

RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification,

Second Edition

Klaus Finkenzeller

Copyright © 2003 John Wiley & Sons, Ltd.

ISBN: 0-470-84402-7

RFID Handbook

Second Edition

RFID Handbook

Fundamentals and Applications in Contactless Smart
Cards and Identification

Second Edition

Klaus Finkenzeller

Giesecke & Devrient GmbH, Munich, Germany

Translated by

Rachel Waddington

Member of the Institute of Translation and Interpreting



First published under the title *RFID-Handbuch, 2 Auflage* by Carl Hanser Verlag
© Carl Hanser Verlag, Munich/FRG, 1999 All rights reserved
Authorized translation from the 2nd edition in the original German language
published by Carl Hanser Verlag, Munich/FRG

Copyright © 2003 John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,
West Sussex PO19 8SQ, England
Telephone (+44) 1243 779777

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

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Copyright, Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London W1T 4LP, UK, without the permission in writing of the Publisher. Requests to the Publisher should be addressed to the Permissions Department, John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, or emailed to permreq@wiley.co.uk, or faxed to (+44) 1243 770571.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the Publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 33 Park Road, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 22 Worcester Road, Etobicoke, Ontario, Canada M9W 1L1

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data

Finkenzeller, Klaus.

[RFID Handbuch. English]

RFID handbook : fundamentals and applications in contactless smart cards and identification/Klaus Finkenzeller; translated by Rachel Waddington. — 2nd ed.

p. cm.

Includes bibliographical references and index.

ISBN 0-470-84402-7 (alk. paper)

1. Inventory control — Automation. 2. Radio frequency identification systems. 3. Smart cards. I. Title.

TS160.F5513 2003

658.7'87 — dc21

2002192439

British Library Cataloguing in Publication Data

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

ISBN 0-470-84402-7

Typeset in 10/12pt Times by Laserwords Private Limited, Chennai, India

Printed and bound in Great Britain by Antony Rowe Ltd, Chippenham, Wiltshire

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.

SML Exhibit 1017

Contents

PREFACE	xiii
LIST OF ABBREVIATIONS	xv
1 Introduction	1
1.1 Automatic Identification Systems	2
1.1.1 Barcode systems	2
1.1.2 Optical character recognition	3
1.1.3 Biometric procedures	4
1.1.3.1 Voice identification	4
1.1.3.2 Fingerprinting procedures (dactyloscopy)	4
1.1.4 Smart cards	5
1.1.4.1 Memory cards	5
1.1.4.2 Microprocessor cards	6
1.1.5 RFID systems	6
1.2 A Comparison of Different ID Systems	7
1.3 Components of an RFID System	7
2 Differentiation Features of RFID Systems	11
2.1 Fundamental Differentiation Features	11
2.2 Transponder Construction Formats	13
2.2.1 Disks and coins	13
2.2.2 Glass housing	14
2.2.3 Plastic housing	14
2.2.4 Tool and gas bottle identification	15
2.2.5 Keys and key fobs	17
2.2.6 Clocks	18
2.2.7 ID-1 format, contactless smart cards	18
2.2.8 Smart label	19
2.2.9 Coil-on-chip	20
2.2.10 Other formats	21
2.3 Frequency, Range and Coupling	22
2.4 Information Processing in the Transponder	23
2.4.1 Low-end systems	23
2.4.2 Mid-range systems	24
2.4.3 High-end systems	25
2.5 Selection Criteria for RFID Systems	25
2.5.1 Operating frequency	26
2.5.2 Range	26

2.5.3	Security requirements	27
2.5.4	Memory capacity	28
3	Fundamental Operating Principles	29
3.1	1-Bit Transponder	29
3.1.1	Radio frequency	30
3.1.2	Microwaves	33
3.1.3	Frequency divider	35
3.1.4	Electromagnetic types	36
3.1.5	Acoustomagnetic	37
3.2	Full and Half Duplex Procedure	40
3.2.1	Inductive coupling	41
3.2.1.1	Power supply to passive transponders	41
3.2.1.2	Data transfer transponder → reader	42
3.2.2	Electromagnetic backscatter coupling	47
3.2.2.1	Power supply to the transponder	47
3.2.2.2	Data transmission → reader	49
3.2.3	Close coupling	49
3.2.3.1	Power supply to the transponder	49
3.2.3.2	Data transfer transponder → reader	50
3.2.4	Electrical coupling	51
3.2.4.1	Power supply of passive transponders	51
3.2.4.2	Data transfer transponder → reader	53
3.2.5	Data transfer reader → transponder	53
3.3	Sequential Procedures	54
3.3.1	Inductive coupling	54
3.3.1.1	Power supply to the transponder	54
3.3.1.2	A comparison between FDX/HDX and SEQ systems	54
3.3.1.3	Data transmission transponder → reader	56
3.3.2	Surface acoustic wave transponder	57
4	Physical Principles of RFID Systems	61
4.1	Magnetic Field	61
4.1.1	Magnetic field strength H	61
4.1.1.1	Path of field strength $H(x)$ in conductor loops	62
4.1.1.2	Optimal antenna diameter	65
4.1.2	Magnetic flux and magnetic flux density	66
4.1.3	Inductance L	67
4.1.3.1	Inductance of a conductor loop	68
4.1.4	Mutual inductance M	68
4.1.5	Coupling coefficient k	70
4.1.6	Faraday's law	71
4.1.7	Resonance	73
4.1.8	Practical operation of the transponder	78
4.1.8.1	Power supply to the transponder	78
4.1.8.2	Voltage regulation	78

4.1.9	Interrogation field strength $H_{\min}$	80
4.1.9.1	Energy range of transponder systems	82
4.1.9.2	Interrogation zone of readers	84
4.1.10	Total transponder — reader system	86
4.1.10.1	Transformed transponder impedance Z'_T	88
4.1.10.2	Influencing variables of Z'_T	90
4.1.10.3	Load modulation	97
4.1.11	Measurement of system parameters	103
4.1.11.1	Measuring the coupling coefficient k	103
4.1.11.2	Measuring the transponder resonant frequency	105
4.1.12	Magnetic materials	106
4.1.12.1	Properties of magnetic materials and ferrite	107
4.1.12.2	Ferrite antennas in LF transponders	108
4.1.12.3	Ferrite shielding in a metallic environment	109
4.1.12.4	Fitting transponders in metal	110
4.2	Electromagnetic Waves	111
4.2.1	The generation of electromagnetic waves	111
4.2.1.1	Transition from near field to far field in conductor loops	112
4.2.2	Radiation density S	114
4.2.3	Characteristic wave impedance and field strength E	115
4.2.4	Polarisation of electromagnetic waves	116
4.2.4.1	Reflection of electromagnetic waves	117
4.2.5	Antennas	119
4.2.5.1	Gain and directional effect	119
4.2.5.2	EIRP and ERP	120
4.2.5.3	Input impedance	121
4.2.5.4	Effective aperture and scatter aperture	121
4.2.5.5	Effective length	124
4.2.5.6	Dipole antennas	125
4.2.5.7	Yagi–Uda antenna	127
4.2.5.8	Patch or microstrip antenna	128
4.2.5.9	Slot antennas	130
4.2.6	Practical operation of microwave transponders	131
4.2.6.1	Equivalent circuits of the transponder	131
4.2.6.2	Power supply of passive transponders	133
4.2.6.3	Power supply of active transponders	140
4.2.6.4	Reflection and cancellation	141
4.2.6.5	Sensitivity of the transponder	142
4.2.6.6	Modulated backscatter	143
4.2.6.7	Read range	145
4.3	Surface Waves	148
4.3.1	The creation of a surface wave	148
4.3.2	Reflection of a surface wave	150
4.3.3	Functional diagram of SAW transponders (Figure 4.95)	151
4.3.4	The sensor effect	153
4.3.4.1	Reflective delay lines	154
4.3.4.2	Resonant sensors	155

4.3.4.3	Impedance sensors	157
4.3.5	Switched sensors	159
5	Frequency Ranges and Radio Licensing Regulations	161
5.1	Frequency Ranges Used	161
5.1.1	Frequency range 9–135 kHz	161
5.1.2	Frequency range 6.78 MHz	163
5.1.3	Frequency range 13.56 MHz	163
5.1.4	Frequency range 27.125 MHz	163
5.1.5	Frequency range 40.680 MHz	165
5.1.6	Frequency range 433.920 MHz	165
5.1.7	Frequency range 869.0 MHz	166
5.1.8	Frequency range 915.0 MHz	166
5.1.9	Frequency range 2.45 GHz	166
5.1.10	Frequency range 5.8 GHz	166
5.1.11	Frequency range 24.125 GHz	166
5.1.12	Selection of a suitable frequency for inductively coupled RFID systems	167
5.2	European Licensing Regulations	169
5.2.1	CEPT/ERC REC 70-03	169
5.2.1.1	Annex 1: Non-specific short range devices	170
5.2.1.2	Annex 4: Railway applications	171
5.2.1.3	Annex 5: Road transport and traffic telematics	172
5.2.1.4	Annex 9: Inductive applications	172
5.2.1.5	Annex 11: RFID applications	172
5.2.1.6	Frequency range 868 MHz	173
5.2.2	EN 300 330: 9 kHz–25 MHz	173
5.2.2.1	Carrier power — limit values for H field transmitters	173
5.2.2.2	Spurious emissions	175
5.2.3	EN 300 220-1, EN 300 220-2	175
5.2.4	EN 300 440	176
5.3	National Licensing Regulations in Europe	177
5.3.1	Germany	177
5.4	National Licensing Regulations	179
5.4.1	USA	179
5.4.2	Future development: USA–Japan–Europe	180
6	Coding and Modulation	183
6.1	Coding in the Baseband	184
6.2	Digital Modulation Procedures	186
6.2.1	Amplitude shift keying (ASK)	186
6.2.2	2 FSK	189
6.2.3	2 PSK	190
6.2.4	Modulation procedures with subcarrier	191
7	Data Integrity	195
7.1	The Checksum Procedure	195

7.1.1	Parity checking	195
7.1.2	LRC procedure	196
7.1.3	CRC procedure	197
7.2	Multi-Access Procedures — Anticollision	200
7.2.1	Space division multiple access (SDMA)	202
7.2.2	Frequency domain multiple access (FDMA)	204
7.2.3	Time domain multiple access (TDMA)	205
7.2.4	Examples of anticollision procedures	206
7.2.4.1	ALOHA procedure	206
7.2.4.2	Slotted ALOHA procedure	208
7.2.4.3	Binary search algorithm	212
8	Data Security	221
8.1	Mutual Symmetrical Authentication	221
8.2	Authentication Using Derived Keys	223
8.3	Encrypted Data Transfer	224
8.3.1	Stream cipher	225
9	Standardisation	229
9.1	Animal Identification	229
9.1.1	ISO 11784 — Code structure	229
9.1.2	ISO 11785 — Technical concept	230
9.1.2.1	Requirements	230
9.1.2.2	Full/half duplex system	232
9.1.2.3	Sequential system	232
9.1.3	ISO 14223 — Advanced transponders	233
9.1.3.1	Part 1 — Air interface	233
9.1.3.2	Part 2 — Code and command structure	234
9.2	Contactless Smart Cards	236
9.2.1	ISO 10536 — Close coupling smart cards	237
9.2.1.1	Part 1 — Physical characteristics	238
9.2.1.2	Part 2 — Dimensions and locations of coupling areas	238
9.2.1.3	Part 3 — Electronic signals and reset procedures	238
9.2.1.4	Part 4 — Answer to reset and transmission protocols	239
9.2.2	ISO 14443 — Proximity coupling smart cards	240
9.2.2.1	Part 1 — Physical characteristics	240
9.2.2.2	Part 2 — Radio frequency interference	240
9.2.2.3	Part 3 — Initialisation and anticollision	245
9.2.2.4	Part 4 — Transmission protocols	251
9.2.3	ISO 15693 — Vicinity coupling smart cards	256
9.2.3.1	Part 1 — Physical characteristics	256
9.2.3.2	Part 2 — Air interface and initialisation	256
9.2.4	ISO 10373 — Test methods for smart cards	260
9.2.4.1	Part 4: Test procedures for close coupling smart cards	261
9.2.4.2	Part 6: Test procedures for proximity coupling smart cards	261
9.2.4.3	Part 7: Test procedure for vicinity coupling smart cards	264

9.3	ISO 69873 — Data Carriers for Tools and Clamping Devices	265
9.4	ISO 10374 — Container Identification	265
9.5	VDI 4470 — Anti-theft Systems for Goods	265
9.5.1	Part 1 — Detection gates — inspection guidelines for customers	265
9.5.1.1	Ascertaining the false alarm rate	266
9.5.1.2	Ascertaining the detection rate	267
9.5.1.3	Forms in VDI 4470	267
9.5.2	Part 2 — Deactivation devices, inspection guidelines for customers	268
9.6	Item Management	268
9.6.1	ISO 18000 series	268
9.6.2	GTAG initiative	269
9.6.2.1	GTAG transport layer (physical layer)	270
9.6.2.2	GTAG communication and application layer	271

10 The Architecture of Electronic Data Carriers **273**

10.1	Transponder with Memory Function	273
10.1.1	HF interface	273
10.1.1.1	Example circuit — load modulation with subcarrier	274
10.1.1.2	Example circuit — HF interface for ISO 14443 transponder	276
10.1.2	Address and security logic	278
10.1.2.1	State machine	279
10.1.3	Memory architecture	280
10.1.3.1	Read-only transponder	280
10.1.3.2	Writable transponder	281
10.1.3.3	Transponder with cryptological function	281
10.1.3.4	Segmented memory	284
10.1.3.5	MIFARE® application directory	286
10.1.3.6	Dual port EEPROM	289
10.2	Microprocessors	292
10.2.1	Dual interface card	293
10.2.1.1	MIFARE® plus	295
10.2.1.2	Modern concepts for the dual interface card	296
10.3	Memory Technology	298
10.3.1	RAM	299
10.3.2	EEPROM	299
10.3.3	FRAM	300
10.3.4	Performance comparison FRAM — EEPROM	302
10.4	Measuring Physical Variables	302
10.4.1	Transponder with sensor functions	302
10.4.2	Measurements using microwave transponders	303
10.4.3	Sensor effect in surface wave transponders	305

11 Readers **309**

11.1	Data Flow in an Application	309
11.2	Components of a Reader	309

11.2.1	HF interface	311
11.2.1.1	Inductively coupled system, FDX/HDX	312
11.2.1.2	Microwave systems — half duplex	313
11.2.1.3	Sequential systems — SEQ	314
11.2.1.4	Microwave system for SAW transponders	315
11.2.2	Control unit	316
11.3	Low Cost Configuration — Reader IC U2270B	317
11.4	Connection of Antennas for Inductive Systems	319
11.4.1	Connection using current matching	320
11.4.2	Supply via coaxial cable	322
11.4.3	The influence of the Q factor	325
11.5	Reader Designs	326
11.5.1	OEM readers	326
11.5.2	Readers for industrial use	327
11.5.3	Portable readers	328

12 The Manufacture of Transponders and Contactless

	Smart Cards	329
12.1	Glass and Plastic Transponders	329
12.1.1	Module manufacture	329
12.1.2	Semi-finished transponder	330
12.1.3	Completion	332
12.2	Contactless Smart Cards	332
12.2.1	Coil manufacture	333
12.2.2	Connection technique	336
12.2.3	Lamination	338

13 Example Applications

Example Applications	341
13.1 Contactless Smart Cards	341
13.2 Public Transport	342
13.2.1 The starting point	343
13.2.2 Requirements	344
13.2.2.1 Transaction time	344
13.2.2.2 Resistance to degradation, lifetime, convenience	344
13.2.3 Benefits of RFID systems	345
13.2.4 Fare systems using electronic payment	346
13.2.5 Market potential	346
13.2.6 Example projects	347
13.2.6.1 Korea — seoul	347
13.2.6.2 Germany — Lüneburg, Oldenburg	349
13.2.6.3 EU Projects — ICARE and CALYPSO	350
13.3 Ticketing	354
13.3.1 Lufthansa miles & more card	354
13.3.2 Ski tickets	356

13.4	Access Control	357
13.4.1	Online systems	357
13.4.2	Offline systems	358
13.4.3	Transponders	360
13.5	Transport Systems	361
13.5.1	Eurobalise S21	361
13.5.2	International container transport	363
13.6	Animal Identification	364
13.6.1	Stock keeping	364
13.6.2	Carrier pigeon races	367
13.7	Electronic Immobilisation	371
13.7.1	The functionality of an immobilisation system	372
13.7.2	Brief success story	375
13.7.3	Predictions	376
13.8	Container Identification	376
13.8.1	Gas bottles and chemical containers	376
13.8.2	Waste disposal	378
13.9	Sporting Events	379
13.10	Industrial Automation	381
13.10.1	Tool identification	381
13.10.2	Industrial production	385
13.10.2.1	Benefits from the use of RFID systems	387
13.10.2.2	The selection of a suitable RFID system	388
13.10.2.3	Example projects	389
13.11	Medical Applications	392
14	Appendix	394
14.1	Contact Addresses, Associations and Technical Periodicals	394
14.1.1	Industrial associations	394
14.1.2	Technical journals	398
14.1.3	RFID on the internet	399
14.2	Relevant Standards and Regulations	400
14.2.1	Sources for standards and regulations	405
14.3	References	406
14.4	Printed Circuit Board Layouts	412
14.4.1	Test card in accordance with ISO 14443	412
14.4.2	Field generator coil	413
	INDEX	419

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 ID Systems

A comparison between the identification systems described above highlights the strengths and weakness of RFID in relation to other systems (Table 1.1). 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.).

