Inhaltsverzeichnis

VORWORT 14

1 RFID GRUNDLAGEN 17

1.1 RFID Einführung 17
  1.1.1 „RF“ 17
  1.1.2 „ID“ 18
  1.1.3 Einteilung von RFID-Systemen 19
    1.1.3.1 Frequenzen und Übertragungsprinzipien 19
    1.1.3.2 Anwendungen 20

1.2 Komponenten eines RFID-Systems 22
  1.2.1 Karte (PICC) 22
  1.2.2 Lesegerät (PCD) 23

1.3 ISO/IEC 14443-Anwendungsbeispiele 24
  1.3.1 Ticketing im Personennahverkehr 24
  1.3.2 Mitarbeiterausweise 25
  1.3.3 Elektronischer Reisepass und Personalausweis 26
  1.3.4 Andere Anwendungen 27

1.4 Physikalische Grundlagen 27
  1.4.1 Energieübertragung 27
  1.4.2 Datenübertragung vom PCD zum PICC 29
    1.4.2.1 Amplitudenmodulation 29
    1.4.2.2 Standarddatenrate 106 kbit/s 29
    1.4.2.3 Höhere Datenraten bis 848 kbit/s 31
  1.4.3 Datenübertragung von PICC zu PCD 32
    1.4.3.1 Lastmodulation 33
    1.4.3.2 Hilfsträgermodulation, manchesterkodiert mit ASK 33
    1.4.3.3 Hilfsträgermodulation, NRZ-kodiert mit BPSK 34

2 ÜBERBLICK ÜBER DIE RELEVANTEN NORMEN 35

2.1 ISO/IEC 14443 35
  2.1.1 Teil 1: Physikalische Eigenschaften 36
  2.1.2 Teil 2: HF Eigenschaften und Signale 37
  2.1.3 Teil 3: Kartenselektion und -aktivierung 38
    2.1.3.1 Typ A: UIDs 38
    2.1.3.2 Typ A: Kartenaktivierung 40

2.1.3.3 Typ A: SAK-Kodierung 42
2.1.3.4 Typ A: Erkennung und Auflösung von Kollisionen 44
2.1.3.5 Typ B: Kartenaktivierung 46
2.1.3.6 Typ B: Parameter zur Kartenaktivierung 48
2.1.4 Teil 4: Kommunikationsprotokoll 49
2.1.4.1 Protokollaktivierung 49
2.1.4.2 Blockstruktur des T=CL-Protokolls 56
2.1.5 Information Block (I-Block) 56
2.1.5.1 Receive Ready Blocks (R-Blöcke) 58
2.1.5.2 Supervisory Blocks (S-Blöcke) 59
2.1.6 Electro Magnetic Disturbance (EMD) 61
2.1.6.1 Ruhezeit 62
2.1.6.2 Ruhepegel 63
2.1.6.3 Unterscheidung zwischen ungültiger Kartenantwort und EMD 63
2.1.6.4 Der Reader-IC MFRC522 und EMD 63

2.2 ISO/IEC 10373-6 Testmethoden 64
2.2.1 Testequipment 65
2.2.1.1 Calibration Coil 65
2.2.1.2 Test-PCD-Aufbau 65
2.2.1.3 ReferencePICC 66
2.2.2 Abstimmung und Kalibrierung 68
2.2.2.1 Tuning 68
2.2.2.2 Kalibrierung 68
2.2.3 Messungen am Lesegerät 69
2.2.3.1 Reichweitenmessung 69
2.2.3.2 Messaufwand 69
2.2.4 Tests für Layer 3 und 4 70

2.3 Near Field Communication (NFC) 70
2.3.1 Einleitung 70
2.3.2 NFC-Luftschnittstelle 71
2.3.2.1 NFC-Gerät als Karte 71
2.3.2.2 NFC-Gerät als Lesegerät 72
2.3.2.3 NFC-Gerät im „Active"-Modus 73

3 RFID-ANTENNENDESIGN 74

3.1 Theoretische Grundlagen 74
3.1.1 Antenne als Resonanzkreis 74
3.1.2 Transformatormodell 78
3.1.3 Biot-Savart-Gesetz 79
3.1.4 Die optimale Antennengröße 80

3.2 Lesegeräteantennen 83
- 3.2.1 Antennengüte 83
  - 3.2.1.1 Bandbreite zur Datenübertragung 83
  - 3.2.1.2 Stabilität gegen Verstimmung 87
- 3.2.2 Elektrisch leitende Flächen in der Nähe der Antenne 89
  - 3.2.2.1 Ferrite 90
- 3.2.3 Symmetrische und asymmetrische Antennen 92
  - 3.2.3.1 Symmetrische Antenne 93
  - 3.2.3.2 Asymmetrische Antenne 96

