HANSER

Chipkarten-Anwendungen

Wolfgang Rankl

Entwurfsmuster für Einsatz und Programmierung von Chipkarten

ISBN 3-446-40403-1

Inhaltsverzeichnis

Weitere Informationen oder Bestellungen unter
http://www.hanser.de/3-446-40403-1 sowie im Buchhandel

Inhaltsverzeichnis

1 Chipkarten im Überblick . . . 1

1.1 Systematik der Karten . . . 1

1.2 Kartenformate . . . 2

1.3 Kartenelemente . . . 3

1.3.1 Druck und Beschriftung . . . 3

1.3.2 Hochprägung . . . 4

1.3.3 Hologramm . . . 4

1.3.4 Unterschriftsstreifen . . . 4

1.3.5 Taktile Elemente . . . 4

1.3.6 Magnetstreifen . . . 5

1.3.7 Chipmodul . . . 5

1.3.8 Antenne . . . 5

1.4 Chipkarten-Mikrocontroller . . . 5

1.4.1 Prozessor . . . 8

1.4.2 Speicher . . . 8

1.4.3 Zusatzhardware . . . 9

1.4.4 Elektrische Eigenschaften . . . 10

2 Chipkarten-Betriebssysteme . . . 11

2.1 Dateiverwaltung . . . 11

2.1.1 Dateitypen . . . 12

2.1.2 Dateinamen . . . 13

2.1.3 Dateistrukturen . . . 13

2.1.4 Dateiattribute . . . 15

2.1.5 Dateiselektion . . . 15

2.1.6 Zugriffsbedingungen . . . 16

2.1.6.1 Zustandsorientierte Zugriffsbedingungen . . . 17

2.1.6.2 Regelbasierte Zugriffsbedingungen . . . 17

2.1.7 Lebenszyklus von Dateien 18
2.2 Kommandos 19
2.3 Datenübertragung 22
2.3.1 Answer to Reset (ATR) 24
2.3.2 Protocol Parameter Selection (PPS) 24
2.3.3 Übertragungsprotokolle 24
2.3.3.1 Kontaktbehaftetes Übertragungsprotokoll T=0 26
2.3.3.2 Kontaktbehaftetes Übertragungsprotokoll T=1 26
2.3.3.3 Kontaktbehaftetes Übertragungsprotokoll USB 26
2.3.3.4 Kontaktlose Übertragungsprotokolle 26
2.3.4 Sicherung der Datenübertragung 27
2.3.5 Logische Kanäle 27
2.4 Besondere Funktionen des Betriebssystems 27
2.4.1 Kryptografische Funktionen 27
2.4.2 Atomare Abläufe 28
2.4.3 Interpreter 29
2.4.4 Anwendungsverwaltung 29

3 Einsatzgebiete 31
3.1 Chipkarten-Systeme 31
3.2 Einsatzmöglichkeiten 32
3.3 Anwendungstypen 33
3.3.1 Speicherbasierte Anwendungen 33
3.3.2 Dateibasierte Anwendungen 34
3.3.3 Kodebasierte Anwendungen 34

4 Muster zu Grundlagen 37
4.1 Datenschutz 37
4.1.1 Begriffsbestimmung 38
4.1.2 Allgemeine Grundsätze 39
4.1.3 Empfehlungen für Chipkarten-Systeme 40
4.1.4 Zusammenfassung 43
4.2 Exportkontrolle 44
4.3 Kryptoregulierung 46
4.4 Normen 47
4.4.1 Normen zum Kartenkörper 48
4.4.2 Normen zum Betriebssystem 48

4.4.3 Normen zu Daten und zur Datenstrukturierung 49
4.4.4 Normen zur Rechneranbindung 49
4.4.5 Normen zu Anwendungen 49
4.5 Dokumente für Chipkarten-Systeme 50
4.5.1 Aufteilung der Spezifikationen 52
4.5.1.1 Systemspezifikationen 52
4.5.1.2 Spezifikationen für das Hintergrundsystem 53
4.5.1.3 Chipkartenspezifikationen 53
4.5.1.4 Terminalspezifikationen 54
4.5.2 Elemente einer typischen Kartenspezifikation 54
4.5.2.1 Allgemeine Abschnitte 54
4.5.2.2 Chipkarte 55
4.5.2.3 Chipkarten-Betriebssystem 56
4.5.2.4 Anwendung 58
4.5.3 Verteilung der Dokumente 59
4.5.4 Versionsnummerierung von Dokumenten 60