1.3 Components of an RFID System

An *RFID system* is always made up of two components (Figure 1.7):

- the *transponder*, which is located on the object to be identified;
- the interrogator or *reader*, which, depending upon the design and the technology used, may be a read or write/read device (in this book — in accordance with normal colloquial usage — the data capture device is always referred to as the *reader*, regardless of whether it can only read data or is also capable of writing).

A practical example is shown in Figure 1.8.

A reader typically contains a radio frequency module (transmitter and receiver), a control unit and a coupling element to the transponder. In addition, many readers are fitted with an additional interface (RS 232, RS 485, etc.) to enable them to forward the data received to another system (PC, robot control system, etc.).

The transponder, which represents the actual *data-carrying device* of an RFID system, normally consists of a *coupling element* and an electronic *microchip* (Figure 1.9).

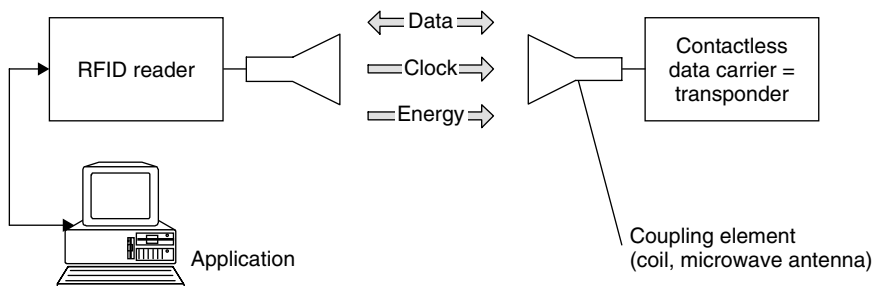


Figure 1.7 The reader and transponder are the main components of every RFID system

Table 1.1 Comparison of different RFID systems showing their advantages and disadvantages

System parameters	Barcode	OCR	Voice recog.	Biometry	Smart card	RFID systems
Typical data quantity (bytes)	1–100	1–100	—	—	16–64 k	16–64 k
Data density	Low	Low	High	High	Very high	Very high
Machine readability	Good	Good	Expensive	Expensive	Good	Good
Readability by people	Limited	Simple	Simple	Difficult	Impossible	Impossible
Influence of dirt/damp	Very high	Very high	—	—	Possible (contacts)	No influence
Influence of (opt.) covering	Total failure	Total failure	—	Possible	—	No influence
Influence of direction and position	Low	Low	—	—	Unidirectional	No influence
Degradation/wear	Limited	Limited	—	—	Contacts	No influence
Purchase cost/reading electronics	Very low	Medium	Very high	Very high	Low	Medium
Operating costs (e.g. printer)	Low	Low	None	None	Medium (contacts)	None
Unauthorised copying/modification	Slight	Slight	Possible* (audio tape)	Impossible	Impossible	Impossible
Reading speed (including handling of data carrier)	Low	Low	Very low	Very low	Low	Very fast
Maximum distance between data carrier and reader	~4 s	~3 s	>5 s	>5–10 s	~4 s	~0.5 s
	0–50 cm	<1 cm	0–50 cm	Direct contact**	Direct contact	0–5-m, microwave

*The danger of 'Replay' can be reduced by selecting the text to be spoken using a random generator, because the text that must be spoken is not known in advance.

**This only applies for fingerprint ID. In the case of retina or iris evaluation direct contact is not necessary or possible.



Figure 1.8 RFID reader and contactless smart card in practical use (reproduced by permission of Kaba Benzing GmbH)

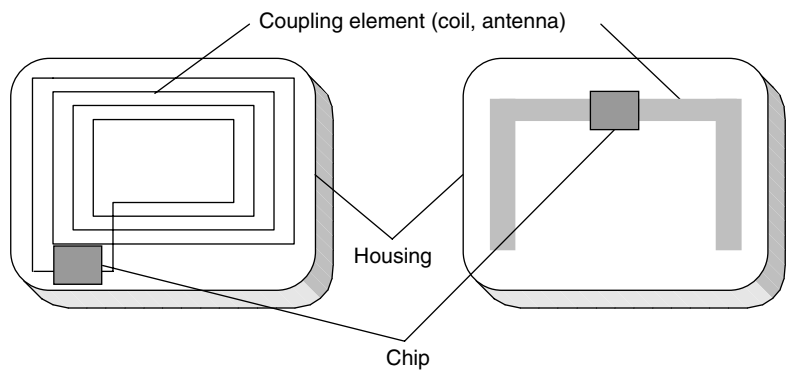


Figure 1.9 Basic layout of the RFID data-carrying device, the transponder. Left, inductively coupled transponder with antenna coil; right, microwave transponder with dipolar antenna

When the transponder, which does not usually possess its own voltage supply (battery), is not within the interrogation zone of a reader it is totally passive. The transponder is only activated when it is within the interrogation zone of a reader. The power required to activate the transponder is supplied to the transponder through the coupling unit (contactless), as are the timing pulse and data.

2

Differentiation Features of RFID Systems

2.1 Fundamental Differentiation Features

RFID systems exist in countless variants, produced by an almost equally high number of manufacturers. If we are to maintain an overview of RFID systems we must seek out features that can be used to differentiate one RFID system from another (Figure 2.1).

RFID systems operate according to one of two basic procedures: full duplex (FDX)/half duplex (HDX) systems, and sequential systems (SEQ).

In *full* and *half duplex* systems the transponder's response is broadcast when the reader's RF field is switched on. Because the transponder's signal to the receiver antenna can be extremely weak in comparison with the signal from the reader itself, appropriate transmission procedures must be employed to differentiate the transponder's signal from that of the reader. In practice, data transfer from transponder to reader takes place using load modulation, load modulation using a subcarrier, but also (sub)harmonics of the reader's transmission frequency.

In contrast, *sequential procedures* employ a system whereby the field from the reader is switched off briefly at regular intervals. These gaps are recognised by the transponder and used for sending data from the transponder to the reader. The disadvantage of the sequential procedure is the loss of power to the transponder during the break in transmission, which must be smoothed out by the provision of sufficient auxiliary capacitors or batteries.

The data capacities of RFID transponders normally range from a few bytes to several kilobytes. So-called 1-bit transponders represent the exception to this rule. A data quantity of exactly 1-bit is just enough to signal two states to the reader: 'transponder in the field' or 'no transponder in the field'. However, this is perfectly adequate to fulfil simple monitoring or signalling functions. Because a 1-bit transponder does not need an electronic chip, these transponders can be manufactured for a fraction of a penny. For this reason, vast numbers of 1-bit transponders are used in *Electronic Article Surveillance* (EAS) to protect goods in shops and businesses. If someone attempts to leave the shop with goods that have not been paid for the reader installed in the exit recognises the state 'transponder in the field' and initiates the appropriate reaction. The 1-bit transponder is removed or deactivated at the till when the goods are paid for.

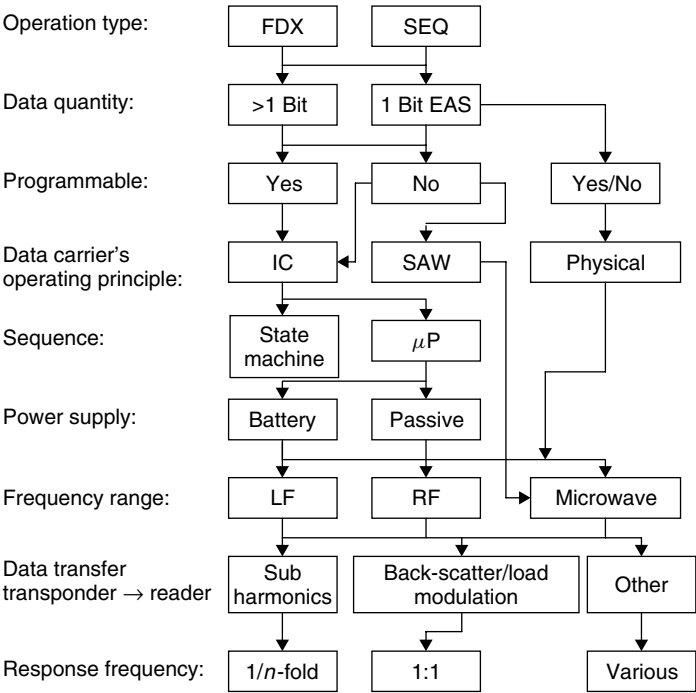


Figure 2.1 The various features of RFID systems (Integrated Silicon Design, 1996)

The possibility of writing data to the transponder provides us with another way of classifying RFID systems. In very simple systems the transponder's data record, usually a simple (serial) number, is incorporated when the chip is manufactured and cannot be altered thereafter. In writable transponders, on the other hand, the reader can write data to the transponder. Three main procedures are used to store the data: in inductively coupled RFID systems EEPROMs (electrically erasable programmable read-only memory) are dominant. However, these have the disadvantages of high power consumption during the writing operation and a limited number of write cycles (typically of the order of 100 000 to 1 000 000). FRAMs (ferromagnetic random access memory) have recently been used in isolated cases. The read power consumption of FRAMs is lower than that of EEPROMs by a factor of 100 and the writing time is 1000 times lower. Manufacturing problems have hindered its widespread introduction onto the market as yet.

Particularly common in microwave systems, SRAMs (static random access memory) are also used for data storage, and facilitate very rapid write cycles. However, data retention requires an uninterruptible power supply from an auxiliary battery.

In programmable systems, write and read access to the memory and any requests for write and read authorisation must be controlled by the data carrier's internal logic. In the simplest case these functions can be realised by a state machine (see Chapter 10 for further information). Very complex sequences can be realised using *state machines*. However, the disadvantage of state machines is their inflexibility regarding changes to the programmed functions, because such changes necessitate changes to the circuitry

of the silicon chip. In practice, this means redesigning the chip layout, with all the associated expense.

The use of a microprocessor improves upon this situation considerably. An operating system for the management of application data is incorporated into the processor during manufacture using a mask. Changes are thus cheaper to implement and, in addition, the software can be specifically adapted to perform very different applications.

In the context of contactless smart cards, writable data carriers with a state machine are also known as ‘memory cards’, to distinguish them from ‘processor cards’.

In this context, we should also mention transponders that can store data by utilising physical effects. This includes the read-only surface wave transponder and 1-bit transponders that can usually be deactivated (set to 0), but can rarely be reactivated (set to 1).

One very important feature of RFID systems is the *power supply* to the transponder. *Passive transponders* do not have their own power supply, and therefore all power required for the operation of a passive transponder must be drawn from the (electrical/magnetic) field of the reader. Conversely, *active transponders* incorporate a battery, which supplies all or part of the power for the operation of a microchip.

One of the most important characteristics of RFID systems is the *operating frequency* and the resulting range of the system. The operating frequency of an RFID system is the frequency at which the reader transmits. The transmission frequency of the transponder is disregarded. In most cases it is the same as the *transmission frequency* of the reader (load modulation, backscatter). However, the transponder’s ‘transmitting power’ may be set several powers of ten lower than that of the reader.

The different transmission frequencies are classified into the three basic ranges, LF (low frequency, 30–300 kHz), HF (high frequency)/RF radio frequency (3–30 MHz) and UHF (ultra high frequency, 300 MHz–3 GHz)/microwave (>3 GHz). A further subdivision of RFID systems according to range allows us to differentiate between close-coupling (0–1 cm), remote-coupling (0–1 m), and long-range (>1 m) systems.

The different procedures for sending data from the transponder back to the reader can be classified into three groups: (i) the use of reflection or backscatter (the frequency of the reflected wave corresponds with the transmission frequency of the reader → frequency ratio 1:1) or (ii) load modulation (the reader’s field is influenced by the transponder → frequency ratio 1:1), and (iii) the use of subharmonics ($1/n$ fold) and the generation of harmonic waves (n -fold) in the transponder.

2.2 Transponder Construction Formats

2.2.1 Disks and coins

The most common construction format is the so-called *disk* (coin), a transponder in a round (ABS) injection moulded housing, with a diameter ranging from a few millimetres to 10 cm (Figure 2.2). There is usually a hole for a fastening screw in the centre. As an alternative to (ABS) injection moulding, polystyrol or even epoxy resin may be used to achieve a wider operating temperature range.

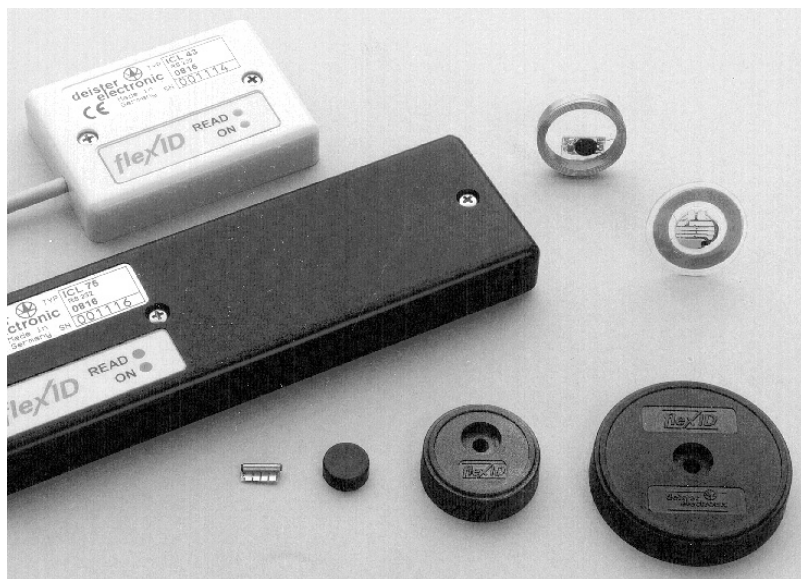


Figure 2.2 Different construction formats of disk transponders. Right, transponder coil and chip prior to fitting in housing; left, different construction formats of reader antennas (reproduced by permission of Deister Electronic, Barsinghausen)

2.2.2 Glass housing

Glass transponders (Figure 2.3) have been developed that can be injected under the skin of an animal for identification purposes (see Chapter 13).

