

Inhaltsverzeichnis für das Handbuch der Chipkarten

von Wolfgang Rankl und Wolfgang Effing
3. Auflage, deutsch

Source:	Wolfgang Rankl		
File:	HdC_Inht.doc/ps/pdf	No. of Pages:	5
Date:	9. Februar 1999	Print Date, Time:	18. February 1999, 17:11
Version:	1.2-19	State:	final
Remarks:	---		

Vorwort von Jürgen Dethloff zur dritten Auflage
Vorwort der Autoren zur dritten Auflage
Inhalt im Überblick
Inhaltsverzeichnis
Symbole/Notationen
Programmcode
Abkürzungen

1 Einleitung

- 1.1 Geschichte der Chipkarten
- 1.2 Anwendungsgebiete
 - 1.2.1 Speicherkarten
 - 1.2.2 Mikroprozessorkarten
 - 1.2.3 Kontaktlose Karten
- 1.3 Normung

2 Arten von Karten

- 2.1 Hochgeprägte Karten
- 2.2 Magnetstreifenkarten
- 2.3 Chipkarten
 - 2.3.1 Speicherkarten
 - 2.3.2 Mikroprozessorkarten
 - 2.3.3 Kontaktlose Chipkarten
- 2.4 Optische Speicherkarten

3 Physikalische und elektrische Eigenschaften

- 3.1 Physikalische Eigenschaften
 - 3.1.1 Formate
 - 3.1.2 Kartenelemente und Sicherheitsmerkmale
- 3.2 Kartenkörper
 - 3.2.1 Kartenmaterialien
 - 3.2.2 Chipmodule
 - 3.2.2.1 Elektrische Kontaktierung zwischen Chip und Modul
 - 3.2.2.2 TAB-Modul
 - 3.2.2.3 Chip-on-Flex-Modul
 - 3.2.2.4 Lead-Frame-Modul
 - 3.2.2.5 Chip-On-Surface-Verfahren

- 3.3 Elektrische Eigenschaften
 - 3.3.1 Beschaltung
 - 3.3.2 Versorgungsspannung
 - 3.3.3 Versorgungsstrom
 - 3.3.4 Taktversorgung
 - 3.3.5 Datenübertragung
 - 3.3.6 An-/Abschaltsequenz
- 3.4 Mikrocontroller für Chipkarten
 - 3.4.1 Prozessortypen
 - 3.4.2 Speicherarten
 - 3.4.3 Zusatzhardware
- 3.5 Kontaktbehaftete Karten
- 3.6 Kontaktlose Karten
 - 3.6.1 ISO/IEC 10536 – Close Coupling Cards
 - 3.6.2 Remote Coupling Karten
 - 3.6.3 Proximity Integrated Circuit(s) Cards nach ISO/IEC 14443
 - 3.6.4 Hands Free Integrated Circuit(s) Cards nach ISO/IEC 15693

4 Informationstechnische Grundlagen

- 4.1 Strukturierung von Daten
- 4.2 SDL-Symbolik
- 4.3 Zustandsautomaten
 - 4.3.1 Grundlagen zur Automatentheorie
 - 4.3.2 Praktische Anwendung
- 4.4 Fehlererkennungs- und Fehlerkorrekturcodes
 - 4.4.1 XOR-Prüfsummen
 - 4.4.2 CRC-Prüfsummen
 - 4.4.3 Fehlerkorrektur
- 4.5 Datenkompression
- 4.6 Kryptologie
 - 4.6.1 Symmetrische Kryptoalgorithmen
 - 4.6.2 Asymmetrische Kryptoalgorithmen
 - 4.6.3 Padding
 - 4.6.4 Message Authentication Code / Cryptographic Checksum
- 4.7 Schlüsselmanagement
 - 4.7.1 Abgeleitete Schlüssel
 - 4.7.2 Schlüsseldiversifizierung
 - 4.7.3 Schlüsselversionen
 - 4.7.4 Dynamische Schlüssel
 - 4.7.5 Schlüsselinformationen
 - 4.7.6 Beispiel für Schlüsselmanagement
- 4.8 Hash-Funktionen
- 4.9 Zufallszahlen
 - 4.9.1 Erzeugung von Zufallszahlen
 - 4.9.2 Prüfung von Zufallszahlen
- 4.10 Authentisierung
 - 4.10.1 Einseitige symmetrische Authentisierung
 - 4.10.2 Gegenseitige symmetrische Authentisierung
 - 4.10.3 Statische asymmetrische Authentisierung
 - 4.10.4 Dynamische asymmetrische Authentisierung
- 4.11 Digitale Signatur
- 4.12 Zertifikate