3.3 Kartenantennen 98
- 3.3.1 Standard Karten (ID-1) 98
- 3.3.2 Token mit kleineren Inlays (kleiner als ID-1) 100

3.4 Impedanzmessungen mit dem miniVNA 101
- 3.4.1 Bediensoftware für den miniVNA 102
- 3.4.2 Nachteile und Einschränkungen des miniVNA 102
  - 3.4.2.1 Fehlendes Vorzeichen beim Imaginärteil 102
  - 3.4.2.2 Fehlende Kalibrierung und Kompensation 102
- 3.4.3 Wie finde ich die richtige Kompensation? 103
- 3.4.4 Messung der Spuleninduktivität 105

4 SICHERHEIT UND KRYPTOGRAFIE 109

4.1 Schutzziele 109
- 4.1.1 Datengeheimhaltung 109
- 4.1.2 Datenintegrität 111
- 4.1.3 Schutz der Privatsphäre 111

4.2 Angriffe auf Smartcards 112
- 4.2.1 Logische Angriffe 112
  - 4.2.1.1 Unerlaubtes Auslesen von Daten 112
  - 4.2.1.2 Unerlaubtes Manipulieren von Daten 113
  - 4.2.1.3 “Reply”-Angriff 114
  - 4.2.1.4 “Relais”-Angriff 114
  - 4.2.1.5 „Man-in-the-middle“-Angriff 116
  - 4.2.1.6 „Denial of service“-Angriff 116
- 4.2.2 Physikalische Angriffe 116
  - 4.2.2.1 Seitenkanalangriffe und Power Analysis 117
  - 4.2.2.2 Reverse Engineering 118
  - 4.2.2.3 Licht- und Laserangriffe 119
  - 4.2.2.4 Temperatur und Frequenz 120
- 4.2.3 Kombinierte Angriffe 120

4.3 Kryptografie 120
4.3.1 Asymmetrische Kryptografie 120
4.3.2 Symmetrische Kryptografie 122
4.3.3 Block- und Stromchiffre 123
4.3.4 Encryption Standards: DES und AES 124
4.3.5 Kaskadierung von DES 125
4.3.6 Operationsmodus 127
4.3.6.1 Electronic Code Book (ECB) 127
4.3.6.2 Cipher Block Chaining (CBC) 127

4.4 Anwendung von Kryptografie 129
4.4.1 Gegenseitige Authentifizierung 129
4.4.2 Verschlüsselung der Daten 131
4.4.3 Message Authentication Code (MAC) 131
4.4.4 Schlüsselmanagement 132
4.4.4.1 Dynamische Schlüssel 132
4.4.4.2 Schlüsseldiversifizierung 132
4.4.5 Secure Application Module (SAM) 135
4.4.6 Bewertung von Sicherheit 135

5 EINFÜHRUNG KARTEN UND TAGS 136

5.1 Übersicht 136
5.1.1 Speicherkarten und Mikrocontrollerkarten 136
5.1.2 Vor- und Nachteile der Kontaktloskarte 136
5.1.2.1 Robustheit 137
5.1.2.2 Langlebigkeit 137
5.1.2.3 Nutzerfreundlichkeit 137
5.1.2.4 Infrastruktur 137
5.1.2.5 Kontakt zwischen Karte und Lesegerät 137
5.1.3 Dual-Interface-Karten 138

5.2 MIFARE 139
5.2.1 MIFARE Übersicht 139
5.2.1.1 Erfolgsstory 139
5.2.1.2 MIFARE Klone 139
5.2.1.3 „MIFARE Hack“ 139
5.2.1.4 MIFARE Produktübersicht 140
5.2.2 MIFARE Ultralight 140
5.2.2.1 Befehlssatz 141
5.2.2.2 Speicherlayout 142
5.2.2.3 Sicherheitsfunktionen 143
5.2.3 MIFARE Ultralight C 144
5.2.3.1 Befehlssatz 145

5.2.3.2 Speicherlayout 146
5.2.3.3 Sicherheitsfunktionen 146
5.2.4 MIFARE Classic 147
5.2.4.1 Befehlssatz 149
5.2.4.2 Speicherlayout 150
5.2.4.3 Sicherheitsfunktionen 151
5.2.5 MIFARE Plus 151
5.2.5.1 Speicherlayout 151
5.2.5.2 MIFARE Plus S und MIFARE Plus X 152
5.2.5.3 Security Level (Sicherheitsstufen) 152
5.2.6 MIFARE DESFire (EV1) 156
5.2.6.1 Speicherlayout 156
5.2.6.2 Filetypen 157
5.2.6.3 Daten File 157