Glass tubes of just 12–32 mm contain a microchip mounted upon a carrier (PCB) and a chip capacitor to smooth the supply current obtained. The transponder coil incorporates wire of just 0.03 mm thickness wound onto a ferrite core. The internal components are embedded in a soft adhesive to achieve mechanical stability (Figure 2.4).

2.2.3 Plastic housing

The *plastic housing* (*plastic package*, PP) was developed for applications involving particularly high mechanical demands. This housing can easily be integrated into other products, for example into *car keys* for *electronic immobilisation systems* (Figure 2.5).

The wedge made of moulding substance (IC casting compound) contains almost the same components as the glass transponder, but its longer coil gives it a greater functional range (Figure 2.6). Further advantages are its ability to accept larger microchips and its greater tolerance to mechanical vibrations, which is required by the automotive industry, for example. The *PP transponder* has proved completely satisfactory with regard to other quality requirements, such as temperature cycles or fall tests (Bruhnke, 1996).

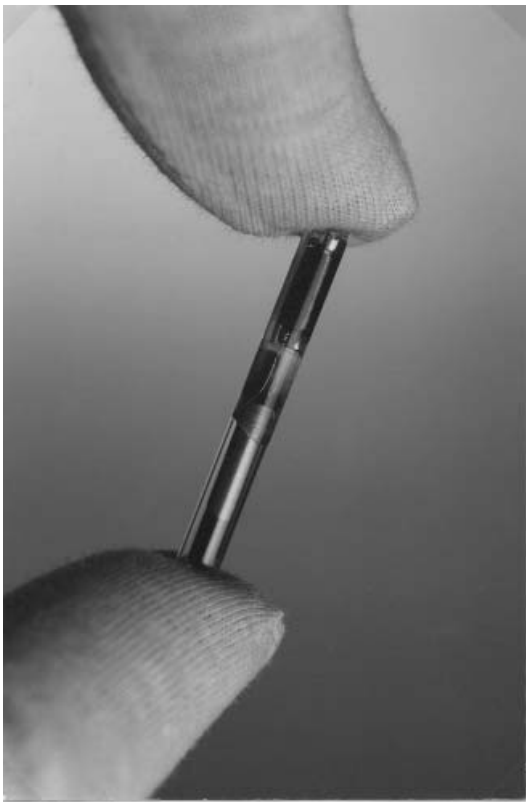


Figure 2.3 Close-up of a 32 mm glass transponder for the identification of animals or further processing into other construction formats (reproduced by permission of Texas Instruments)

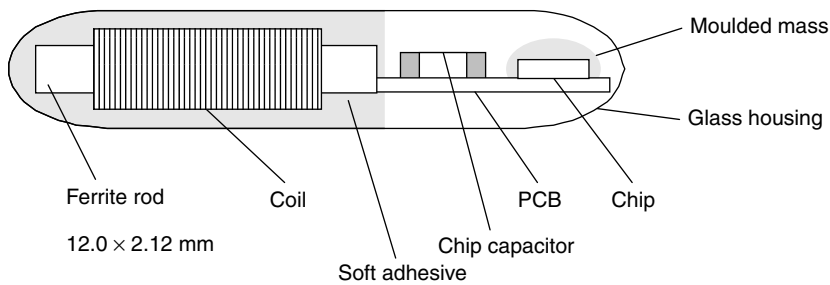


Figure 2.4 Mechanical layout of a glass transponder

2.2.4 Tool and gas bottle identification

Special construction formats have been developed to install inductively coupled transponders into *metal surfaces*. The transponder coil is wound in a ferrite pot core. The transponder chip is mounted on the reverse of the *ferrite pot core* and contacted with the transponder coil.

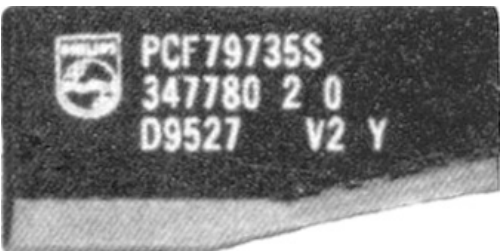


Figure 2.5 Transponder in a plastic housing (reproduced by permission of Philips Electronics B.V.)

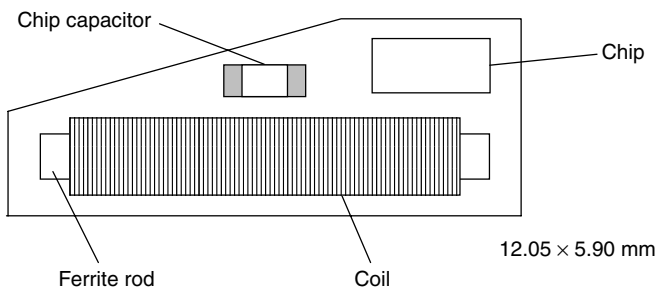


Figure 2.6 Mechanical layout of a transponder in a plastic housing. The housing is just 3 mm thick



Figure 2.7 Transponder in a standardised construction format in accordance with ISO 69873, for fitting into one of the retention knobs of a CNC tool (reproduced by permission of Leitz GmbH & Co., Oberkochen)

In order to obtain sufficient mechanical stability, vibration and heat tolerance, transponder chip and ferrite pot core are cast into a PPS shell using epoxy resin (Link, 1996, 1997). The external dimensions of the transponder and their fitting area have been standardised in *ISO 69873* for incorporation into a retention knob or quick-release taper for tool identification (Figure 2.7). Different designs are used for the

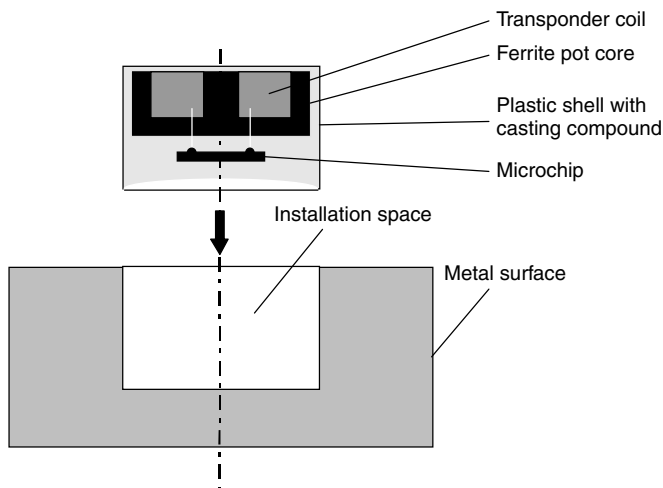


Figure 2.8 Mechanical layout of a transponder for fitting into metal surfaces. The transponder coil is wound around a U-shaped ferrite core and then cast into a plastic shell. It is installed with the opening of the U-shaped core uppermost



Figure 2.9 Keyring transponder for an access system (reproduced by permission of Intermarketing)

identification of gas bottles. Figure 2.8 shows the mechanical layout of a transponder for fitting into a metal surface.

2.2.5 Keys and key fobs

Transponders are also integrated into mechanical keys for immobilisers or door locking applications with particularly high security requirements. These are generally based upon a transponder in a plastic housing, which is cast or injected into the key fob.

The keyring transponder design has proved very popular for systems providing access to office and work areas (Figure 2.9).



Figure 2.10 Watch with integral transponder in use in a contactless access authorisation system (reproduced by permission of Junghans Uhren GmbH, Schramberg)

2.2.6 Clocks

This construction format was developed at the beginning of the 1990s by the Austrian company Ski-Data and was first used in ski passes. These *contactless clocks* were also able to gain ground in access control systems (Figure 2.10). The clock contains a frame antenna with a small number of windings printed onto a thin printed circuit board, which follows the clock housing as closely as possible to maximise the area enclosed by the antenna coil — and thus the range.

2.2.7 ID-1 format, contactless smart cards

The ID-1 format familiar from credit cards and telephone cards (85.72 mm × 54.03 mm × 0.76 mm ± tolerances) is becoming increasingly important for *contactless smart cards* in RFID systems (Figure 2.11). One advantage of this format for inductively coupled RFID systems is the large coil area, which increases the range of the smart cards.

Contactless smart cards are produced by the lamination of a transponder between four PVC foils. The individual foils are baked at high pressure and temperatures above 100 °C to produce a permanent bond (the manufacture of contactless smart cards is described in detail in Chapter 12).

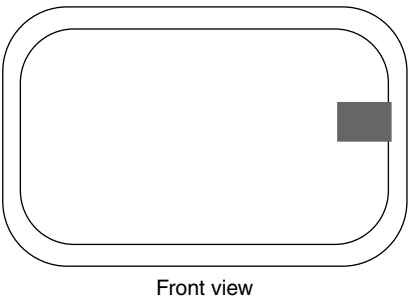


Figure 2.11 Layout of a contactless smart card: card body with transponder module and antenna

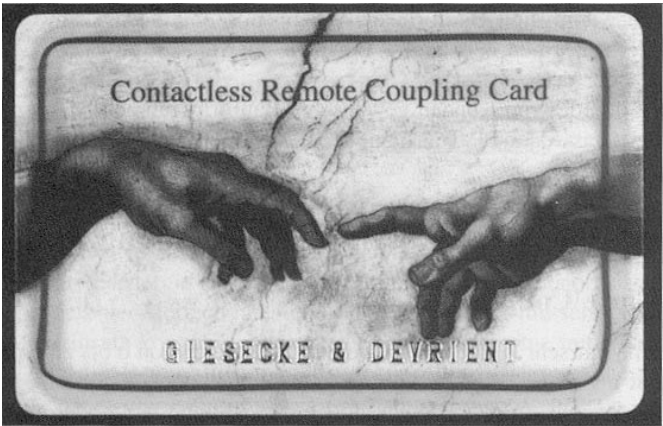


Figure 2.12 Semitransparent contactless smart card. The transponder antenna can be clearly seen along the edge of the card (reproduced by permission of Giesecke & Devrient, Munich)

Contactless smart cards of the design ID-1 are excellently suited for carrying adverts and often have artistic overprints, like those on telephone cards, for example (Figure 2.12).

However, it is not always possible to adhere to the maximum thickness of 0.8 mm specified for ID-1 cards in ISO 7810. Microwave transponders in particular require a thicker design, because in this design the transponder is usually inserted between two PVC shells or packed using an (ABS) injection moulding procedure (Figure 2.13).

2.2.8 Smart label

The term *smart label* refers to a paper-thin transponder format. In transponders of this format the transponder coil is applied to a plastic foil of just 0.1 mm thickness by *screen printing* or *etching*. This foil is often laminated using a layer of paper and its back coated with adhesive. The transponders are supplied in the form of self-adhesive stickers on an endless roll and are thin and flexible enough to be stuck to luggage, packages and goods of all types (Figures 2.14, 2.15). Since the *sticky labels* can easily



Figure 2.13 Microwave transponders in plastic shell housings (reproduced by permission of Pepperl & Fuchs GmbH)

be overprinted, it is a simple matter to link the stored data to an additional barcode on the front of the *label*.

2.2.9 Coil-on-chip

In the construction formats mentioned previously the transponders consist of a separate transponder coil that functions as an antenna and a transponder chip (hybrid technology). The transponder coil is bonded to the transponder chip in the conventional manner.



Figure 2.14 Smart label transponders are thin and flexible enough to be attached to luggage in the form of a self-adhesive label (reproduced by permission of i-code-Transponder, Philips Semiconductors, A-Gratkorn)

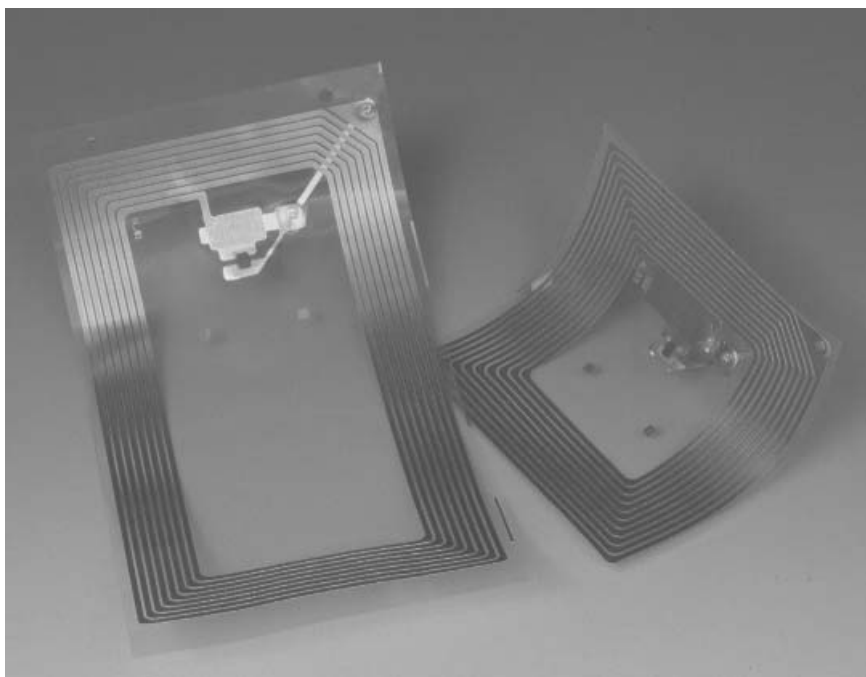


Figure 2.15 A smart label primarily consists of a thin paper or plastic foil onto which the transponder coil and transponder chip can be applied (Tag-It Transponder, reproduced by permission of Texas Instruments, Friesing)

An obvious step down the route of miniaturisation is the integration of the coil onto the chip (*coil-on-chip*) (Figure 2.16). This is made possible by a special microgalvanic process that can take place on a normal CMOS wafer. The coil is placed directly onto the isolator of the silicon chip in the form of a planar (single layer) spiral arrangement and contacted to the circuit below by means of conventional openings in the passivation layer (Jurisch, 1995, 1998). The conductor track widths achieved lie in the range of $5\text{--}10\text{ }\mu\text{m}$ with a layer thickness of $15\text{--}30\text{ }\mu\text{m}$. A final passivation onto a polyamide base is performed to guarantee the mechanical loading capacity of the contactless memory module based upon coil-on-chip technology.

The size of the silicon chip, and thus the entire transponder, is just $3\text{ mm} \times 3\text{ mm}$. The transponders are frequently embedded in a plastic shell for convenience and at $\varnothing 6\text{ mm} \times 1.5\text{ mm}$ are among the smallest RFID transponders available on the market.

2.2.10 Other formats

In addition to these main designs, several application-specific special designs are also manufactured. Examples are the ‘racing pigeon transponder’ or the ‘champion chip’ for sports timing. Transponders can be incorporated into any design required by the customer. The preferred options are glass or PP transponders, which are then processed further to obtain the ultimate form.

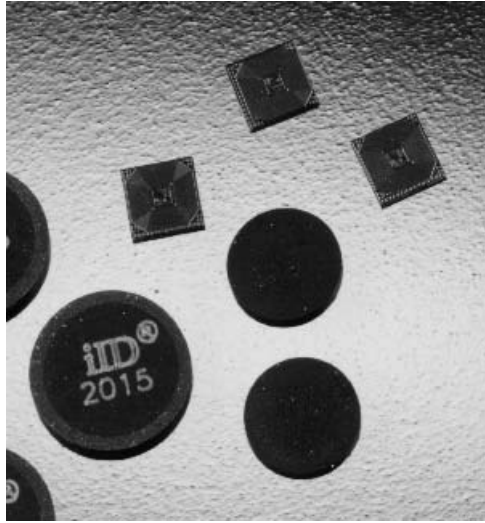


Figure 2.16 Extreme miniaturisation of transponders is possible using coil-on-chip technology (reproduced by permission of Micro Sensys, Erfurt)

2.3 Frequency, Range and Coupling

The most important differentiation criteria for RFID systems are the operating frequency of the reader, the physical coupling method and the range of the system. RFID systems are operated at widely differing frequencies, ranging from 135 kHz longwave to 5.8 GHz in the microwave range. *Electric*, *magnetic* and *electromagnetic fields* are used for the physical coupling. Finally, the achievable range of the system varies from a few millimetres to above 15 m.

