WILEY

RFID HANDBOOK

Radio-Frequency Identification Fundamentals and Applications

KLAUS FINKENZELLER

RFID HANDBOOK

Radio-Frequency Identification Fundamentals and Applications

KLAUS FINKENZELLER

Giesecke & Devrient GmbH, Munich, Germany

Translated by
Rachel Waddington
Swadlincote, UK

JOHN WILEY & SON, LTD
Chichester • New York • Weinheim • Brisbane • Singapore •Toronto

First published under the title *RFID-Handbuch* by Carl Hanser Verlag

Copyright ©1999 John Wiley & Sons Ltd
Baffins Lane, Chichester,
West Sussex, PO19 1UD, England
National 01243 779777
International (+44) 1243 779777

e-mail (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on http://www.wiley.co.uk or http://www.wiley.com

Reprinted June 2000, April 2001

Neither the author nor John Wiley & Sons Ltd accept any responsibility or liability for loss or damage occasioned to any person or property through using the material, instructions, methods or ideas contained herein, or acting or refraining from acting as a result of such use. The author(s) and Publisher expressly disclaim all implied warranties, including merchantability or fitness for any particular purpose.

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons is aware of a claim, the product names appear in initial capital or all capital letters. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

Other Wiley Editorial Offices

John Wiley & Sons, Inc., 605 Third Avenue,
New York, NY 10158-0012, USA

Weinheim • Brisbane • Singapore • Toronto

Library of Congress Cataloging-in-Publication Data

Finkenzeller, Klaus.
[RFID Handbuch. English]
RFID handbook : radio-frequency identification fundamentals and applications / Klaus Finkenzeller : translated by Rachel Waddington
p. cm.
Includes bibliographical references and index.
ISBN 0-471-98851-0 (alk. paper)
1. Inventory control—Automation. 2. Radio frequency identification systems. I. Title.
TS160.F5513 1999 99-16221
658.7—dc21 CIP

British Library Cataloguing in Publication Data

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

ISBN 0 471 98851 0

Produced from PostScript files supplied by the translator
Printed and bound in Great Britain by Antony Rowe Ltd, Chippenham
This book is printed on acid-free paper responsibly manufactured from sustainable forestry in which at least two trees are planted for each one used for paper production.

Contents

Preface

This book is aimed at an extremely wide range of readers. First and foremost it is intended for students and engineers 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 this book has proved. This book therefore aims to fill a gap in the range of literature on the subject of RFID.

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 practical considerations. For this reason the chapter entitled "Example Applications" is particularly comprehensive.

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. 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.

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

Munich, January 1998 Klaus Finkenzeller

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 device 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 that are actively involved in the development and sale of RFID systems indicates that this is a market that should be taken seriously. Total worldwide sales of RFID systems for the year 2000 are estimated at above 2 billion US$. The *RFID market* therefore belongs to the fastest growing sector of the radio technology industry, including mobile phones and cordless telephones.

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

As an introduction, the following chapter gives a brief overview of different auto ID systems, that perform similar functions to RFID.

specific parts of the programme are not loaded into the EEPROM until after manufacture and can be initiated via the operating system.

Microprocessor cards are primarily used in security sensitive applications. Examples are smart cards for GSM mobile phones and the new EC (electronic cash) cards. The option of programming the microprocessor cards also facilitates rapid adaptation to new applications [rankl].

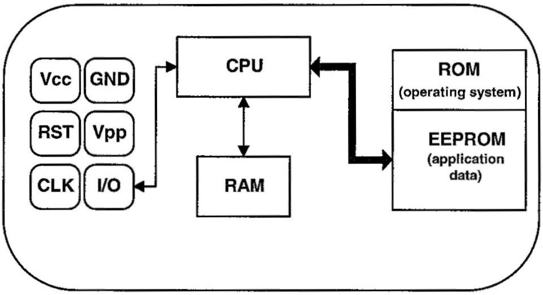


Figure 1.5: Typical architecture of a microprocessor card

1.1.5 RFID systems

RFID systems are closely related to the smart cards described above. Like smart card systems, data is stored on an electronic data carrying device – the transponder. However, unlike the smart card, the power supply to the data carrying device and the data exchange between data carrying device and reader are achieved without the use of galvanic contacts, using instead magnetic or electromagnetic fields. The underlying technical procedure is drawn from the fields of radio and radar engineering. The abbreviation RFID stands for radio frequency identification, i.e. information carried by radio waves. Due to the numerous advantages of RFID systems compared with other identification systems, RFID systems are now beginning to conquer new mass markets. One example is the use of contactless smart cards as tickets for short-distance public transport.

1.2 A Comparison of Different 1D Systems

A comparison between the identification systems described above highlights the strengths and weakness of RFID in relation to other systems. Here too, there is a close relationship between contact based smart cards and RFID systems, however the latter circumvents all the disadvantages related to faulty contacting (sabotage, dirt, unidirectional insertion, time consuming insertion, etc.).