5 Chipkarten-Betriebssysteme

- 5.1 Bisherige Entwicklung der Betriebssysteme
- 5.2 Grundlagen
- 5.3 Entwurfs- und Implementierungsprinzipien
- 5.4 Aufteilung des Programmcodes
- 5.5 Speicherorganisation
- 5.6 Dateien in der Chipkarte
 - 5.6.1 Dateitypen
 - 5.6.2 Dateinamen
 - 5.6.3 Selektion von Dateien
 - 5.6.4 Dateistrukturen von EFs
 - 5.6.5 Zugriffsbedingungen auf Dateien
 - 5.6.6 Attribute von Dateien
- 5.7 Dateiverwaltung
- 5.8 Ablaufsteuerung
- 5.9 Atomare Abläufe
- 5.10 Chipkarten-Betriebssystem mit nachladbarem Programmcode
 - 5.10.1 Executable Native-Code
 - 5.10.2 JavaCard
- 5.11 Chipkarten-Betriebssystem „Small-OS“

6 Datenübertragung zur Chipkarte

- 6.1 Physikalische Übertragungsschicht
- 6.2 AntwortoReset-ATR
- 6.3 ProtocolTypeSelection-PTS
- 6.4 Übertragungsprotokolle
 - 6.4.1 Synchrone Datenübertragung
 - 6.4.1.1 Protokoll für Telefonchips
 - 6.4.1.2 I2C-Bus
 - 6.4.2 Übertragungsprotokoll T=0
 - 6.4.3 Übertragungsprotokoll T=1
 - 6.4.4 Übertragungsprotokoll T=14 (Deutschland)
 - 6.4.5 Vergleich der asynchronen Übertragungsprotokolle
- 6.5 Struktur der Nachrichten-APDUs
 - 6.5.1 Struktur der Kommando-APDUs
 - 6.5.2 Struktur der Antwort-APDUs
- 6.6 Sicherung der Datenübertragung
 - 6.6.1 Das Authentic-Verfahren
 - 6.6.2 Das Combined-Verfahren
 - 6.6.3 Sendefolgezähler
- 6.7 Logische Kanäle

7 Kommandos von Chipkarten

- 7.1 Kommandos zur Auswahl von Dateien
- 7.2 Schreib- und Lesekommandos
- 7.3 Suchkommandos
- 7.4 Operationen auf Dateien
- 7.5 Identifizierungskommandos
- 7.6 Authentisierungskommandos
- 7.7 Kommandos für kryptografische Algorithmen
- 7.8 Kommandos zur Verwaltung von Dateien
- 7.9 Datenbankkommandos-SCQL
- 7.10 Kommandos für elektronische Geldbörsen
- 7.11 Kommandos für Kredit- und Debitkarten
- 7.12 Kommandos zur Komplettierung des Betriebssystems
- 7.13 Kommandos zum Test der Hardware
- 7.14 Anwendungsspezifische Kommandos
- 7.15 Kommandos für Übertragungsprotokolle

8 Sicherheitstechnik

- 8.1 Benutzeridentifizierung
 - 8.1.1 Prüfung einer Geheimzahl
 - 8.1.2 Biometrische Verfahren
 - 8.1.2.1 Grundlagen
 - 8.1.2.2 Physiologische Merkmale
 - 8.1.2.3 Verhaltensbasierte Merkmale
- 8.2 Sicherheit einer Chipkarte
 - 8.2.1 Systematik der Angriffe und Angreifer
 - 8.2.2 Angriffe und Abwehrmaßnahmen während der Entwicklung
 - 8.2.2.1 Entwicklung des Chipkarten-Mikrocontrollers
 - 8.2.2.2 Entwicklung des Chipkarten-Betriebssystems
 - 8.2.3 Angriffe und Abwehrmaßnahmen während der Produktion
 - 8.2.4 Angriffe und Abwehrmaßnahmen während der Kartenbenutzung
 - 8.2.4.1 Angriffe auf der physikalischen Ebene
 - 8.2.4.2 Angriffe auf der logischen Ebene

