Klaus Finkenzeller

# RFID Handbook

## Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication

THIRD EDITION




WILEY

# RFID HANDBOOK

## FUNDAMENTALS AND APPLICATIONS IN CONTACTLESS SMART CARDS, RADIO FREQUENCY IDENTIFICATION AND NEAR-FIELD COMMUNICATION, THIRD EDITION

**Klaus Finkenzeller**

*Giesecke & Devrient GmbH, Munich, Germany*

**Translated by Dörte Müller**

*Powerwording.com*



WILEY

A John Wiley and Sons, Ltd., Publication

This edition first published 2010



*Registered office*
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom



*Library of Congress Cataloging-in-Publication Data*

Finkenzeller, Klaus.
[RFID Handbuch. English]
Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition / Klaus Finkenzeller ; translated by Dörte Müller. – 3rd ed.
p. cm.
Includes index.
ISBN 978-0-470-69506-7 (cloth)
1. Inventory control–Automation. 2. Radio frequency identification systems. 3. Smart cards. I. Title.
TS160.F5513 2010
658.7′87 – dc22

2010008338

A catalogue record for this book is available from the British Library.

ISBN: 978-0-470-69506-7

Typeset in 9/11 Times by Laserwords Private Limited, Chennai, India
Printed and bound in Great Britain by CPI Antony Rowe, Chippenham, Wiltshire, UK

# Preface to the Third Edition

This book is aimed at an extremely wide range of readers. First and foremost it is intended for engineers and students who find themselves confronted with RFID technology for the first time. A few basic chapters are provided for this audience describing the functionality of RFID technology and the physical and IT-related principles underlying this field. The book is also intended for practitioners who, as users, wish to or need to obtain as comprehensive and detailed an overview of the various technologies, the legal framework or the possible applications of RFID as possible.

Although a wide range of individual articles are now available on this subject, the task of gathering all this scattered information together when it is needed is a tiresome and time-consuming one – as researching each new edition of this book proves. This book therefore aims to fill a gap in the range of literature on the subject of RFID. The need for well-founded technical literature in this field is proven by the fortunate fact that this book has now already appeared in five languages. Editions in two further languages are currently being prepared. Further information on the German version of the RFID handbook and the translations can be found on the homepage of this book, http://RFID-handbook.com.

This book uses numerous pictures and diagrams to attempt to give a graphic representation of RFID technology in the truest sense of the word. Particular emphasis is placed on the physical principles of RFID, which is why the chapter on this subject is by far the most comprehensive of the book. However, great importance is also assigned to providing an understanding of the basic concepts, data carrier and reader, as well as of the relevant standards and radio-technology regulations.

Technological developments in the field of RFID technology are proceeding at such a pace that although a book like this can explain the general scientific principles it is not dynamic enough to be able to explore the latest trends regarding the most recent products on the market and the latest standards and regulations. With the widespread use of RFID technology, it becomes also increasingly difficult not to lose track of applications. In ever-shorter intervals, the media provides information on new applications for RFID systems. I am therefore grateful for any suggestions and advice – particularly from the field of industry. The basic concepts and underlying physical principles remain, however, and provide a good background for understanding the latest developments.

A new addition to this third edition is Near-Field Communication (NFC) which has been introduced to several different chapters. Chapter 3 now includes the fundamentals of NFC; and Chapter 13 presents NFC interface components and describes the extension from NFC to secure-NFC.

Another addition is a complete wiring diagram and proposed circuit for an RFID reader according to ISO/IEC 14443. A layout and complete component kit of this wiring diagram and circuit is also available on the Internet.

It was a very special occasion when the Fraunhofer Smart Card Prize 2008 – which annually honors special contributions to smart-card technology - was awarded to the known smart-card

handbook of my two colleagues Rankl and Effing as well as to this RFID handbook. The prize-giving ceremony took place on the occasion of the 18th Smart-Card Workshop of the Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt on 5 February 2008.

In March 2008, we were able to look back on ten successful years of the RFID Handbook. The first German-language edition was published in March 1998 and comprised 280 pages. At that time, RFID was still a niche technology and hardly known to the public; this has completely changed. Today, RFID has become an established term; and due to applications such as the electronic passport and electronic product code (EPC), a broad public has become aware of this technology.