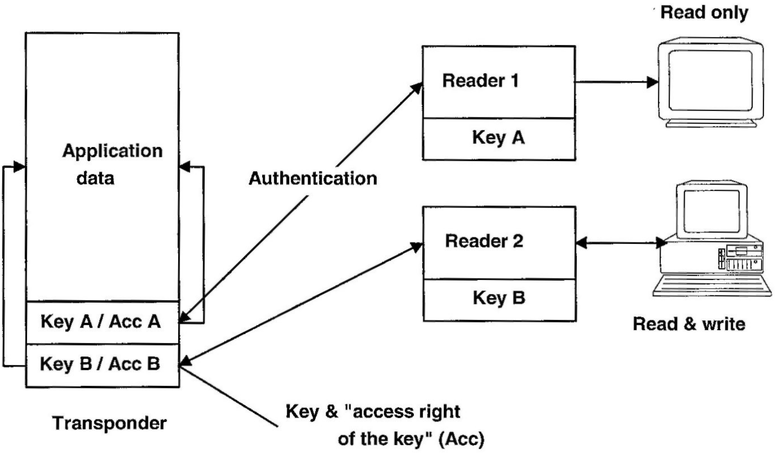


Figure 10.10: A transponder with two key memories facilitates the hierarchical allocation of access rights, in connection with the authentication keys used

The access rights to the transponder's two access registers A and B are configured such that, after successful authentication using key A, the system only permits the deduction of monetary amounts (the devaluation of a counter in the transponder). Only after authentication with key B may monetary amounts be added (the revaluation of the same counter).

In order to protect against attempted fraud, the readers in vehicles or subway entrances, i.e. devaluers, are only provided with key A. This means that a transponder can never be revalued using a devaluer, not even if the software of a stolen devaluer is manipulated. The transponder itself refuses to add to the internal counter unless the transaction has been authenticated by the correct key.

The high-security key B is only loaded into selected secure readers that are protected against theft. The transponder can only be revalued using these readers.

10.1.3.4 Segmented memory

Transponders can also be protected from access by readers that belong to other applications using authentication procedures, as we described in a previous chapter. In transponders with large memory capacities, it is possible to divide the entire memory into small units called segments, and protect each of these from unauthorised access with a separate key. A *segmented transponder* like this permits data from different applications to be stored completely separately.

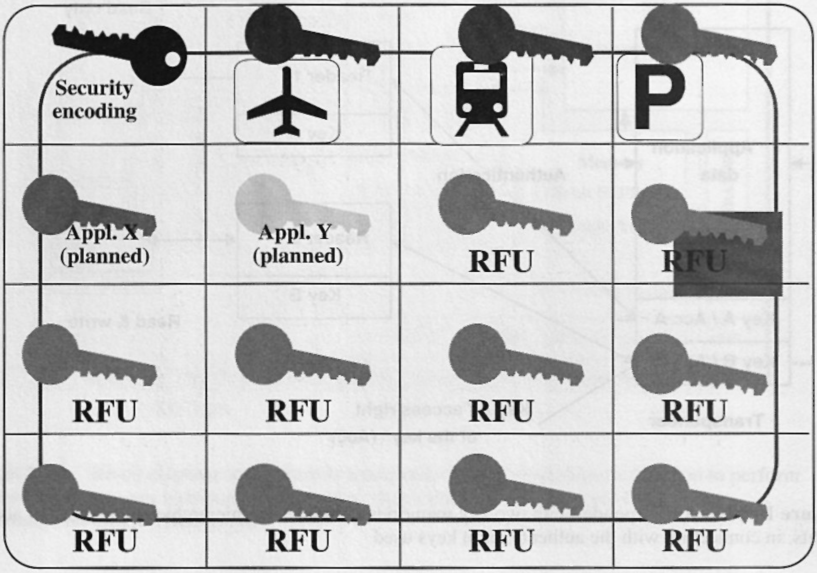


Figure 10.11: Several applications on one transponder – each protected by its own secret key

Access to an individual segment can only be gained after successful authentication with the appropriate key. Therefore, a reader belonging to one application can only gain access to its "own" segment if it only knows the *application's own key*.

The majority of segmented memory systems use fixed segment sizes. In these systems, the storage space within a segment cannot be altered by the user. A fixed segment size has the advantage that it is very simple and cheap to realise upon the transponder's microchip.

However, it is very rare for the storage space required by an application to correspond with the segment size of the transponder.

In small applications, valuable storage space is wasted on the transponder, because the segments are only partially used. Very large applications, on the other hand, need to be distributed across several segments, which means that the application specific key must be stored in each of the occupied segments. This multiple storage of an identical key also wastes valuable storage space.

A much better use of space is achieved by the use of variable length segments. Here, the memory allocated to a segment can be matched to the requirements of the application using the memory area. Because of the difficulty in realising *variable segmentation*, this variant is rare in transponders with state machines.