9 Qualitätssicherung und Test

- 9.1 Test der Kartenkörper
- 9.2 Test der Hardware von Mikrocontrollern
- 9.3 Evaluierung und Test von Software
 - 9.3.1 Evaluierung
 - 9.3.2 Testmethoden für Software
 - 9.3.2.1 Grundlegendes Testen von Chipkarten-Software
 - 9.3.2.2 Testverfahren und Teststrategien
 - 9.3.3 Dynamische Tests von Betriebssystemen und Anwendungen

10 Lebenszyklus einer Chipkarte

- 10.1 Die 5 Phasen des Chipkarten-Lebenszyklus
- 10.2 Phase 1 des Lebenszyklus im Detail
 - 10.2.1 Erstellung des Betriebssystems und Herstellung der Chips
 - 10.2.2 Herstellung der Kartenkörper ohne integrierte Spule
 - 10.2.3 Herstellung von Kartenkörpern mit integrierter Spule
 - 10.2.4 Zusammenführen von Kartenkörper und Chip
- 10.3 Phase 2 des Lebenszyklus im Detail
- 10.4 Phase 3 des Lebenszyklus im Detail
- 10.5 Phase 4 des Lebenszyklus im Detail
- 10.6 Phase 5 des Lebenszyklus im Detail

11 Chipkarten-Terminals

- 11.1 Mechanische Eigenschaften
- 11.2 Elektrische Eigenschaften
- 11.3 Sicherheitstechnik
- 11.4 Anbindung eines Terminals mit PC/SC

12 Chipkarten im Zahlungsverkehr

- 12.1 Zahlungsverkehr mit Karten
 - 12.1.1 Elektronischer Zahlungsverkehr mit Chipkarten
 - 12.1.2 Elektronisches Geld
 - 12.1.3 Grundsätzliche Möglichkeiten der Systemstruktur
- 12.2 Vorbezahlte Speicherkarten
- 12.3 Elektronische Geldbörsen
 - 12.3.1 CEN-Norm EN 1546
 - 12.3.2 Das Mondex-System
- 12.4 Dasec-System in Deutschland
- 12.5 Kreditkarten mit Chip

13 Beispielhafte Anwendungen

- 13.1 Öffentliches Kartentelefon in Deutschland
- 13.2 Kontaktlose Speicherkarte für Flugverkehr
- 13.3 Krankenversichertenkarte
- 13.4 Elektronische Mautsysteme
- 13.5 Global System for Mobile Communications – GSM
- 13.6 Digitale Signatur

14 Design von Anwendungen

- 14.1 Allgemeine Hinweise und Kennzahlen
 - 14.1.1 Mikrocontroller
 - 14.1.2 Anwendungen
 - 14.1.3 System
- 14.2 Formelsammlung zur Abschätzung von Ausführungszeiten
- 14.3 Zeitfunktion typischer Chipkarten-Kommandos
- 14.4 Typische Ausführungszeiten von Kommandos
- 14.5 Hilfsmittel zur Anwendungsgenerierung
- 14.6 Ablauf eines Chipkarten-Projekts
- 14.7 Beispiele für die Konzeption von Chipkarten-Anwendungen
 - 14.7.1 Börse für Spielautomat
 - 14.7.2 Zugangskontrolle
 - 14.7.3 Prüfung auf Echtheit eines Terminals

15 Anhang

- 15.1 Glossar
- 15.2 Übersetzung von Fachwörtern
 - 15.2.1 Übersetzungsliste Deutsch – Englisch
 - 15.2.2 Übersetzungsliste Englisch – Deutsch
- 15.3 Literatur
- 15.4 Kommentiertes Normenverzeichnis
- 15.5 Registrierungsstellen für RID
- 15.6 Veranstaltungen
- 15.7 World-Wide-Web-Adressen
- 15.8 Kennwerte und Tabellen
 - 15.8.1 Zeitbereich für den ATR
 - 15.8.2 Umrechnungstabelle für Datenelemente des ATR
 - 15.8.3 Tabelle zur Ermittlung der Übertragungsgeschwindigkeit
 - 15.8.4 Tabelle mit Abtastzeitpunkten
 - 15.8.5 Tabelle der wichtigsten Chipkarten-Kommandos
 - 15.8.6 Übersicht über die verwendeten Instruction-Bytes
 - 15.8.7 Codierung von Chipkarten-Kommandos
 - 15.8.8 Chipkarten-Returncodes
 - 15.8.9 Ausgewählte Chips für Speicherkarten
 - 15.8.10 Ausgewählte Mikrocontroller für Chipkarten

Sachverzeichnis

Informationen aus der Industrie