6 ANTENNENDESIGN DES LESEGERÄTES 159

6.1 Readerbaustein MFRC522 159
6.1.1 Digitalschnittstellen 160
6.1.1.1 UART 160
6.1.1.2 SPI 160
6.1.1.3 I^2C 160
6.1.2 Oszillator 161
6.1.3 Analogschnittstellen 161
6.1.3.1 Sendeausgänge 161
6.1.3.2 Empfangseingang 165
6.1.4 Testsignale 169
6.1.4.1 MFOUT 170
6.1.4.2 AUX1 und AUX2 171
6.1.5 Sonstiges 173
6.1.5.1 Versorgungsspannung und GND 173
6.1.5.2 Toleranzen 173

6.2 Antennendesign 173
6.2.1 Spulendesign 174
6.2.1.1 Messen der Spulenparameter 175
6.2.1.2 Bestimmen der Güte und der Serienwiderstände 176
6.2.2 Anpassung: Berechnen der Startwerte 176
6.2.2.1 Parallelersatzschaltbild 176
6.2.2.2 Auftrennen und Vereinfachen der Schaltung 177
6.2.2.3 Tiefpassfilter 177
6.2.2.4 Anpassnetzwerk 178
6.2.3 Anpassung: Simulation und Messung 179
6.2.4 Messungen der Sendepulse 181

6.2.5 Messung und Anpassung des Empfangspfades 183
6.2.6 Störsignalbeseitigung 183
6.2.7 Reichweitenüberprüfung 185

7 DER ELEKTOR-RFID-READER 187

7.1 Einführung 187

7.2 Reader Hardware 190
7.2.1 Spannungsversorgung 192
7.2.2 Der P89LPC936 Mikrocontroller 193
7.2.3 Der Reader-IC MFRC522 194
7.2.4 Der USB/RS232 Konverter FT232R 197
7.2.4.1 FT232R Konfiguration 199
7.2.4.2 USB Treiber Modifikation 201

7.3 Aufbau und Inbetriebnahme 202
7.3.1 Installation des USB Treibers 202
7.3.2 Reader Firmware Update 203
7.3.3 Firmware Versionskontrolle 205

7.4 Reader-Betriebsarten 205
7.4.1 Terminal-Mode 205
7.4.2 PC Reader-Mode 207
7.4.2.1 Aktivierung des PC Reader-Mode 207

7.5 Die Firmware 208
7.5.1 Die Softwarearchitektur 208
7.5.2 Das Hauptprogramm 208
7.5.3 Die Funktion „PC_ReaderMode" 210
7.5.3.1 Das RS232 Übertragungsprotokoll 210

7.6 Die PC Entwicklungswerkzeuge 212
7.6.1 Elektor-RFID-Reader Programmierung unter .NET 212
7.6.2 Smart Card Magic.NET 214
7.6.2.1 Es geht auch ohne Programmieren 214
7.6.2.2 Ein Skript-Tool oder doch ein C# Compiler? 215
7.6.2.3 Unser erstes Programm: „Hello World" 216
7.6.2.4 Übersetzen und Ausführen 219
7.6.2.5 Benutzereingabe mit dem Konsolenfenster 220
7.6.2.6 Gibt es wirklich keinen Haltepunkt? 222
7.6.3 Visual C# 2010 Express Edition 222
7.6.3.1 Erstellen einer einfachen Konsolenanwendung 223
7.6.3.2 Einbinden der Elektor-RFID-Reader Library 226

8 KARTEN UND TAGS ANGEWANDT 228

8.1 ISO/IEC 14443 Typ A Kartenaktivierung 229
8.1.1 Kartentypen aus Sicht der Kartenaktivierung 229
8.1.2 Die Aktivierungssequenz 231
8.1.2.1 Das „Request“ und „Wakeup“ Kommando 232
8.1.2.2 Das „Anticollision“ und „Select“ Kommando 234
8.1.2.3 Das „Halt“ Kommando 236
8.1.3 Elektor-RFID-Reader Library: Kartenaktivierung 237
8.1.4 Programmbeispiele 242
8.1.4.1 Kartenaktivierung 242
8.1.4.2 Readerauswahl 244
8.1.4.3 Pollen nach Karten 245
8.1.4.4 Vereinfachte Kartenaktivierung 248
8.1.4.5 Testen der Lesereichweite 249
8.1.4.6 Alle Karten im Ansprechfeld des Readers auflisten 251