At this point I would also like to express my thanks to all companies which were kind enough to contribute to the success of this project by providing numerous technical data sheets, lecture manuscripts, drawings and photographs.

Klaus Finkenzeller

Munich, Autumn 2008

# List of Abbreviations

| | |
|---|---|
| µP | Microprocessor |
| µs | Microsecond ($10^{-6}$s) |
| ABS | Acrylnitrilbutadienstyrol |
| ACM | Access configuration matrix |
| AFC | Automatic fare collection |
| AFI | Application family identifier (see ISO 14443-3) |
| AI | Application identifier |
| AM | Amplitude modulation |
| APDU | Application data unit |
| ASCII | American Standard Code for Information Interchange |
| ASIC | Application specific integrated circuit |
| ASK | Amplitude shift keying |
| ATQ | Answer to request (ATQA, ATQB: see ISO 14443-3) |
| ATR | Answer to reset |
| AVI | Automatic vehicle identification (for railways) |
| BAC | Basic access control (ePassport) |
| BAPT | Bundesamt für Post und Telekommunikation (now the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway) |
| Bd | Baud, transmission speed in bit/s |
| BGT | Block guard time |
| BKA | Germany's Federal Criminal Police Office |
| BMBF | Bundesministerium für Bildung und Forschung (Ministry for Education and Research, was BMFT) |
| BMI | German Federal Ministry of the Interior |
| BP | Bandpass filter |
| BSI | German Federal Office for Information Security |
| C | Capacitance (of a capacitor) |
| CCG | Centrale für Coorganisation GmbH (central allocation point for EAN codes in Germany) |
| CCITT | Comité Consultatif International Télégraphique et Téléphonique |
| CEN | Comité Européen de Normalisation |
| CEPT | Conférence Européene des Postes et Télécommunications |
| CERP | Comité Européen de Règlementation Postale |
| CICC | Close coupling integrated circuit chip card |
| CIU | Contactless interface unit (transmission/receiving module for contactless microprocessor interfaces) |
| CLK | Clock (timing signal) |
| CRC | Cyclic redundancy checksum |

| | |
|---|---|
| dBm | Logarithmic measure of power, related to 1 mW HF-power (0 dBm = 1 mW, 30 dBm = 1 W) |
| DBP | Differential bi-phase encoding |
| DIN | Deutsche Industrienorm (German industrial standard) |
| DoD | Department of Defense (USA) |
| DS | Discovery services (EPC) |
| DWD | German Weather Service |
| EAN | European Article Number (barcode on groceries and goods) |
| EAS | Electronic article surveillance |
| EC | Eurocheque or electronic cash |
| ECC | European Communications Committee |
| ECTRA | European Committee for Regulatory Telecommunications Affairs |
| EDI | Electronic document interchange |
| EEPROM | Electric erasable and programmable read-only memory |
| EIRP | Equivalent isotropic radiated power |
| EMC | Electromagnetic compatibility |
| EOF | End of frame |
| EPC | Electronic product code |
| EPCIS | EPC Information Services |
| ERC | European Radiocommunications Committee |
| ERM | Electromagnetic compatibility and radio spectrum matters |
| ERO | European Radiocommunications Office |
| ERO | European Radio Office |
| ERP | Equivalent radiated power |
| ETCS | European Train Control System |
| ETS | European Telecommunication Standard |
| ETSI | European Telecommunication Standards Institute |
| EVC | European Vital Computer (part of ETCS) |
| FCC | Federal Commission of Communication |
| FDX | Full-duplex |
| FHSS | Frequency hopping spread spectrum |
| FM | Frequency modulation |
| FRAM | Ferroelectric random access memory |
| FSK | Frequency shift keying |
| GIAI | Global individual asset identifier (EPC) |
| GID | General identifier (EPC) |
| GRAI | Global returnable asset identifier (EPC) |
| GSM | Global System for Mobile Communication (was Groupe Spécial Mobile) |
| GTAG | Global-tag (RFID Initiative of EAN and the UCC) |
| HDX | Half-duplex |
| HF | High frequency (3–30 MHz) |
| $I^2C$ | Inter-IC-bus |
| ICAO | International Civil Aviation Organization |
| ICC | Integrated chip card |
| ID | Identification |
| ISM | Industrial scientific medical (frequency range) |
| ISO | International Organization for Standardization |
| ITU | International Telecommunication Union |
| L | Loop (inductance of a coil) |
| LAN | Local area network |

