umgekehrt proportional mit der ...“
198	8te Zeile von unten	„... RSA-Algorithmus entschlüsselt und mit ...“	„... RSA-Algorithmus verschlüsselt und mit ...“
205	Tabellenüberschrift 5.1	„... Dies Liste ...“	„... Diese Liste ...“
211	2ter Abschnitt von unten	„... sind in den Tabellen 5.2 und 5.3 im Überblick ...“	„... ist in der Tabelle 5.2 im Überblick ...“
221	2ter Abschnitt von unten	„... ist in Bild 5.6 nochmals ...“	„... ist in Bild 5.7 nochmals ...“
226	1ter Abschnitt von unten	„... zu den EFs existieren für Anwendungen noch interne ...“	„... zu den EFs für Anwendungen existieren noch interne ...“
229	Tabelle 5.5	„... die Datei EFKey_MAN wird ...“	„... die Datei EFKey_OP wird...“
239	2ter Abschnitt von oben	„... werden in kommandoorientierten Betriebssystemen die vor ...“	„... werden bei kommandoorientierten Zugriffsbedingungen die vor ...“
239	3ter Abschnitt von unten	„... die drei wichtigsten Zugriffsbedingungen im ...“	„... die drei wichtigsten Zugriffskommandos ...“
253	Bild 5.22	Zeichnung „DF Header“ ist unvollständig	Zeichnung „DF Header“ durch einen Zeiger auf DF Hedaer n+1 direkt vor dem EDC ergänzen
253	Bild 5.22	Zeichnung „DF Header“ ist unvollständig	Zeichnung „DF Header“ durch einen Zeiger auf DF Hedaer n+1 direkt vor dem EDC ergänzen
258	1ter Abschnitt von unten	„... daß das EF zuerst muß und ...“	„... daß das EF zuerst selektiert werden muß und ...“
272	letzte Zeile	„... dazugehörigen Verschlüsselungsmethoden enthält.“	„... dazugehörigen Entschlüsselungsmethoden enthält.“
281 ff	Programmtabellen im Abschnitt 5.11	an diversen Stellen den Unterstrich bei Programmzeilen die größer sind als eine Zeile vergessen	Unterstrich an den entsprechenden Stellen ergänzen
281 ff	Programmtabellen im Abschnitt 5.11	„Status“ ist ein Funktionsaufruf und muß deshalb in Großbuchstaben geschrieben sein	ersetze im Programmcode durchgehend „Status“ durch „STATUS“
318	Tabelle 5.63	„... Fall ein Schlüssel PIN mit der angegebenen Referenznummer gefunden wurde, dann ...“	„... Fall ein Schlüssel mit der angegebenen Referenznummer gefunden wurde, dann ...“
320	Tabelle 5.64, Bei Read und Update	„... Der notwendige Zustand der Zugriffsbedingung, damit das Kommando ...“	„... Der notwendige Zustand, damit das Kommando ...“
335	dritte Textzeile	Referenz auf 15.4.2 ist falsch	Referenz muß 15.8.2 sein

336	ab der fünften Zeile nach Global Interface Character TC1	„... zwei etu beträgt ... gesendet werden muß.“	... zwei etu beträgt, bei T=1 auf 11 etu verkürzt werden muß. Bei T=0 bleibt die zusätzliche Schutzzeit auf N=12 etu, um die Fehlersignalisierung durch einen low-Pegel innerhalb der Schutzzeit zu ermöglichen. In der Praxis bedeutet eine bei T=1 auf 11 etu reduzierte Schutzzeit eine Geschwindigkeitssteigerung um ca. 10 %, da ein Bit weniger gesendet werden muß.
336	Tabelle 6.9	eine Zeile ergänzen	X=255 und T=0: N=12 etu X=255 und T=1: N=11 etu
337	dritte Zeile nach Tabelle 6.11	„Datenelemente - wie ... ergeben würde.“	ersatzlos streichen, daß mißverständlich
337	beide Fußzeilen	...	“siehe auch Abschnitt 6.4.3 Übertragungsprotokoll T=1”
338	Formel, erste Zeile	„... $372/(f*s) + \dots$ “	„... $(372/f)*s + \dots$ “
366	5te Zeile von oben	“... zu kurz ist ...”	“... zu lang ist ...”
371	Bild 6.42	Class-Byte fehlt im allen APDU-Feldern	Class-Byte '00' in allen 3 Kommando-APDU Feldern ergänzen.
371	Bild 6.42	alle EDC-Bytes sind falsch	Kommando 1: EDC='9E' Antwort 1: EDC='92' Kommando 2: EDC='DE' Antwort 2: EDC='D2' Kommando 3: EDC='9E' Antwort 3: EDC='92'
378	Fußnote Nr. 1	---	ersatzlos streichen (da rekursiv)
379	5te Zeile im 3ten Absatz	“... Escape-Sequenz 'FF' codiert ...”	“... Escape-Sequenz '00' codiert ...”
379	Bild 6.47	Text in Bild ist falsch	Byte 1 muß statt den Wert 'FF' den '00' haben
426	Bild 7.17	“S' := verify (...) IF (S=S') THEN ...”	“H' := encrypt (...) H := Hash-Wert der Daten IF (H=H') THEN ...”
439	erste Zeile von oben	“... on “for load”. Die Chipkarte ...”	“... on “for purchase”. Die Chipkarte ...”
462	letzter Absatz	„FAR ist die ... und FRR die Wahrscheinlichkeit für ...“	„FRR ist die ... und FAR die Wahrscheinlichkeit für ...“
471	Bildunterschrift Bild 8.15	„Klassifizierungsbaum für mögliche Angriffe auf Chipkarten.“	„Klassifizierungsbaum zur Einstufung von Angriffen auf Chipkarten.“