RFID systems with a very small range, typically in the region of up to 1 cm, are known as *close coupling systems*. For operation the transponder must either be inserted into the reader or positioned upon a surface provided for this purpose. Close coupling systems are coupled using both electric and magnetic fields and can theoretically be operated at any desired frequency between DC and 30 MHz because the operation of the transponder does not rely upon the radiation of fields. The close coupling between data carrier and reader also facilitates the provision of greater amounts of power and so even a microprocessor with non-optimal power consumption, for example, can be operated. Close coupling systems are primarily used in applications that are subject to strict security requirements, but do not require a large range. Examples are electronic door locking systems or contactless smart card systems with payment functions. Close coupling transponders are currently used exclusively as ID-1 format contactless smart cards (ISO 10536). However, the role of close coupling systems on the market is becoming less important.

Systems with write and read ranges of up to 1 m are known by the collective term of remote coupling systems. Almost all *remote coupled systems* are based upon an *inductive (magnetic) coupling* between reader and transponder. These systems are therefore also known as *inductive radio systems*. In addition there are also a few systems with

capacitive (electric) coupling (motorola Inc., 1999). At least 90% of all RFID systems currently sold are inductively coupled systems. For this reason there is now an enormous number of such systems on the market. There is also a series of standards that specify the technical parameters of transponder and reader for various standard applications, such as contactless smart cards, animal identification or industrial automation. These also include *proximity coupling* (ISO 14443, *contactless smart cards*) and *vicinity coupling systems* (ISO 15693, *smart label* and contactless smart cards). Frequencies below 135 kHz or 13.56 MHz are used as transmission frequencies. Some special applications (e.g. Eurobalise) are also operated at 27.125 MHz.

RFID systems with ranges significantly above 1 m are known as *long-range systems*. All long-range systems operate using electromagnetic waves in the *UHF* and *microwave range*. The vast majority of such systems are also known as *backscatter systems* due to their physical operating principle. In addition, there are also long-range systems using *surface acoustic wave transponders* in the microwave range. All these systems are operated at the UHF frequencies of 868 MHz (Europe) and 915 MHz (USA) and at the microwave frequencies of 2.5 GHz and 5.8 GHz. Typical ranges of 3 m can now be achieved using passive (battery-free) backscatter transponders, while ranges of 15 m and above can even be achieved using active (battery-supported) backscatter transponders. The battery of an active transponder, however, never provides the power for data transmission between transponder and reader, but serves exclusively to supply the microchip and for the retention of stored data. The power of the electromagnetic field received from the reader is the only power used for the data transmission between transponder and reader.

In order to avoid reference to a possibly erroneous range figure, this book uses only the terms *inductively* or *capacitively coupled system* and *microwave system* or *backscatter system* for classification.

2.4 Information Processing in the Transponder

If we classify RFID systems according to the range of information and data processing functions offered by the transponder and the size of its data memory, we obtain a broad spectrum of variants. The extreme ends of this spectrum are represented by low-end and high-end systems (Figure 2.17).

2.4.1 Low-end systems

EAS systems (*Electronic Article Surveillance systems*; see Section 3.1) represent the bottom end of *low-end systems*. These systems check and monitor the possible presence of a transponder in the interrogation zone of a detection unit's reader using simple physical effects.

Read-only transponders with a microchip are also classified as low-end systems. These transponders have a permanently encoded data set that generally consists only of a unique *serial number* (unique number) made up of several bytes. If a read-only transponder is placed in the HF field of a reader, the transponder begins to continuously

The transmission frequency of the transponder corresponds with the resonant frequency of the transponder coil, which was adjusted to the transmission frequency of the reader when it was generated.

In order to be able to modulate the HF signal generated in the absence of a power supply, an additional modulation capacitor is connected in parallel with the resonant circuit in time with the data flow. The resulting frequency shift keying provides a 2 *FSK modulation*.

After all the data has been transmitted, the discharge mode is activated to fully discharge the charging capacitor. This guarantees a safe Power-On-Reset at the start of the next charging cycle.

3.3.2 Surface acoustic wave transponder

Surface acoustic wave (SAW) devices are based upon the piezoelectric effect and on the surface-related dispersion of elastic (=acoustic) waves at low speed. If an (ionic) crystal is elastically deformed in a certain direction, surface charges occur, giving rise to electric voltages in the crystal (application: piezo lighter). Conversely, the application of a surface charge to a crystal leads to an elastic deformation in the crystal grid (application: piezo buzzer). Surface acoustic wave devices are operated at microwave frequencies, normally in the ISM range 2.45 GHz.

Electroacoustic transducers (interdigital transducers) and *reflectors* can be created using planar electrode structures on piezoelectric substrates. The normal substrate used for this application is *lithium niobate* or *lithium tantalate*. The electrode structure is created by a photolithographic procedure, similar to the procedure used in microelectronics for the manufacture of integrated circuits.

Figure 3.30 illustrates the basic layout of a surface wave transponder. A finger-shaped electrode structure — the *interdigital transducer* — is positioned at the end of a long piezoelectrical substrate, and a suitable *dipole antenna* for the operating frequency is attached to its busbar. The interdigital transducer is used to convert between electrical signals and acoustic surface waves.

An electrical impulse applied to the busbar causes a mechanical deformation to the surface of the substrate due to the piezoelectrical effect between the electrodes (fingers), which disperses in both directions in the form of a surface wave (rayleigh wave). For a normal substrate the dispersion speed lies between 3000 and 4000 m/s. Similarly, a *surface wave* entering the converter creates an electrical impulse at the busbar of the interdigital transducer due to the piezoelectric effect.

Individual electrodes are positioned along the remaining length of the surface wave transponder. The edges of the electrodes form a reflective strip and reflect a small proportion of the incoming surface waves. Reflector strips are normally made of aluminium; however some reflector strips are also in the form of etched grooves (Meinke, 1992).

A high frequency *scanning pulse* generated by a reader is supplied from the dipole antenna of the transponder into the interdigital transducer and is thus converted into an acoustic surface wave, which flows through the substrate in the longitudinal direction. The frequency of the surface wave corresponds with the carrier frequency of the sampling pulse (e.g. 2.45 GHz) (Figure 3.31). The carrier frequency of the reflected

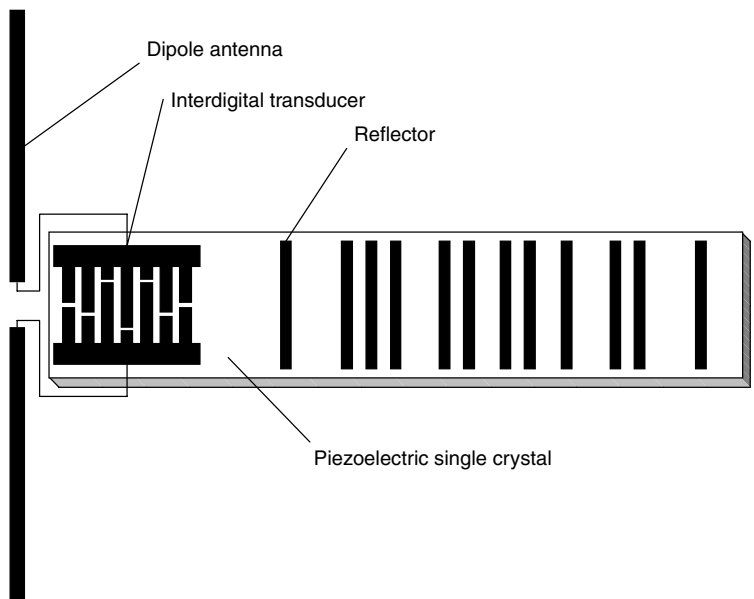


Figure 3.30 Basic layout of an SAW transponder. Interdigital transducers and reflectors are positioned on the piezoelectric crystal

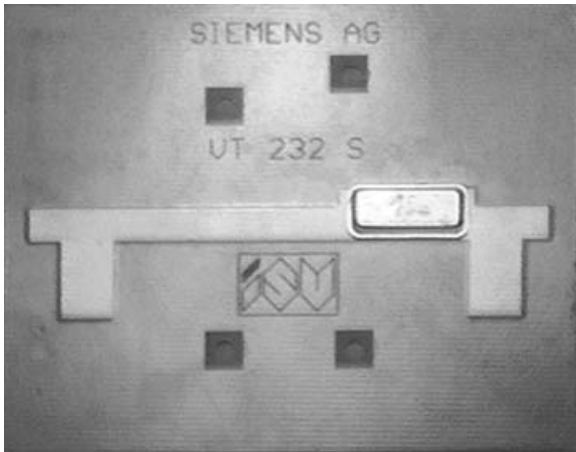


Figure 3.31 Surface acoustic wave transponder for the frequency range 2.45 GHz with antenna in the form of microstrip line. The piezocrystal itself is located in an additional metal housing to protect it against environmental influences (reproduced by permission of Siemens AG, ZT KM, Munich)

and returned pulse sequence thus corresponds with the transmission frequency of the sampling pulse.

Part of the surface wave is reflected off each of the reflective strips that are distributed across the substrate, while the remaining part of the surface wave continues to travel to the end of the substrate and is absorbed there.

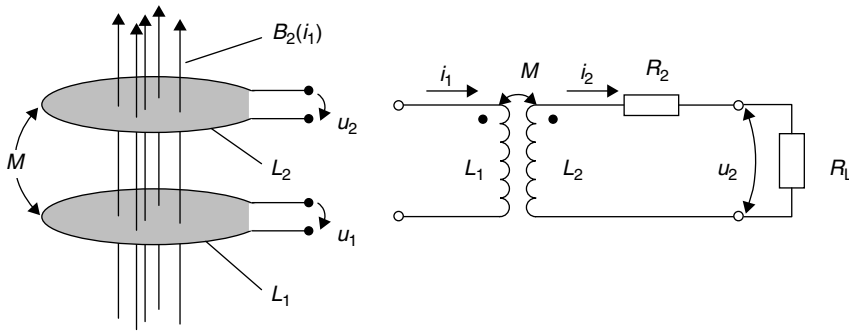


Figure 4.12 Left, magnetically coupled conductor loops; right, equivalent circuit diagram for magnetically coupled conductor loops

L_2 represents the antenna of the transponder, where R_2 is the *coil resistance* of the transponder antenna. The current consumption of the data memory is symbolised by the load resistor R_L .

A time varying flux in the conductor loop L_1 induces voltage u_{2i} in the conductor loop L_2 due to mutual inductance M . The flow of current creates an additional voltage drop across the coil resistance R_2 , meaning that the voltage u_2 can be measured at the terminals. The current through the load resistor R_L is calculated from the expression u_2/R_L . The current through L_2 also generates an additional magnetic flux, which opposes the magnetic flux $\Psi_1(i_1)$. The above is summed up in the following equation:

$$u_2 = + \frac{d\Psi_2}{dt} = M \frac{di_1}{dt} - L_2 \frac{di_2}{dt} - i_2 R_2 \quad (4.22)$$

Because, in practice, i_1 and i_2 are sinusoidal (HF) alternating currents, we write equation (4.22) in the more appropriate complex notation (where $\omega = 2\pi f$):

$$u_2 = j\omega M \cdot i_1 - j\omega L_2 \cdot i_2 - i_2 R_2 \quad (4.23)$$

If i_2 is replaced by u_2/R_L in equation (4.23), then we can solve the equation for u_2 :

$$u_2 = \frac{j\omega M \cdot i_1}{1 + \frac{j\omega L_2 + R_2}{R_L}} \begin{cases} \rightarrow R_L \rightarrow \infty: u_2 = j\omega M \cdot i_1 \\ \rightarrow R_L \rightarrow 0: u_2 \rightarrow 0 \end{cases} \quad (4.24)$$

4.1.7 Resonance

The voltage u_2 induced in the transponder coil is used to provide the power supply to the data memory (*microchip*) of a passive transponder (see Section 4.1.8.1). In order to significantly improve the efficiency of the equivalent circuit illustrated in Figure 4.12, an additional capacitor C_2 is connected in parallel with the transponder coil L_2 to form a *parallel resonant circuit* with a *resonant frequency* that corresponds with the

$$X_T = \text{Im} \left(\frac{1}{j\omega C_2 + \frac{1}{R_L} + \frac{1}{Z_{\text{mod}}}} \right) \quad (4.98)$$

4.2.6.2 Power supply of passive transponders

A passive transponder does not have its own *power supply* from an internal voltage source, such as a battery or solar cell. If the transponder is within range of the reader a voltage U_0 is induced in the transponder antenna by the field strength E that occurs at distance r . Part of this voltage is available at the terminals of the antenna as voltage U_T . Only this voltage U_T is rectified and is available to the transponder as supply voltage (rectenna) (Jurianto and Chia, n.d. a, b).

In the case of power matching between the radiation resistor R_r and the input impedance Z_T of the transponder, power $P_2 = P_e$ can be derived from equation (4.87). Figure 4.76 shows the power available in RFID systems at different distances at the

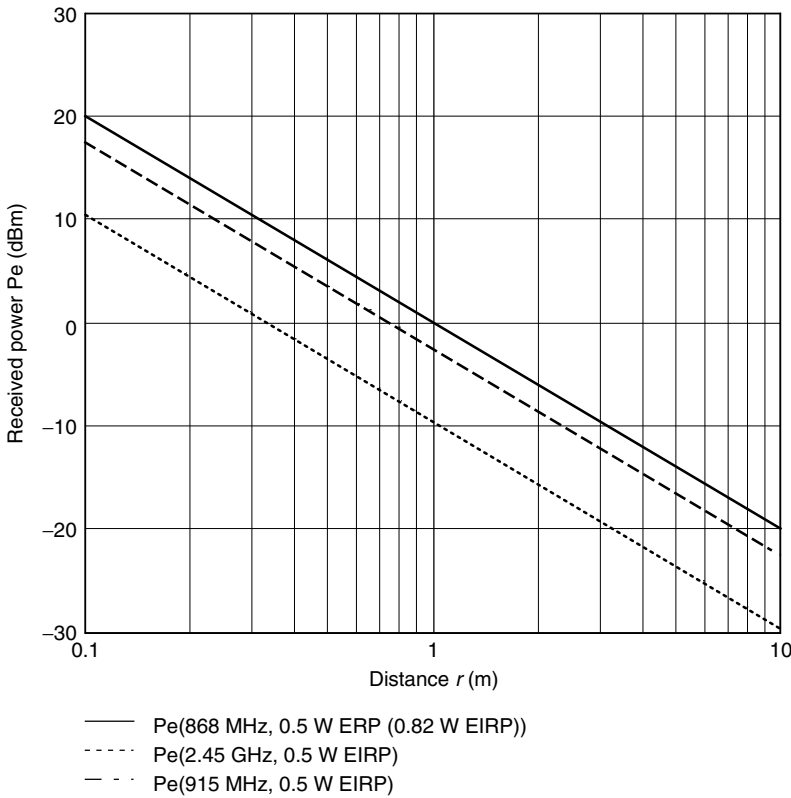


Figure 4.76 The maximum power P_e (0 dBm = 1 mW) available for the operation of the transponder, in the case of power matching at the distance r , using a dipole antenna at the transponder

reader's normal transmission power. In order to use this low power as effectively as possible a *Schottky detector* with *impedance matching* is typically used as a rectifier.