| | |
|---|---|
| LBT | Listen before talk |
| LF | Low frequency (30–300 kHz) |
| LPD | Low-power device (low-power radio system for the transmission of data or speech over a few hundred metres) |
| LRC | Longitudinal redundancy check |
| LSB | Least significant bit |
| MAD | MIFARE® Application Directory |
| MRZ | Machine readable zone (ePassport) |
| MSB | Most significant bit |
| NAD | Node address |
| NFC | Near field communication |
| nomL | Nonpublic mobile land radio (industrial radio, transport companies, taxi radio, etc.) |
| NRZ | Non-return-to-zero encoding |
| NTC | Negative temperature coefficient (thermal resistor) |
| NTWC | New Technologies Working Group (ICAO) |
| NVB | Number of valid bits (see ISO 14443-3) |
| OCR | Optical character recognition |
| OEM | Original equipment manufacturer |
| ONS | Object naming server (EPC) |
| OTA | Over the air (possibility to program a SIM card or a secure element via the GPRS/UMTS interface of a mobile phone) |
| OTP | One time programmable |
| PC | Personal computer |
| PCD | Proximity card device (see ISO 14443) |
| PICC | Proximity integrated contactless chip card (see ISO 14443) |
| PIN | Personal identification number |
| PKI | Public key infrastructure |
| PMU | Power management unit |
| POS | Point of sale |
| PP | Plastic package |
| PPS | Polyphenylensulfide |
| PSK | Phase shift keying |
| PUPI | Pseudo-unique PICC identifier (see ISO 14443-3) |
| PVC | Polyvinylchloride |
| R&TTE | Radio and Telecommunication Terminal Equipment (The Radio Equipment and Telecommunications Terminal Equipment Directive (1999/5/EC)) |
| RADAR | Radio detecting and ranging |
| RAM | Random access memory |
| RCS | Radar cross-section |
| REQ | Request |
| RFID | Radio frequency identification |
| RFU | Reserved for future use |
| RTI | Returnable trade items |
| RTI | Road transport information system |
| RTTT | Road transport and traffic telematics |
| RWD | Read–write device |
| SAM | Security authentication module |
| SAW | Surface acoustic wave |
| SCL | Serial clock ($I^2C$ bus interface) |
| SDA | Serial data address input–output ($I^2C$ bus interface) |

| | |
|---|---|
| SEQ | Sequential system |
| SGLN | Serialised global location number (EPC) |
| SMD | Surface-mounted devices |
| SNR | Serial number |
| SOF | Start of frame |
| SRAM | Static random access memory |
| SRD | Short-range devices (low-power radio systems for the transmission of data or voice over short distances, typically a few hundred metres) |
| SSCC | Serial shipping container code (EPC) |
| TR | Technical Regulation |
| UART | Universal asynchronous receiver–transmitter (transmission/receiving module for computer interfaces) |
| UCC | Universal Code Council (American standard for barcodes on groceries and goods) |
| UHF | Ultra-high frequency (300 Mhz to 3 GHz) |
| UN | United Nations |
| UPC | Universal Product Code |
| UPU | Universal Postal Union |
| VCD | Vicinity card device (see ISO 15693) |
| VDE | Verein Deutscher Elektrotechniker (German Association of Electrical Engineers) |
| VHE | Very high frequency (30 MHz to 300 MHz) |
| VICC | Vicinity integrated contactless chip card (see ISO 15693) |
| VSWR | Voltage standing wave ratio |
| XOR | Exclusive OR |
| ZV | Zulassungsvorschrift (Licensing Regulation) |

## Trademarks

# Contents

# 1

# Introduction

In recent years automatic identification procedures (Auto-ID) have become very popular in many service industries, purchasing and distribution logistics, industry, manufacturing companies and material flow systems. Automatic identification procedures exist to provide information about people, animals, goods and products in transit.

The omnipresent barcode labels that triggered a revolution in identification systems some considerable time ago, are being found to be inadequate in an increasing number of cases. Barcodes may be extremely cheap, but their stumbling block is their low storage capacity and the fact that they cannot be reprogrammed.