8.2 MIFARE Karten-Typerkennung 254
8.2.1 Programmbeispiel 255

8.3 Die MIFARE Ultralight Karte 258
8.3.1 Speicherlayout 258
8.3.2 Befehlssatz 259
8.3.3 Funktion der One Time Programmable (OTP) Bytes 260
8.3.3.1 Funktion der Lock Bits 262
8.3.4 Elektor-RFID-Reader Library: MIFARE Ultralight 262
8.3.5 Programmbeispiele 263
8.3.5.1 Schreiben und Löschen von Daten 263
8.3.5.2 Auslesen des gesamten Speicherinhalts 265
8.3.5.3 Schreiben und Lesen von Zeichenketten (Strings) 266
8.3.5.4 Eine einfache Ticket Anwendung 267
8.3.5.5 Klonen des Speicherinhalts 270
8.3.5.6 Sichere Datenspeicherung 271

8.4 Die MIFARE Classic Karte 278
8.4.1 Speicherlayout einer MIFARE Classic 1K Karte 278
8.4.2 Speicherlayout einer MIFARE Classic 4K Karte 279
8.4.3 Speicherlayout einer MIFARE Mini Karte 280
8.4.4 Befehlssatz 280
8.4.5 Das MIFARE Value Format 283
8.4.6 Decrement, Increment, Restore und Transfer 286
8.4.7 Ändern der Schlüsseln und der Zugriffsbedingung 287
8.4.8 Elektor-RFID-Reader Library: MIFARE Classic 291
8.4.8.1 Die Klasse „MIFAREClassicUtil“ 291

8.4.8.2 Das Interface „IMifareClassic“ ... 293
8.4.9 Programm- und Fallbeispiele ... 296
8.4.9.1 Schreiben und Löschen von Daten ... 296
8.4.9.2 Auslesen des gesamten Speicherinhalts ... 297
8.4.9.3 Optimierung der Lese- und Schreibgeschwindigkeit ... 298
8.4.9.4 Optimiertes Auslesen des gesamten Speicherinhalts ... 302
8.4.9.5 Das Problem der Datenkorruption ... 305
8.4.9.6 Die MIFARE Value Format Methoden ... 309
8.4.9.7 Elektronische Geldbörse mit Backup-Management ... 311

8.5 Die MIFARE Ultralight C Karte ... 317
8.5.1 Speicherlayout ... 317
8.5.2 Befehlssatz ... 318
8.5.3 Triple-DES Authentifizierung ... 318
8.5.4 Elektor-RFID-Reader Library: MIFARE Ultralight C ... 321
8.5.5 Programmbeispiele ... 322
8.5.5.1 Die MIFARE Ultralight C Authentifizierungssequenz ... 322
8.5.5.2 Personalisierung einer MIFARE Ultralight C Karte ... 327

8.6 Das Übertragungsprotokoll T=CL ... 331
8.6.1 T=CL Protokoll Aktivierung und Deaktivierung ... 332
8.6.1.1 Multi-Karten-Aktivierung (Multi Card Activation) ... 334
8.6.2 Datenaustausch ... 334
8.6.2.1 Smart Card Magic.NET - Exchange Mode ... 336
8.6.2.2 Blockverkettung (Chaining) ... 337
8.6.2.3 Wartezeitverlängerung (Waiting Time Extension) ... 337
8.6.2.4 Fehlererkennung und Fehlerkorrektur ... 338
8.6.3 Elektor-RFID-Reader Library: T=CL ... 339
8.6.4 Programmbeispiele ... 343
8.6.4.1 T=CL Protokoll Aktivierung und Deaktivierung ... 343
8.6.4.2 Multi-Karten-Aktivierung (Multi Card Activation) ... 345

8.7 Die MIFARE DESFire EV1 Karte ... 348
8.7.1 MIFARE DESFire EV1 Kommandos ... 349
8.7.2 Struktur der DESFire Native- Kommandos ... 349
8.7.2.1 Die Struktur der Kartenkommandos ... 350
8.7.2.2 Die Struktur der Kartenantworten ... 350
8.7.2.3 DESFire Blockverkettung (Chaining) ... 350
8.7.3 Das DESFire Filesystem ... 351
8.7.3.1 Dateitypen ... 351
8.7.3.2 Strukturen von Datendateien ... 352
8.7.3.3 Verzeichnisnamen ... 353
8.7.3.4 Dateinamen ... 354
8.7.4 Strukturierung der Daten ... 355