A *Schottky diode* consists of a metal–semiconductor sequence of layers. At the boundary layer there is, as in the p-n junction, a charge-free space-charge zone and a potential barrier that hinders charge transport. The current–voltage characteristic of the metal–semiconductor transition has a diode characteristic. Schottky diodes function as a rectifier at wavelengths below the microwave range since, unlike the pn diode, there are no inertia effects caused by minority carrier injection. Further advantages in comparison to pn diodes are the low voltage drop in the direction of flow and the low noise. A possible layout of a Schottky diode is shown in Figure 4.77 (Agilent Technologies, n.d.).

A Schottky diode can be represented by a linear *equivalent circuit* (Figure 4.77b). C_j represents the parasitic *junction capacitance* of the chip and R_s is the loss resistance in the terminals of the diode. R_j is the *junction resistor* of the diode, which can be calculated as follows (Agilent Technologies, n.d.):

$$R_j = \frac{8.33 \cdot 10^{-5} \cdot n \cdot T}{I_s + I_b} \quad (4.99)$$

where n is the ideality factor, T the temperature in Kelvin, I_s the saturation current and I_b the bias current through the Schottky diode.

By a suitable combination of the p- or n-doped semiconductor with the various metals the properties of the Schottky diode can be varied across a wide range. In RFID transponders primarily p-doped Schottky diodes are used, since these are particularly suitable for detectors with no zero bias in small signal operation, i.e. for the conditions that occur in every transponder (Hewlett Packard, 1988).

The circuit of a Schottky detector for voltage rectification is shown in Figure 4.78. Such a Schottky detector has different operating ranges. If it is driven at power above -10 dBm (0.1 mW) the Schottky detector lies in the range of *linear detection* (Hewlett Packard, 1986). Here there is *peak value rectification*, as is familiar from the field of power electronics. The following holds:

$$u_{\text{chip}} \sim \hat{u}_{\text{in}} \Rightarrow u_{\text{chip}} \sim \sqrt{P_{\text{in}}} \quad (4.100)$$

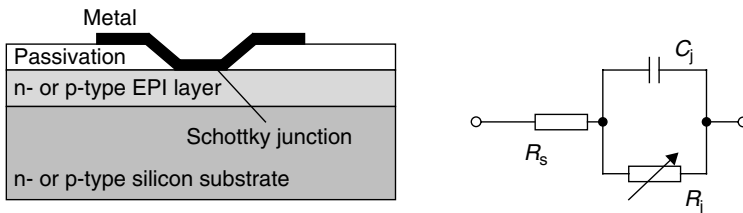


Figure 4.77 A Schottky diode is created by a metal–semiconductor junction. In small signal operation a Schottky diode can be represented by a linear equivalent circuit

10

The Architecture of Electronic Data Carriers

Before we describe the functionality of the data carriers used in RFID systems we must first differentiate between two fundamental operating principles: there are *electronic data carriers* based upon integrated circuits (*microchips*) and data carriers that exploit physical effects for data storage. Both 1-bit transponders and surface wave components belong to the latter category.

Electronic data carriers are further subdivided into data carriers with a pure memory function and those that incorporate a programmable microprocessor (Figure 10.1).

This chapter deals exclusively with the functionality of electronic data carriers. The simple functionality of physical data carriers has already been described in Chapter 3.

10.1 Transponder with Memory Function

Transponders with a memory function range from the simple *read-only transponder* to the *high end transponder* with intelligent cryptological functions (Figure 10.2).

Transponders with a memory function contain RAM, ROM, EEPROM or FRAM and an *HF interface* to provide the *power supply* and permit communication with the reader. The main distinguishing characteristic of this family of transponders is the realisation of address and security logic on the chip using a *state machine*.

10.1.1 HF interface

The HF interface forms the interface between the analogue, high frequency transmission channel from the reader to the transponder and the digital circuitry of the transponder. The HF interface therefore performs the functions of a classical modem (modulator–demodulator) used for analogue data transmission via telephone lines.

The modulated HF signal from the reader is reconstructed in the HF interface by *demodulation* to create a digital serial data stream for reprocessing in the address and security logic. A clock-pulse generation circuit generates the system clock for the data carrier from the carrier frequency of the HF field.

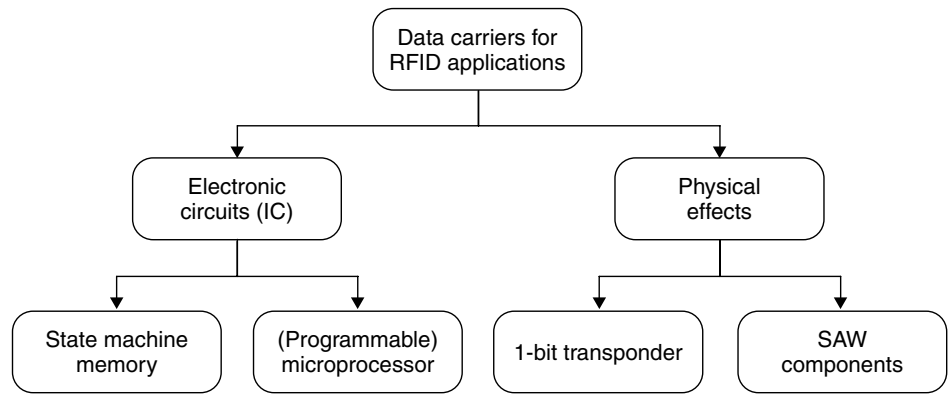


Figure 10.1 Overview of the different operating principles used in RFID data carriers

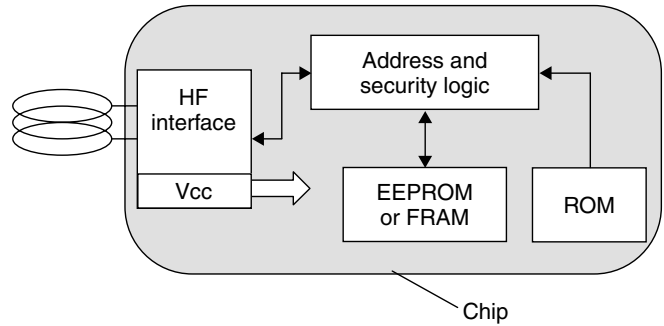


Figure 10.2 Block diagram of an RFID data carrier with a memory function

The HF interface incorporates a *load modulator* or *backscatter modulator* (or an alternative procedure, e.g. frequency divider), controlled by the digital data being transmitted, to return data to the reader (Figure 10.3).

Passive transponders, i.e. transponders that do not have their own power supply, are supplied with energy via the HF field of the reader. To achieve this, the HF interface draws current from the transponder antenna, which is rectified and supplied to the chip as a regulated supply voltage.

10.1.1.1 Example circuit – load modulation with subcarrier

The principal basic circuit of a load modulator is shown in Figure 10.4. This generates an ohmic load modulation using an ASK or FSK modulated *subcarrier*. The frequency of the subcarrier and the baud rates are in accordance with the specifications of the standard ISO 15693 (Vicinity coupling smart cards).

The high-frequency input voltage u_2 of the data carrier (transponder chip) serves as the time basis of the HF interface and is passed to the input of a binary divider.

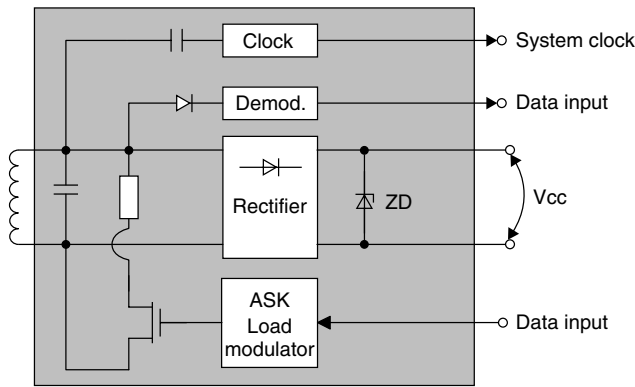


Figure 10.3 Block diagram of the HF interface of an inductively coupled transponder with a load modulator

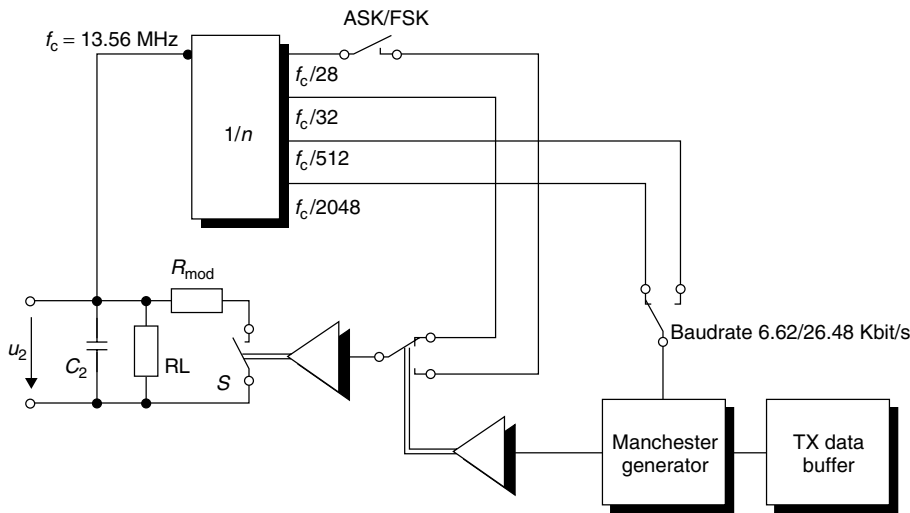


Figure 10.4 Generation of a load modulation with modulated subcarrier: the subcarrier frequency is generated by a binary division of the carrier frequency of the RFID system. The subcarrier signal itself is initially ASK or FSK modulated (switch position ASK/FSK) by the Manchester coded data stream, while the modulation resistor in the transponder is finally switched on and off in time with the modulated subcarrier signal

The frequencies specified in the standard for the subcarrier and the baud rate can be derived from the single binary division of the 13.56 MHz input signal (Table 10.1).

The serial data to be transmitted is first transferred to a Manchester generator. This allows the baud rate of the baseband signal to be adjusted between two values. The Manchester coded baseband signal is now used to switch between the two subcarrier frequencies f_1 and f_2 using the ‘1’ and ‘0’ levels of the signal, in order to generate an FSK modulated subcarrier signal. If the clock signal f_2 is interrupted, this results in an ASK modulated subcarrier signal, which means that it is very simple to switch

Table 10.1 The clock frequencies required in the HF interface are generated by the binary division of the 13.56 MHz carrier signal

Splitter N	Frequency	Use
1/28	485 kHz	$\phi 2$ of the FSK subcarrier
1/32	423 kHz	$\phi 1$ of the FSK subcarrier, plus ASK subcarrier
1/512	26.48 kHz	Bit clock signal for high baud rate
1/2048	6.62 kHz	Bit clock signal for slow baud rate

between ASK and FSK modulation. The modulated subcarrier signal is now transferred to switch S , so that the *modulation resistor* of the load modulator can be switched on and off in time with the subcarrier frequency.

10.1.1.2 Example circuit – HF interface for ISO 14443 transponder

The circuit in Figure 10.5 provides a further example of the layout of a HF interface. This was originally a simulator for contactless smart cards in accordance with ISO 14443, which can be used to simulate the data transmission from the smart card to a reader by load modulation. The circuit was taken from a proposal by Motorola for a contactless smart card in ISO 10373-6 (Baddeley and Ruiz, 1998).

A complete layout is available for the duplication of this test card (see Section 14.4.1). The circuit is built upon an FR4 printed circuit board. The transponder coil is realised in the form of a large area conductor loop with four windings of a printed conductor. The dimensions of the transponder coil correspond with the ratios in a real smart card.

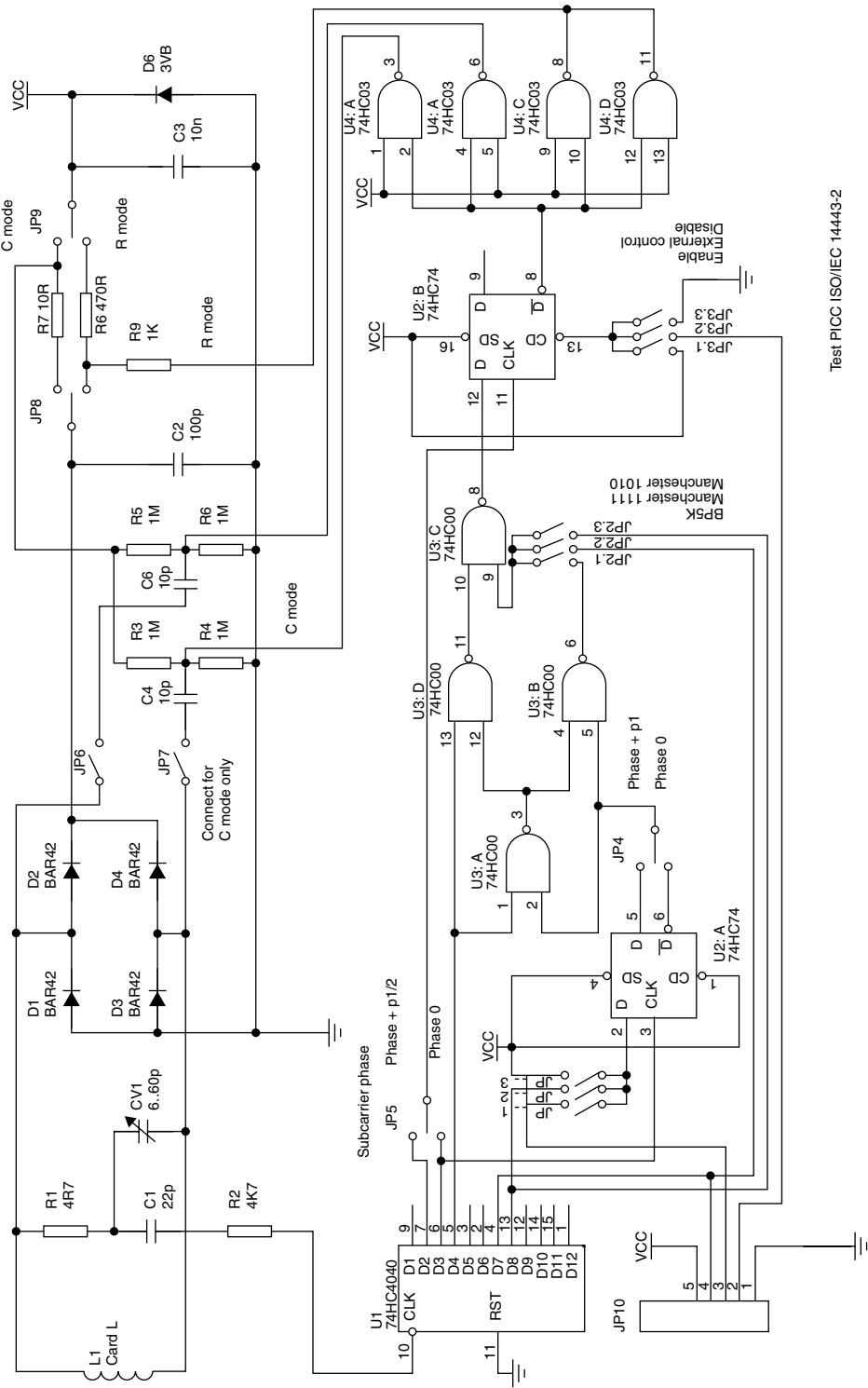
The *transponder resonant circuit* of the test card is made up of the transponder coil L_1 and the trimming capacitor CV_1 . The resonant frequency of the transponder resonant circuit should be tuned to the transmission frequency of the reader, 13.56 MHz (compare Section 4.1.11.2). The HF voltage present at the transponder resonant circuit is rectified in the bridge rectifier $D_1–D_4$ and maintained at approximately 3 V by the zener diode D_6 for the power supply to the test card.