The technically optimal solution would be the storage of data in a silicon chip. The most common form of electronic data-carrying devices in use in everyday life is the smart card based upon a contact field (telephone smart card, bank cards). However, the mechanical contact used in the smart card is often impractical. A contactless transfer of data between the data-carrying device and its reader is far more flexible. In the ideal case, the power required to operate the electronic data-carrying device would also be transferred from the reader using contactless technology. Because of the procedures used for the transfer of power and data, contactless ID systems are called *RFID systems* (radio frequency identification).

The number of companies actively involved in the development and sale of RFID systems indicates that this is a market that should be taken seriously. Whereas global sales of RFID systems were approximately 900 million $US in the year 2000 it is estimated that this figure will reach 2650 million $US in 2005 (Krebs, n.d.). The *RFID market* therefore belongs to the fastest growing sector of the radio technology industry, including mobile phones and cordless telephones (Figure 1.1).

Furthermore, in recent years contactless identification has been developing into an independent interdisciplinary field, which no longer fits into any of the conventional pigeonholes. It brings together elements from extremely varied fields: RF technology and EMC, semiconductor technology, data protection and cryptography, telecommunications, manufacturing technology and many related areas.

As an introduction, the following section gives a brief overview of different automatic ID systems that perform similar functions to RFID (Figure 1.2).

*RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition.* Klaus Finkenzeller

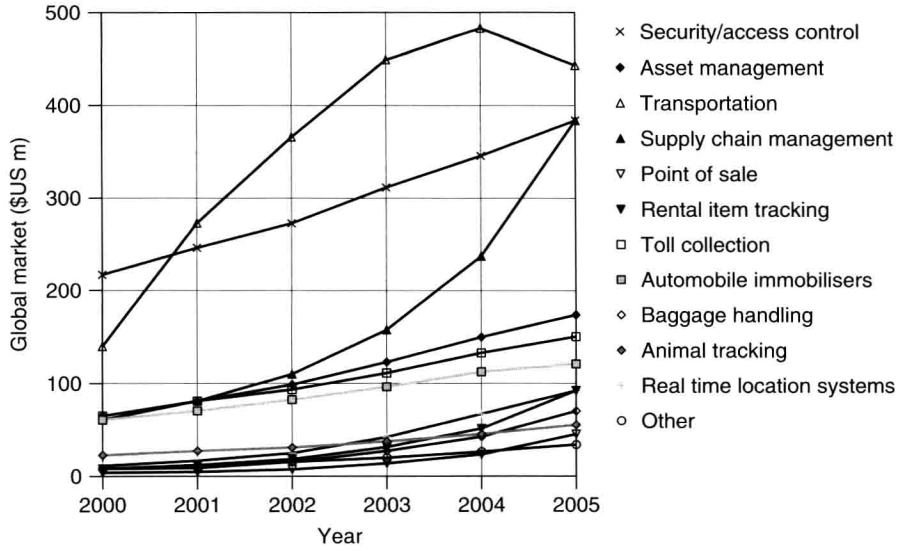


**Figure 1.1** The estimated growth of the global market for RFID systems between 2000 and 2005 in million $US, classified by application (Krebs, n.d.)

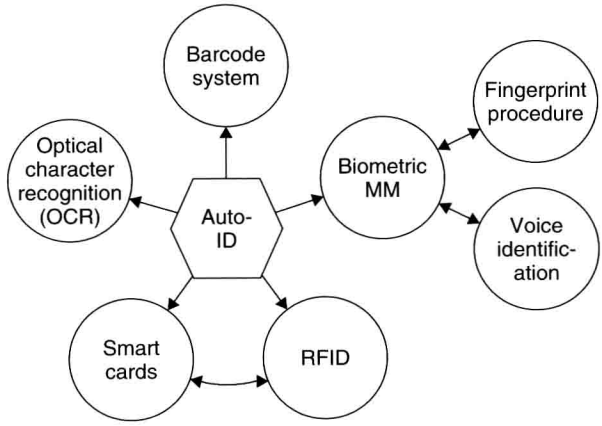


**Figure 1.2** Overview of the most important auto-ID procedures

## 1.1 Automatic Identification Systems

### *1.1.1 Barcode Systems*

*Barcodes* have successfully held their own against other identification systems over the past 20 years. According to experts, the turnover volume for barcode systems totalled around 3 billion DM in Western Europe at the beginning of the 1990s (Virnich and Posten, 1992).