8.7.5 Elektor-RFID Reader Library: MIFARE DESFire EV1 355
8.7.6 Programmbeispiele 356
8.7.6.1 Erzeugen einer DESFire Anwendung 356
8.7.6.2 Standard Data File – Lesen und Schreiben von Daten 358

8.8 Application Protocol Data Units (APDUs) 360
8.8.1 Die Datenstruktur einer Command-APDU 361
8.8.1.1 Class-Byte (CLA-Byte) 361
8.8.1.2 Instruction-Byte (INS-Byte) 361
8.8.1.3 Parameter-Bytes P1 und P2 362
8.8.1.4 Codierung der Längenfelder Lc und Le 362
8.8.2 Die Datenstruktur einer Response-APDU 364
8.8.3 Beispiele von ISO/IEC 7816 kompatiblen APDUs 364
8.8.3.1 Das „SELECT„ Kommando 365
8.8.3.2 Das „READ BINARY" Kommando 366
8.8.3.3 Das „Update Binary" Kommando 367
8.8.4 Elektor-RFID-Reader Library: APDU 368
8.8.5 Zugriff auf ein ISO/IEC 7816 Filesystem 370
8.8.5.1 Programmbeispiel 372

9 ELEKTOR-RFID-READER PROJEKTE 376

9.1 Programmierung des Reader-IC MFRC522 376
9.1.1 Elektor-RFID-Reader Library: MFRC522 377
9.1.2 Programmbeispiele 377
9.1.2.1 Verändern der HF-Parameterkonfiguration 377
9.1.2.2 MFRC522 SFR Programmierung - Kartenaktivierung 378

9.2 RFID-Zutrittskontrollsysteme 386
9.2.1 Online-Systeme 386
9.2.2 Offline-Systeme 386
9.2.3 Der Elektor-RFID-Reader als Zutrittssystem 387
9.2.3.1 Funktionsbeschreibung 387
9.2.3.2 Access Control Manager 389
9.2.3.3 Mikrocontroller Firmware 390
9.2.3.4 Lesen und Löschen des P89LPC936 Daten-EEPROMs 394

9.3 Ein elektronischer Ausweis 395
9.3.1 Personalisierung 395
9.3.2 Lesen der Ausweisdaten 396

9.4 Starten einer Windows-Anwendung 397

10 SMARTCARD READER API-STANDARDS 399

10.1 Einleitung 399

10.2 Card Terminal-API (CT-API) 400

10.3 Open Card Framework (OCF) 400

10.4 Personal Computer/Smartcard (PC/SC) 401
10.4.1 Die PC/SC Architektur 401
10.4.1.1 Integrated Circuit Card (ICC) 401
10.4.1.2 Interface Device (IFD) 402
10.4.1.3 Interface Device Handler (IFD-Handler) 402
10.4.1.4 ICC Resource Manager (RM) 403
10.4.1.5 Service Provider 404
10.4.1.6 ICC-Aware Application 405

11 PC/SC READER 406

11.1 Kontaktlose Karten 406
11.1.1 Kontaktlose Mikrocontroller-Chipkarten 406
11.1.2 Kontaktlose Speicherkarten 406
11.1.2.1 PC/SC konforme APDUs 407
11.1.3 Answer To Reset (ATR) 408
11.1.3.1 Aktivierungssequenz einer kontaktbehafteten Karte 408
11.1.3.2 Die ATR-Struktur einer kontaktbehafteten Karte 410
11.1.3.3 Die pseudo ATR-Struktur einer kontaktlosen Karte 412

11.2 Die Microsoft WinSCard-API 414
11.2.1 WinSCard-API Programmierung 414
11.2.1.1 Programmieren der WinSCard-API in C 417

11.3 Java und PC/SC 424
11.3.1 JPC/SC Java API 424
11.3.2 Java Smartcard I/O API 426

11.4 Der CSharpPCSC Wrapper für .NET 427
11.4.1 Wie erstellt man einen API-Wrapper? 427
11.4.2 Die Klasse WinSCard 428
11.4.3 Die Klasse PCSCReader 430
11.4.4 Programmbeispiele 431
11.4.4.1 „Hello contactless Card“ 431
11.4.4.2 Alle installierten PC/SC Treiber ermitteln 434
11.4.4.3 Reader- und Karteneigenschaften ermitteln 435

11.4.4.4 Test der Lesereichweite 436
11.4.4.5 Kontaktlose Speicherkartentyp-Erkennung 438
11.4.4.6 MIFARE Classic 1/4K und MIFARE Ultralight 438
11.4.4.7 MIFARE DES Fire EV1 442

12 ABKÜRZUNGSVERZEICHNIS 446

13 LITERATURVERZEICHNIS 450

14 INDEX 452