The binary divider U_1 derives the required system clocks of 847.5 kHz (subcarrier, divider 1/16) and 105.93 kHz (baud rate, divider 1/128) from the carrier frequency 13.56 MHz.

The circuit made up of U_2 and U_3 is used for the ASK or BPSK modulation of the subcarrier signal (847.5 kHz) with the Manchester or NRZ coded data stream (jumper 1–4). In addition to the simple infinite bit sequences 1111 and 1010, the supply of an external data stream (jumper 10) is also possible. The test smart card thus supports both procedures for data transfer between smart card and reader defined in ISO 14443-2.

Either a capacitive (C_4 , C_5) or an ohmic (R_9) load modulation can be selected. The ‘open collector’ driver U_4 serves as the output stage (‘switch’) for the load modulator.

The *demodulation* of a data stream transmitted from the reader is not provided in this circuit. However, a very simple extension of the circuit (see Figure 10.6) facilitates the demodulation of at least a 100% ASK modulated signal. This requires only an



Test PICC ISO/IEC 14443-2

Figure 10.5 Example circuit of a HF interface in accordance with ISO 14443

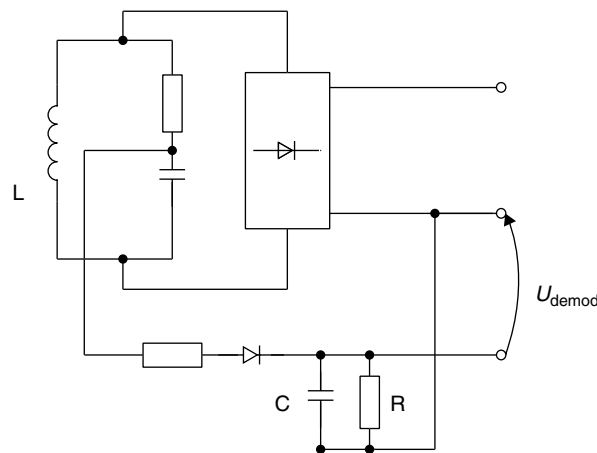


Figure 10.6 A 100% ASK modulation can be simply demodulated by an additional diode

additional diode to rectify the HF voltage of the transponder resonant circuit. The time constant $\tau = R \cdot C$ should be dimensioned such that the carrier frequency (13.56 MHz) is still effectively filtered out, but the modulation pulse ($t_{\text{pulse}} = 3 \mu\text{s}$ in accordance with ISO 14443-2) is retained as far as is possible.

10.1.2 Address and security logic

The *address and security logic* forms the heart of the data carrier and controls all processes on the chip (Figure 10.7).

The *power on logic* ensures that the data carrier takes on a defined state as soon as it receives an adequate power supply upon entering the HF field of a reader. Special I/O registers perform the data exchange with the reader. An optional *cryptological unit* is required for authentication, data encryption and key administration.

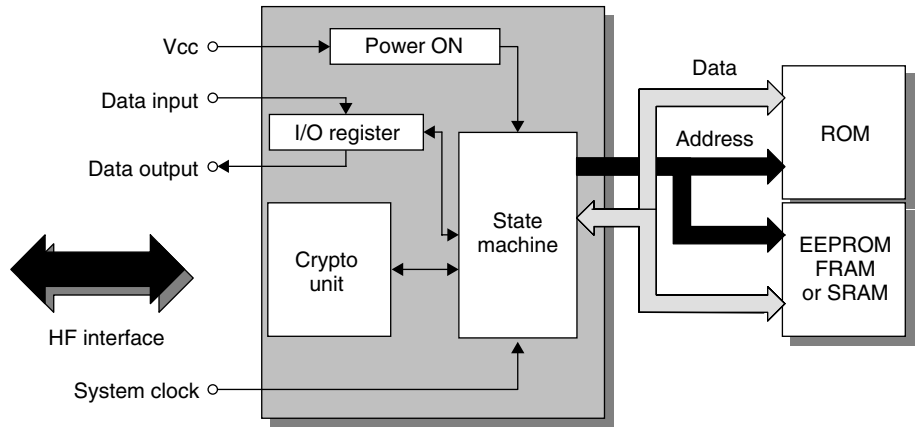


Figure 10.7 Block diagram of address and security logic module

The data memory, which comprises a ROM for permanent data such as serial numbers, and EEPROM or FRAM is connected to the address and security logic via the address and data bus inside the chip.

The *system clock* required for sequence control and system synchronisation is derived from the HF field by the HF interface and supplied to the address and security logic module. The state-dependent control of all procedures is performed by a state machine ('hard-wired software'). The complexity that can be achieved using state machines comfortably equals the performance of microprocessors (high end transponders). However the 'programme sequence' of these machines is determined by the chip design. The functionality can only be changed or modified by modifying the chip design and this type of arrangement is thus only of interest for very large production runs.

10.1.2.1 State machine

A *state machine* (also switching device, Mealy machine) is an arrangement used for executing logic operations, which also has the capability of storing variable states (Figure 10.8). The output variable Y depends upon both the input variable X and what has gone before, which is represented by the switching state of flip-flops (Tietze and Schenk, 1985).

The state machine therefore passes through different states, which can be clearly represented in a *state diagram* (Figure 10.9). Each possible state S_Z of the system is represented by a circle. The transition from this state into another is represented by an arrow. The arrow caption indicates the conditions that the transition takes place under. An arrow with no caption indicates an unspecified transition (power on $\rightarrow S_1$). The current new state $S_Z(t + 1)$ is determined primarily by the old state $S_Z(t)$ and, secondly, by the input variable x_i .

The order in which the states occur may be influenced by the input variable x . If the system is in state S_Z and the transition conditions that could cause it to leave this state are not fulfilled, the system remains in this state.

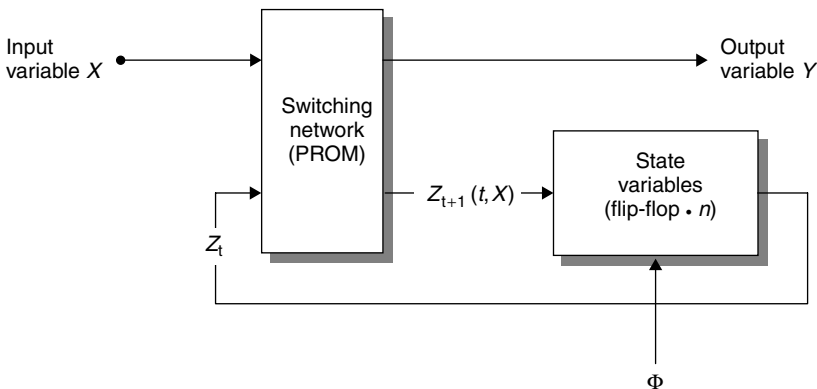


Figure 10.8 Block diagram of a state machine, consisting of the state memory and a backcoupled switching network

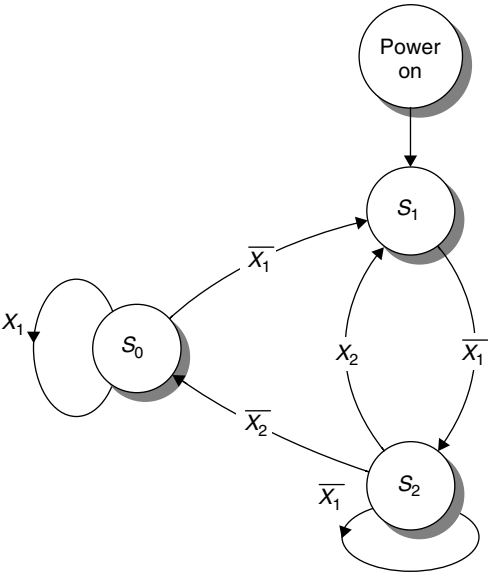


Figure 10.9 Example of a simple state diagram to describe a state machine

A switching network performs the required classification: If the state variable $Z(t)$ and the input variable are fed into its inputs, then the new state $Z(t + 1)$ will occur at the output (Figure 10.8). When the next timing signal is received this state is transferred to the output of (transition triggered) flip-flops and thus becomes the new system state $S(t + 1)$ of the state machine.

10.1.3 Memory architecture

10.1.3.1 Read-only transponder

This type of transponder represents the low-end, low-cost segment of the range of RFID data carriers. As soon as a *read-only transponder* enters the interrogation zone of a reader it begins to continuously transmit its own identification number (Figure 10.10). This identification number is normally a simple *serial number* of a few bytes with a check digit attached. Normally, the chip manufacturer guarantees that each serial number is only used once. More complex codes are also possible for special functions.

The transponder’s unique identification number is incorporated into the transponder during chip manufacture. The user cannot alter this serial number, nor any data on the chip.

Communication with the reader is unidirectional, with the transponder sending its identification number to the reader continuously. Data transmission from the reader to the transponder is not possible. However, because of the simple layout of the data carrier and reader, read-only transponders can be manufactured extremely cheaply.

Read-only transponders are used in price-sensitive applications that do not require the option of storing data in the transponder. The classic fields of application are

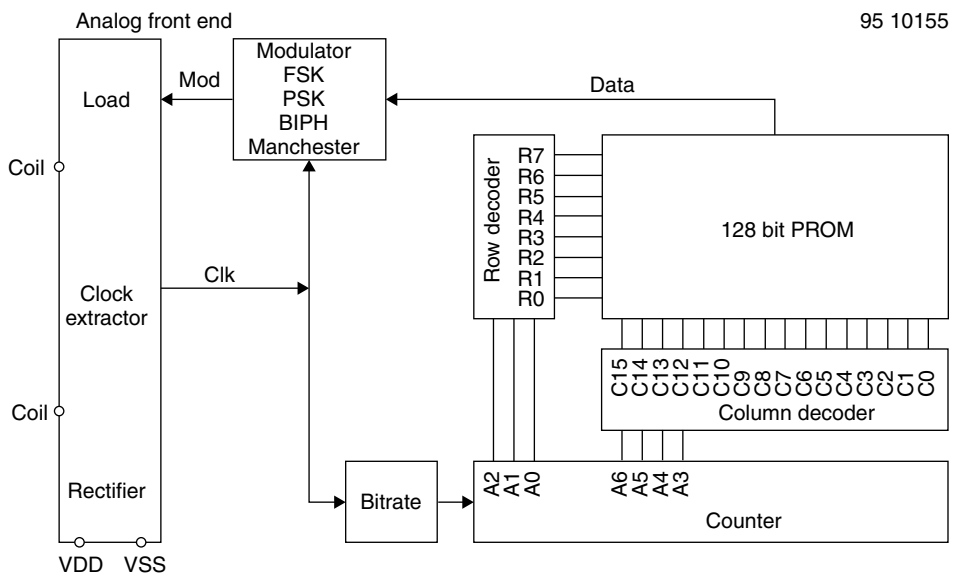


Figure 10.10 Block diagram of a read-only transponder. When the transponder enters the interrogation zone of a reader a counter begins to interrogate all addresses of the internal memory (PROM) sequentially. The data output of the memory is connected to a load modulator which is set to the baseband code of the binary code (modulator). In this manner the entire content of the memory (128-bit serial number) can be emitted cyclically as a serial data stream (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

therefore animal identification, access control and industrial automation with central data management.

A low-cost transponder chip is shown in Figure 10.11.

10.1.3.2 Writable transponder

Transponders that can be written with data by the reader are available with memory sizes ranging from just 1 byte (‘pigeon transponder’) to 64 Kbytes (microwave transponders with SRAM).

Write and read access to the transponder is often in blocks. Where this is the case, a block is formed by assembling a predefined number of bytes, which can then be read or written as a single unit. To change the data content of an individual block, the entire block must first be read from the transponder, after which the same block, including the modified bytes, can be written back to the transponder.

Current systems use block sizes of 16 bits, 4 bytes or 16 bytes. The *block structure* of the memory facilitates simple addressing in the chip and by the reader.

10.1.3.3 Transponder with cryptological function

If a writable transponder is not protected in some way, any reader that is part of the same RFID system can read from it, or write to it. This is not always desirable, because

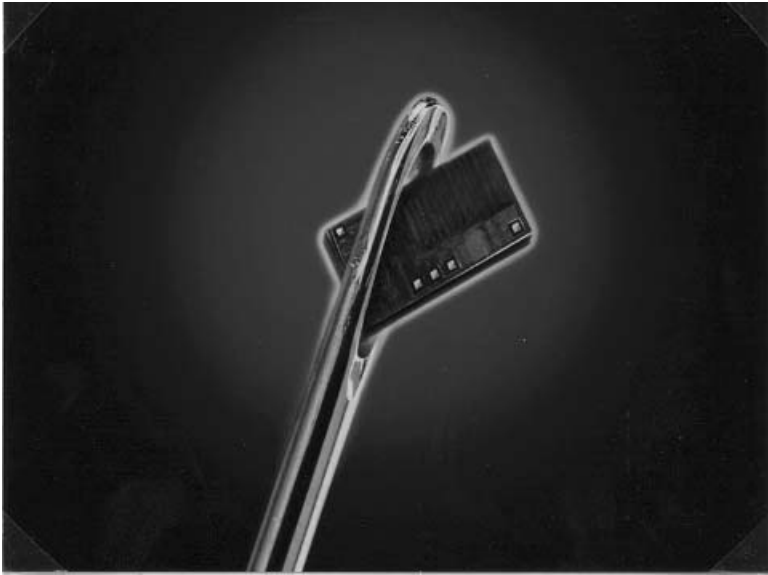


Figure 10.11 Size comparison: low-cost transponder chip in the eye of a needle (reproduced by permission of Philips Electronics N.V.)

sensitive applications may be impaired by unauthorised reading or writing of data in the transponder. Two examples of such applications are the contactless cards used as tickets in the public transport system and transponders in vehicle keys for electronic immobilisation systems.

There are various procedures for preventing unauthorised access to a transponder. One of the simplest mechanisms is read and write protection by checking a *password*. In this procedure, the card compares the transmitted password with a stored reference password and permits access to the data memory if the passwords correspond.

However, if mutual authorisation is to be sought or it is necessary to check that both components belong to the same application, then authentication procedures are used. Fundamentally, an *authentication procedure* always involves a comparison of two secret *keys*, which are not transmitted via the interface. (A detailed description of such procedures can be found in Chapter 8). Cryptological authentication is usually associated with the encryption of the data stream to be transmitted (Figure 10.12). This provides an effective protection against attempts to eavesdrop into the data transmission by monitoring the wireless transponder interface using a radio receiver.

In addition to the memory area allocated to application data, transponders with cryptological functions always have an additional memory area for the storage of the secret key and a *configuration register* (*access register*, Acc) for selectively write protecting selected address areas. The secret key is written to the *key memory* by the manufacturer before the transponder is supplied to the user. For security reasons, the key memory can never be read.