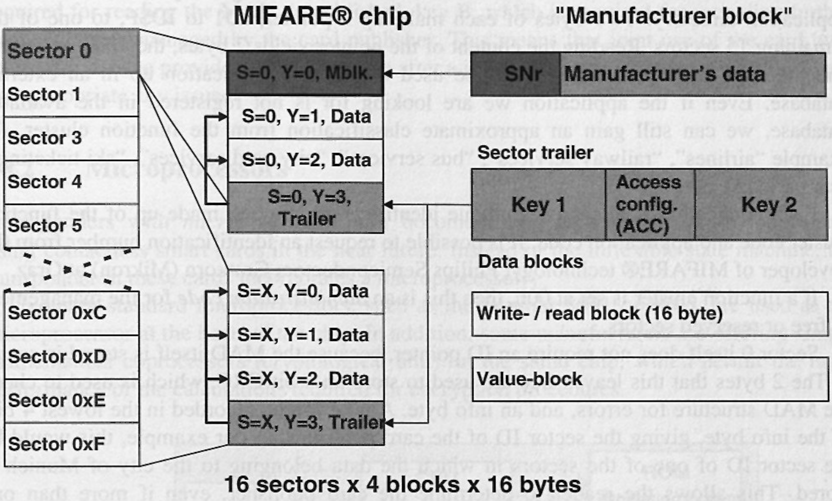
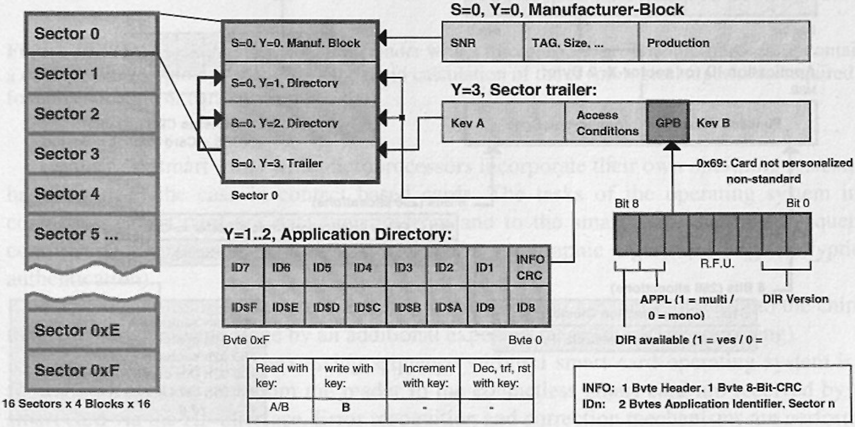


Figure 10.14: Memory configuration of a MIFARE® data carrier [koo]. The entire memory is divided into 16 independent sectors. Thus a maximum of separate 16 applications can be loaded onto a MIFARE® card



ID7	ID6	ID5	ID4	ID3	ID2	ID1	INFO CRC
ID$F	ID$E	ID$D	ID$C	ID$B	ID$A	ID9	ID8

Read with key:	write with key:	Increment with key:	Dec, trf, rst with key:
A/B	B	-	-

INFO: 1 Bvte Header. 1 Bvte 8-Bit-CRC
IDn: 2 Bvtes Application Identifier. Sector n

Figure 10.15: The data structure of the MIFARE® application directory consists of an arrangement of 15 pointers (ID1 to ID$F), which point to the subsequent sectors

Table 14.1 continued: Overview of RFID systems on the market

System manufacturer:	Coupling, operating method, energy, distance:	Memory: gross / net:	Security logic	Downlink reader → transponder:	Uplink transponder → reader:
SLE44R42S (MIFARE® plus)	-“-	14 k Mask ROM 4 k EEPROM 7816 contacts	-“- + 8 bit,	-“-	-“-
MOBY-F	125 kHz, ind., 0 – 7 cm	240 Byte EEPROM	n.i.	n.i.	n.i.
MOBY-L	4 MHz, ind., 0 – 5 cm	512 Byte EEPROM	n.i.	0.1 kbyte/s	n.i.
MOBY-I	1.81 MHz, ind., 0 – 1 m	128 Byte EEPROM, 32 k RAM	n.i.	n.i.	n.i.
MOBY-E	13.56 MHz, ind., 0 – 10 cm	752 Byte EEPROM	n.i.	n.i.	n.i.
MOBY-V	433 MHz, em., battery, 0 – 80 cm	32 k RAM	n.i.	>1 kbyte/s	n.i.
SOFIS	2.45 GHz, em., 0 – 1.3 m	20 bit fix. SAW	n.i.	(read only)	surface wave
Sokymat Titan 4000	125 kHz, ind.	128 Byte EEPROM	password	ASK	load modulation
Unique 1200	125 kHz, ind., 0 – 20 cm	8 Byte, OTP Laser-ROM	n.i.	ASK	load modulation
Sony, FeliCa	13.56 MHz, ind., 0 – 10 cm	1 kByte	authentication encryption	modified ASK 250 kbit/s	n.i.
TagMaster AB, Confident S1251, S1255	2.45 Ghz, em., 0–4 m (read) 0–0.5m (write), Li battery	8 – 75 Byte	anticollision	(random interval mode) 4 kBit/s	backscatter, 16 kBit/s
Temic, TK 5530	125 kHz, ind.	16 Byte PROM (Laser cutting)	n.i.	read-only	load modulation FSK, PSK, / Manchester, bi-phase, max. 15 kbit/s