472	Bildunterschrift Bild 8.17	„Klassifizierungsbaum für mögliche Angriffe auf Chipkarten.“	„Klassifizierungsbaum der Typen von Angriffen auf Chipkarten.“
500	Bild 8.34	...	ersetzte im Bild Befehls-APDU durch Kommando-APDU
512	vierte Textzeile	Referenz auf 4.4 ist falsch	Referenz muß 4.9 sein
535	erster Absatz	Referenz auf 9.5 ist falsch	Referenz muß 9.3 und 9.4 sein
547	vorletzte Zeile	„Paritätsfehlern, Zeichenwiederholung, falls T=0 vorhanden, Struktur ...“	„Paritätsfehlern, falls T=0 vorhanden dann Zeichenwiederholung, Struktur ...“
554	Tabelle 10.2, Phase 1	„ID der Fertigung“	„ID der Fertigungslinie“
554	Tabelle 10.2, Phase 2	„ID der Fertigung“	„ID der Fertigungsmaschine“
554	Tabelle 10.2, Phase 3	„ID der Fertigung“	„ID der Fertigungsmaschine“
609	Tabelle 12.1	Tabellennumerierung 12.1 ist falsch	Tabellennumer muß 11.1 sein
629	Fußnote	„Ein mögliches Schlüsselmanagement ... erläutert.“	„Siehe auch Abschnitt 4.6 Kryptologie“
635	fünfte Zeile	„... von Debitkarten mit ...“	„... von vorbezahlten elektronischen Geldbörsen mit ...“
663	vorletzte Zeile	„... eine Debitkarte, die vom ...“	„... eine elektronische Geldbörsen, die vom ...“
669	Fußzeile	„... Abschnitt 3.1.3 Kontaktlose Karte“	„... Abschnitt 3.6 Kontaktlose Karte“
696	Tabelle 13.3	Tabellenüberschrift ist falsch	„Tabelle 13.3 Gegenüberstellung der wesentlichen Unterschiede zwischen der ITSEC Prüfstufe E2 und E4.“
714	Tabelle 14.3	Variablenbeschreibung $t_{\text{Kommandoabarbeitung}}$ ist ungenau	„ $t_{\text{Kommandoabarbeitung}}$ = Zeitdauer für die Abarbeitung eines Kommandos.“
714	Tabelle 14.3	Variablenbeschreibung $t_{\text{Kommandocode}}$ ist ungenau	„ $t_{\text{Kommandocode}}$ = Zeitdauer für die Abarbeitung eines speziellen Programmteils (z.B. Kryptoalgorithmus) für ein Kommando.“
716	fünfte Textzeile	Referenz auf 6.2.2 ist falsch	Referenz muß 6.4.2 sein
716	sechste Textzeile	Referenz auf 6.2.3 ist falsch	Referenz muß 6.4.3 sein
724	letzte Textzeile	„... der Größe problematisch ...“	„... der Größe dieses Simulationsaufbaus problematisch ...“
727	erste Textzeile unter 14.7	„... werden zwei typische ...“	„... werden drei typische ...“
737	Tabellenunterschrift von 14.10	„... Kommandos während der Zugangskontrolle für die Prüfung ...“	„... Kommandos bei der Prüfung ...“

751	Definition „Ladebeauftragter“	„... zum Leistungsanbieter, der die ... wieder aufladen kann.“	„... zum Leistungsanbieter.“
758	Definition „Signaturgesetz“	„... von digitalen Signaturen für den Einsatz in Deutschland vorgegeben.“	„... von digitalen Signaturen in Deutschland vorgegeben.“
760	Definition „Stack“	„... Objekte als letzte wieder entfernt ...“	„... Objekte als erste wieder entfernt ...“
761	Definition „UIM“	„Veralteter Begriff für UIM ...“	„Veralteter Begriff für USIM ...“
762	Definition „USIM“	„Das SIM ist der Träger ...“	„Das USIM ist der Träger ...“
804	ab der 4ten Zeile von oben	fehlender Text	„Die Adressen der nationalen Registrierungsinstanz sowie die entsprechenden Registrierungsverfahren für RIDs können in der Regel bei der jeweiligen nationalen Normungsinstanz erfragt werden.“
805	Tabelle 15.4, dreizehnte Zeile von unten	Erklärung zu „Kartenherausgeber“ fehlt	„Kartenherausgeber Herausgeber von Karten und/oder Chipkarten“
826	Tabelle 15.21	„... P2.b3 ... P2.b1 = °010° ...“	„... P2.b3 ... P2.b1 = °011° ...“
826	Tabelle 15.22	„... P2.b3 ... P2.b1 = °010° ...“	„... P2.b3 ... P2.b1 = °011° ...“
828	zweite Zeile	„... beschriebenen Kommandos sind ...“	„... beschriebenen Returncodes sind ...“