Hierarchical key concept Some systems provide the option of storing two separate keys — key A and key B — that give different access rights. The authentication between transponder and reader may take place using key A or key B. The option of

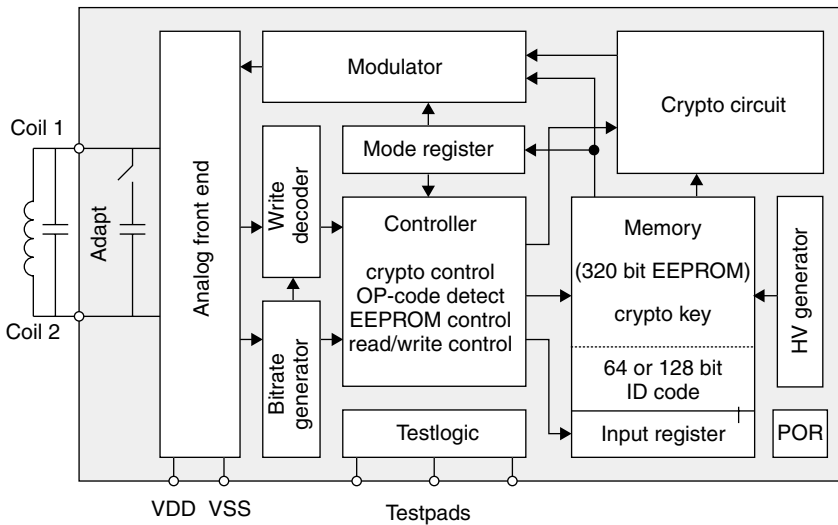


Figure 10.12 Block diagram of a writable transponder with a cryptological function to perform authentication between transponder and reader (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

allocating different *access rights* (Acc) to the two keys may therefore be exploited in order to define hierarchical security levels in an application.

Figure 10.13 illustrates this principle for clarification. The transponder incorporates two key memories, which are initialised by the two keys A and B. The access rights that the readers are allocated after successful authentication depends upon the setting that has been selected in the transponder (access register) for the key that has been used.

Reader 1 is only in possession of key A. After successful authentication, the selected settings in the access register (Acc) only permit it to read from the transponder memory. Reader 2, on the other hand, is in possession of key B. After successful authentication using key B, the settings selected in the access register (Acc) permit it to write to the transponder memory as well as reading from it.

Sample application — hierarchical key Let us now consider the system of travel passes used by a public transport network as an example of the practical use of *hierarchical keys*. We can differentiate between two groups of readers: the ‘devaluers’ for fare payments and the ‘revaluers’ which revalue the contactless smart cards.

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.

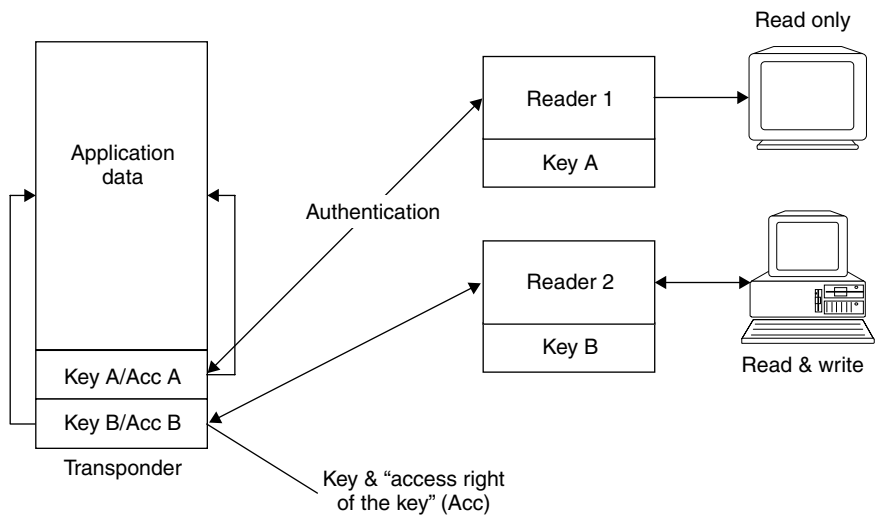


Figure 10.13 A transponder with two key memories facilitates the hierarchical allocation of access rights, in connection with the authentication keys used

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 10.14).

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 on the transponder is wasted 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 (Figure 10.15). In this approach, the memory allocated to a segment can be matched to

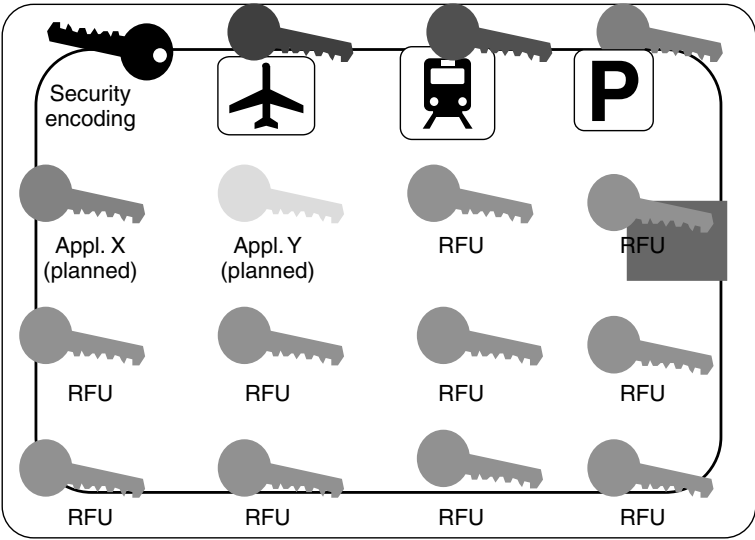


Figure 10.14 Several applications on one transponder — each protected by its own secret key

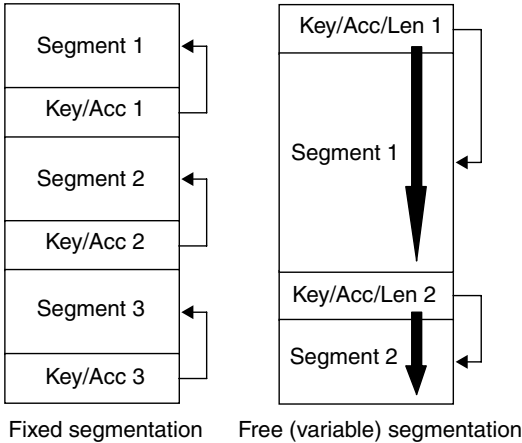


Figure 10.15 Differentiation between fixed segmentation and free segmentation

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 10.16 illustrates the memory configuration of a transponder with fixed segmentation. The available memory, totalling 128 bytes, is divided into four segments, known as ‘pages’. Each of the four segments can be protected against unauthorised reading or writing by its own password. The access register of this transponder (‘OTP write protection’) consists of an additional memory area of 16 bits per segment. Deleting a single bit from the access register permanently protects 16 bits of the application memory against overwriting.

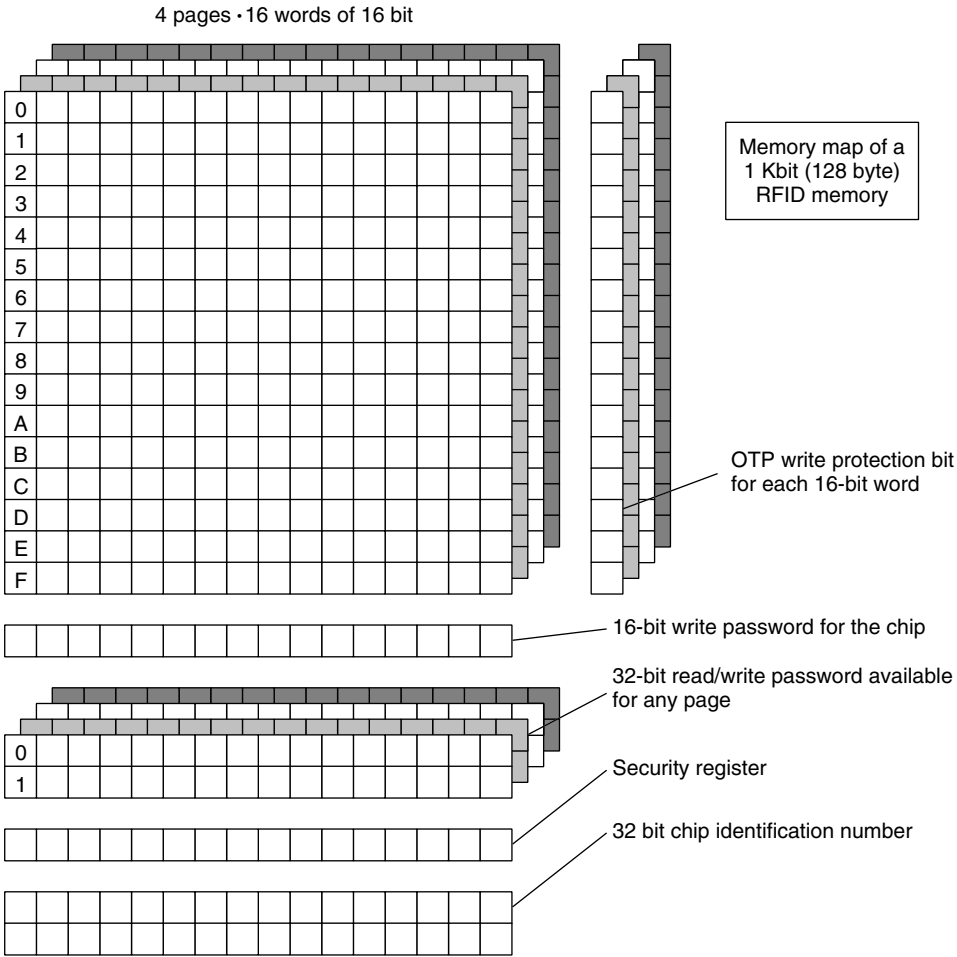


Figure 10.16 Example of a transponder with fixed segmentation of the memory (IDESCO MICROLOG®) The four ‘pages’ can be protected against unauthorised reading or writing using different passwords (IDESCO, n.d.)

10.1.3.5 MIFARE® application directory

The memory of a *MIFARE® transponder* is divided into 16 independent segments, known as sectors. Each sector is protected against unauthorised access by two different keys (hierarchical structure). Different access rights can be allocated to each of the two keys in its own access register (config.). Thus, 16 independent *applications* that are protected from each other by secret keys can be loaded onto the transponder (Figure 10.17). None of the applications can be read without the secret key, not even for checking or identification. So it is not even possible to determine what applications are stored on the transponder.

Let us now assume that the city of Munich has decided to issue a contactless City-Card, which citizens can use to avail themselves of city services, and which occupies

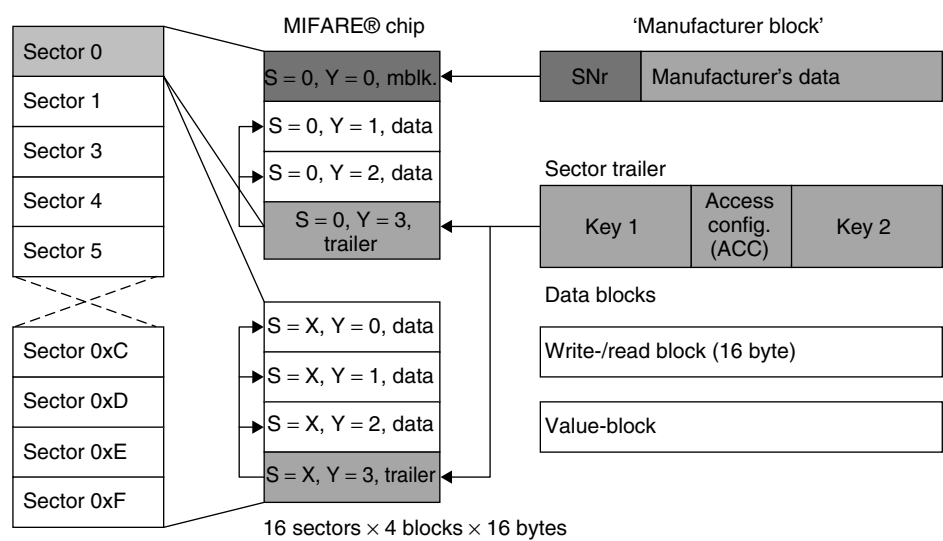


Figure 10.17 Memory configuration of a MIFARE® data carrier. The entire memory is divided into 16 independent sectors. Thus a maximum of separate 16 applications can be loaded onto a MIFARE® card

only a small part of the available memory on the card. The remaining memory units on the card could be used by other service providers for their own applications, such as local transport tickets, car rental, filling station cards, parking passes, bonus cards for restaurants and supermarket chains, and many others. However, we cannot find out which of the many possible applications are currently available on the card, because each reader belonging to an application only has access to its own sector, for which it also has the correct key.

To get around this problem, the author, in conjunction with Philips Semiconductors Gratkorn (was Mikron), has developed an *application directory* for the MIFARE® smart card. Figures 10.18 and 10.19 illustrate the data structure of this directory, the *MAD* (MIFARE® application directory).

Blocks 1 and 2 of sector 0 are reserved for the MAD, leaving 32 bytes available for the application directory. Two bytes of each make up a pointer, ID1 to ID\$F, to one of the remaining 15 sectors. Reading the content of the pointer yields 2 bytes, the *function cluster* and the *application code*, which can be used to look the application up in an external database. Even if the application we are looking for is not registered in the available database, we can still gain an approximate classification from the function cluster, for example 'airlines', 'railway services', 'bus services', 'city card services', 'ski ticketing', 'car parking', etc.

Each application is allocated a unique identification number, made up of the function cluster code and application code. It is possible to request an identification number from the developer of MIFARE® technology, Philips Semiconductors Gratkorn (Mikron) at Graz.

If a function cluster is set at 00h, then this is an *administration code* for the management of free or reserved sectors.

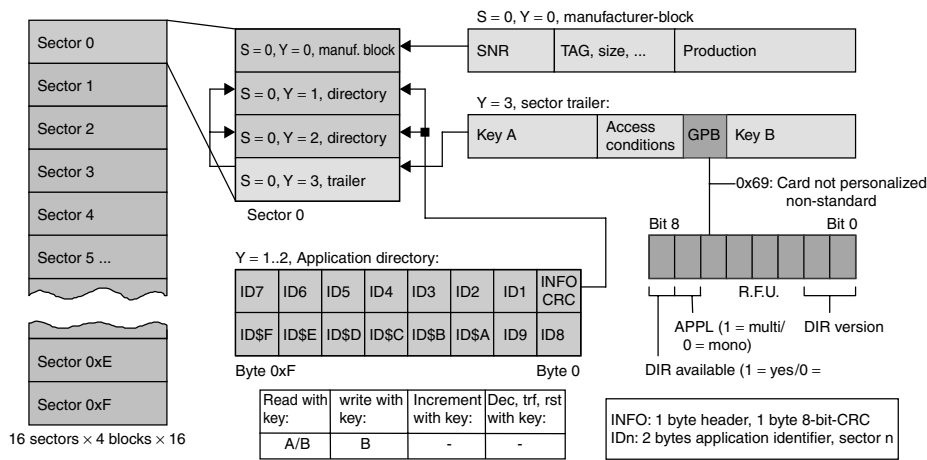


Figure 10.18 The data structure of the MIFARE® application directory consists of an arrangement of 15 pointers (ID1 to ID\$F), which point to the subsequent sectors

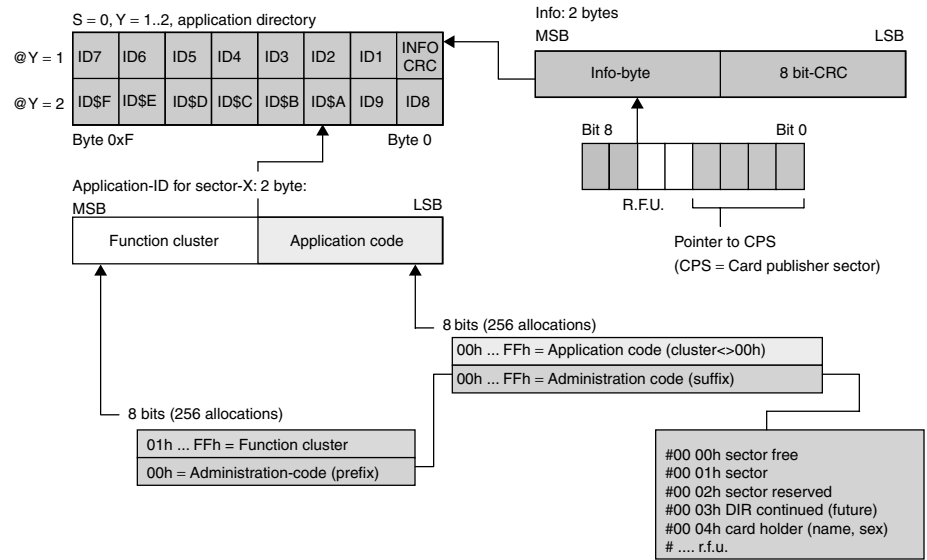


Figure 10.19 Data structure of the MIFARE® application directory: it is possible to find out what applications are located in each sector from the contents of the 15 pointers (ID1 to ID\$F)

Sector 0 itself does not require an ID pointer, because the MAD itself is stored in sector 0. The 2 bytes that this leaves free are used to store an 8-bit CRC, which is used to check the MAD structure for errors, and an info byte. A note can be recorded in the lowest 4 bits of the info byte, giving the sector ID of the card publisher. In our example, this would be the sector ID of one of the sectors in which the data belonging to the city of Munich is stored. This allows the reader to determine the card publisher, even if more than one application is recorded on the smart card.