5 Muster zur Architektur 63
5.1 Daten 63
5.2 Kodierung von Daten 65
5.3 Dateien 65
5.3.1 Zugriffsbedingungen 66
5.3.2 Dateinamen 69
5.4 Protokolldateien 70
5.4.1 Datenablage 70
5.4.2 Aufteilung in Protokolldateien 70
5.4.3 Auslöser der Protokollierung 71
5.4.4 Zugriffsbedingungen auf Protokolldateien 71
5.4.5 Protokollierte Daten 73
5.4.6 Konsistenz und Authentizität von Protokolldaten 73
5.4.7 Größe der Protokolldatei 74
5.4.8 Ablauf der Protokollierung 75
5.5 Prägung 76
5.6 Schutz von Transaktionsdaten 78
5.7 Reset-sicherer Zähler 80
5.8 Proaktivität 81
5.9 Authentisierungszähler 83

5.10 Manuelle Echtheitsprüfung eines Terminals 85
5.11 Verwaltung von PINs 86
5.12 Einmalpasswörter 88
5.13 Schlüsselmanagement 92
5.14 Zustandsautomat für Kommandosequenzen 93
5.15 Geschwindigkeitsverbesserung 96
5.15.1 Rechenleistung 97
5.15.2 Kommunikation 98
5.15.3 Kommandos 98
5.15.4 Daten und Dateien 99

6 Muster zur Realisierung 101
6.1 Anwendungsprinzipien 101
6.1.1 Programmkode 101
6.1.2 Kommandos 103
6.1.3 Daten 104
6.1.4 Sicherheit 105
6.1.5 Anwendungsaufbau 107
6.1.6 System 110
6.2 Test 112
6.3 Benutzerschnittstelle am Terminal 118
6.4 Aufbau eines Kommandos 120
6.4.1 Aufbau eines Kommandos 120
6.4.2 Unterbrechung von Kommandos 122
6.4.3 Kodierung von Kommandos 123
6.4.4 Parametrisierung 124
6.4.5 Testkommandos 124
6.4.6 Geheimkommandos 124
6.5 Java Card 125
6.5.1 Datentypen 128
6.5.2 Arithmetik 133
6.5.3 Kontrollstrukturen 135
6.5.4 Methoden 137
6.5.5 Applets 138

7 Muster zum Betrieb 143
7.1 Initialisierung und Personalisierung 143

7.2 Migration 147
7.3 Überwachung 149
7.3.1 Systemintegrität 149
7.3.2 Angriffserkennung 150

8 Chipkarten in der Praxis 153
8.1 Akzeptanz 153
8.2 Indizien für schwierige Chipkarten-Systeme 156
8.2.1 Nicht adäquater Einsatz von Chipkarten 156
8.2.2 Unklare Spezifikationen 157
8.2.3 Viele Optionen 157
8.2.4 „Huckepack“-Anwendungen 158
8.2.5 Sparsamkeit beim Test 159
8.2.6 Nachladen von Anwendungen 160
8.2.7 Offline-Systeme 161
8.2.8 Intolerante Chipkarten und Terminals 162
8.2.9 Hohe Kompatibilitätsanforderungen 162
8.2.10 Überhöhte Sicherheitsanforderungen 163
8.2.11 Übertriebene Zukunftssicherheit 164
8.3 Voraussetzungen für einfache Chipkarten-Systeme 165
8.3.1 Einbindung von Experten 165
8.3.2 Vorausschauende Anwendungsgestaltung 166
8.3.3 Mit Prototypen zur reifen Anwendung 166
8.3.4 Eine einzige Anwendung auf der Chipkarte 167
8.3.5 Einfache Anwendungen 168
8.3.6 Robuste Anwendungen 168
8.3.7 Zentral betriebene Systeme 169
8.3.8 Stufenweise Inbetriebnahme des gesamten Systems 169
8.4 Fehler im Feld 170
8.4.1 Systematik der Fehlerarten 171
8.4.2 Auswirkungen von Fehlern 172
8.4.3 Maßnahmen beim Auftritt eines Fehlers 174
8.4.4 Vorgehen bei der Fehlersuche 175
8.4.5 Reaktionsmöglichkeiten nach erfolgreicher Fehlersuche 177

9 Diskussion von Fallbeispielen 179
9.1 Karte im Kloster 179

9.1.1 Verbesserung mit kryptografischer Prüfsumme 181
9.1.2 Verbesserung mit Prozessorkarten 181
9.2 Karte für Zutritt 182
9.3 Telemetriemodul 190
9.4 Visitenkarte 193
9.5 Karte als Diebstahlschutz 197
9.6 Eintrittskarte 200
9.7 PKI-Karte 203
9.8 SIM 206

Anhang 1 – Beschreibung Java Card 209

Anhang 2 – Beschreibung BasicCard 211

Literaturverzeichnis 217

Stichwortverzeichnis 221