Another special feature is MAD’s key management system. While key A, which is required for reading the MAD, is published, key B, which is required for recording further applications, is managed by the card publisher. This means that joint use of the card by a secondary service provider is only possible after a joint use contract has been concluded and the appropriate key issued.

10.1.3.6 Dual port EEPROM

EEPROM modules with a serial I^2C (IIC) bus interface established themselves years ago, particularly in consumer electronics. I^2C bus is the abbreviation for Inter IC bus, because originally it was developed for the connection of microprocessors and other ICs on a common printed circuit board. The I^2C bus is a serial bus and requires only two bidirectional lines, SDA (Serial Data) and SCL (Serial Clock). A serial EEPROM can be read or written by the transmission of defined commands via the two lines of the I^2C bus.

Some of these serial EEPROM modules now also have an HF interface and can thus be read or written either via the two SDA and SCL lines or via the contactless interface. The block diagram of such a dual port EEPROM (Atmel, 1998) is shown in Figure 10.20.

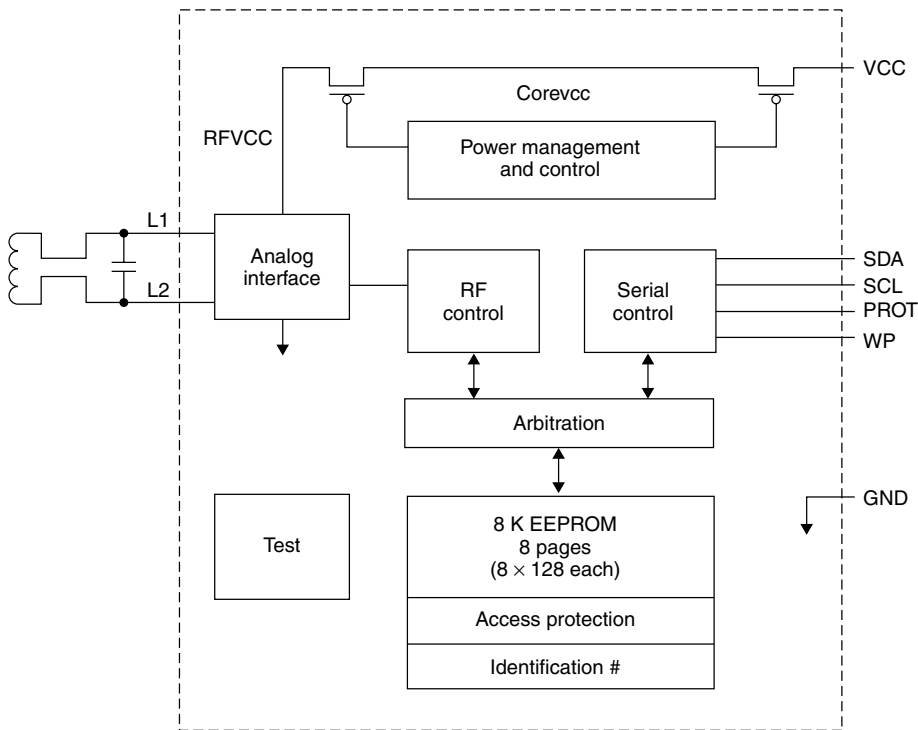


Figure 10.20 Block diagram of a dual port EEPROM. The memory can be addressed either via the contactless HF interface or an IIC bus interface (reproduced by permission of Atmel Corporation, San Jose, USA)

The EEPROM is accessed via two state machines ('RF control' and 'serial control') that are largely independent of each other. The additional arbitration logic prevents conflicts as a result of simultaneous access to the EEPROM via the HF and serial interfaces by simply blocking access to the other interface for the duration of a write or read operation.

The HF interface of the module is designed for inductive coupling in the frequency range of 125 kHz. If no supply voltage is available via the V_{cc} pin of the module, then the dual port EEPROM can also be supplied with power entirely via the HF interface. The integral power management simply switches off parts of the circuit that are not required in pure contactless operation. The data transfer from the serial EEPROM to a contactless reader takes place by ohmic load modulation in the baseband. Commands from a reader are transferred to the dual port EEPROM by a simple ASK modulation (modulation index $m > 10\%$). See Figures 10.21 and 10.22 for the pin assignment and memory configuration.

The total memory space of 1 Kbyte (8 Kbit) available on the dual port EEPROM was divided into eight segments (blocks 0–7). Each of these eight blocks was subdivided into eight subsegments (pages 0–7), each of 16 bytes. An additional 16 bytes are available as an *access protection page*. The structure of the access protection page is shown in Figure 10.23. The access protection page permits different access rights to the eight blocks of the EEPROM to be set independently of each other for the I²C bus and the HF interface. However, read and write access to the access protection page itself is only possible via the I²C bus interface.

The access rights of the HF interface on memory block Y are defined in the bits RF_Y of the access protection page (e.g. RF_7 contains the access rights on block 7) (Table 10.2). In a similar manner, the access rights of the I²C bus interface are defined on a memory block Y in the bit PB_Y of the access protection page (PB_5 contains access rights on block 5).

Furthermore, block 0 permits the access rights of the individual 16 byte pages of the block to be set independently of each other. Bits WP_7 – WP_0 of the access protection page serve this purpose.

A peculiarity is the tamper bit in the access protection page. This bit can be set only to '1' by the HF interface and only to '0' by the I²C bus interface. In this manner a previous write or read access of the EEPROM via the HF interface can be signalled to the master of the connected I²C bus.

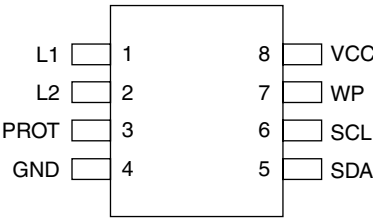


Figure 10.21 Pin assignment of a dual port EEPROM. The transponder coil is contacted to pins L_1 and L_2 . All other pins of the module are reserved for connection to the I²C bus and for the power supply in 'contact mode' (reproduced by permission of Atmel Corporation, San Jose, USA)

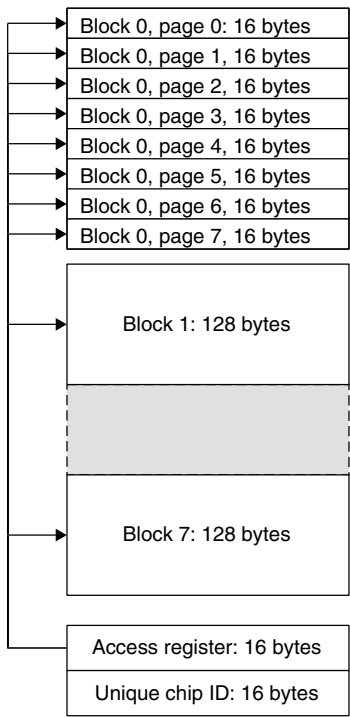


Figure 10.22 Memory configuration of the AT24RF08. The available memory of 1 Kbyte is split into 16 segments (blocks 0–7) of 128 bytes each. An additional memory of 32 bytes contains the access protection page and the unique serial numbers. The access protection page permits different access rights to be set in the memory for the HF and I²C bus interface

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0	
SB0		RF0				PB0		Addr 0
SB1		RF1				PB1		Addr 1
SB2		RF2				PB2		Addr 2
SB3		RF3				PB3		Addr 3
SB4		RF4				PB4		Addr 4
SB5		RF5				PB5		Addr 5
SB6		RF6				PB6		Addr 6
SB7		RF7				PB7		Addr 7
SBAP						PBAP		Addr 8
WP7	WP6	WP5	WP4	WP3	WP2	WP1	WP0	Addr 9
DE	DC						Tamper	Addr A
Reserved								Addr B
Reserved								Addr C
Reserved								Addr D
Reserved								Addr E
Chip-revision								Addr F

Figure 10.23 The access configuration matrix of the module AT24RF08 facilitates the independent setting of access rights to the blocks 0–7

Table 10.2 Setting options for the access rights of the HF interface to individual memory blocks in the bits $RF_0 - RF_7$ of the access protection page

MSB	LSB	Access rights via HF interface
0	0	No access to EEPROM
0	1	No access to EEPROM
1	0	Read access to EEPROM only
1	1	No restrictions

10.2 Microprocessors

Transponders with *microprocessors* will become increasingly common in applications using contactless smart cards in the near future. Instead of the inflexible state machine, the transponder in these cards incorporates a microprocessor.

Industry standard microprocessors, such as the familiar 8051 or 6805, are used as the microprocessor at the heart of the chip. In addition, some manufacturers are offering simple mathematical coprocessors (cryptological unit) on the same chip, which permit the rapid performance of the calculations required for encryption procedures (Figure 10.24).

Contactless smart cards with microprocessors incorporate their own *operating system*, as has long been the case in contact-based cards. The tasks of the operating system in a contactless smart card are data transfer from and to the smart card, command sequence control, file management and the execution of cryptographic algorithms (e.g. encryption, authentication).

The programme modules are written in ROM code and are incorporated into the chip at the chip manufacturing stage by an additional exposure mask (mask programming).

The typical command processing sequence within a smart card operating system is as follows: commands sent from the reader to the contactless smart card are received by the smart card via the HF interface. Error recognition and correction mechanisms are performed by the I/O manager irrespective of higher-level procedures. An error-free command received by the secure messaging manager is decrypted or checked for integrity. After decryption the higher-level command interpreter attempts to decode

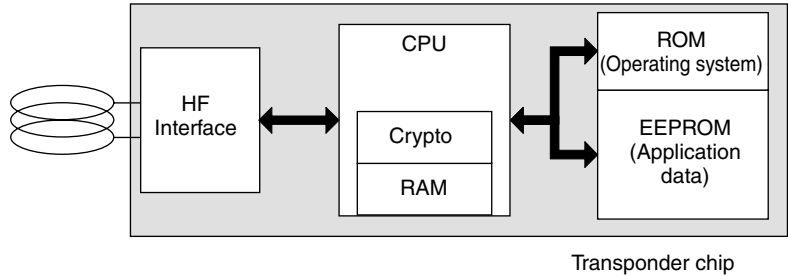


Figure 10.24 Block diagram of a transponder with a microprocessor. The microprocessor contains a coprocessor (cryptological unit) for the rapid calculation of the cryptological algorithms required for authentication or data encryption

the command. If this is not possible, then the return code manager is called, which generates the appropriate return code and sends it back to the reader via the I/O manager (Figure 10.25).

If a valid command is received, then the actual programme code associated with this application command is executed. If access to the application data in the EEPROM is necessary, this is performed exclusively by the file management system and the memory manager, which convert all symbolic addresses into the corresponding physical addresses of the memory area. The file manager also checks access conditions (authorisation) for the data in question.

A more detailed introduction to the procedures for the development of operating systems and smart card applications can be found in the book *The Smart Card Handbook* published by John Wiley & Sons.

10.2.1 Dual interface card

The traditional key markets for *contact smart cards* are *payment* applications (cash card, electronic purse) and *mobile telephones* (SIM card for GSM mobile telephone), applications that necessitate a high degree of security in the processing and transmission

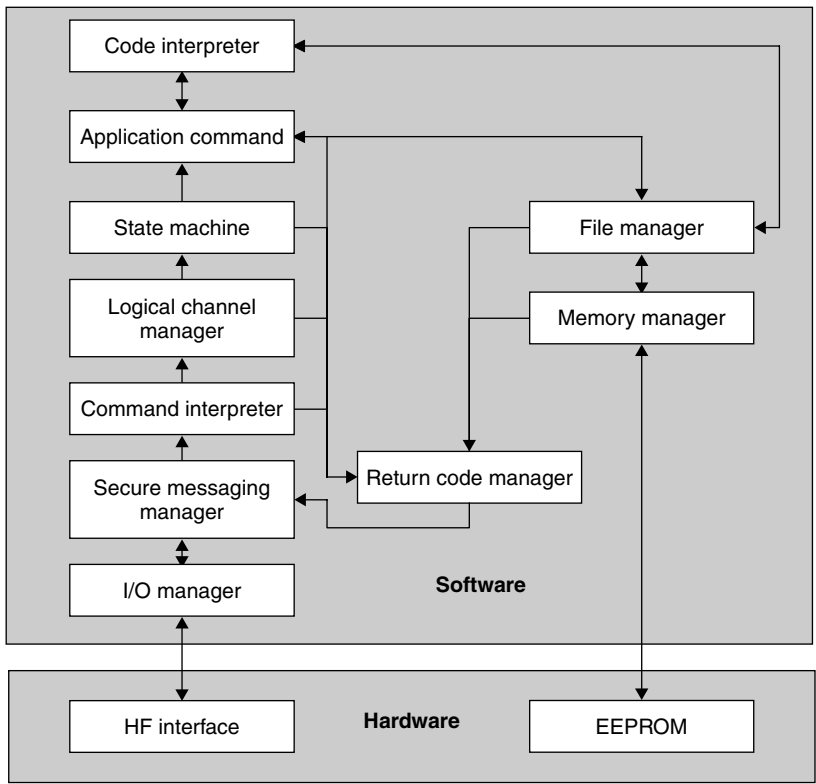


Figure 10.25 Command processing sequence within a smart card operating system (Rankl and Effing, 1996)

of data. The resulting necessity of being able to quickly and simply calculate complex *cryptographic* algorithms led to the development of powerful cryptographic *coprocessors* on the card chips.

Contactless smart cards, on the other hand, are traditionally used in applications that require a combination of user-friendliness (access control) and short *transaction times* (ticketing). The trend towards combining payment applications with typical contactless applications (cash card with ticketing function) finally led to the development of the *dual interface card*, in which both a contact and a contactless interface are available on one chip. A dual interface card can thus be addressed either via the contactless or the contact interface.

The philosophy underlying the dual interface card is that the smart card interface is completely independent of the smart card logic or smart card software. The interface, whether contact or contactless, is completely transparent to the transmitted application data so that, from the point of view of the application software, the interface used is unimportant. The interface is thus exchangeable at will, and interface and logic components can be combined as desired. The greatest advantage of the dual interface card for the user and system operator is the option of being able to draw upon existing infrastructure (generally contact readers) when introducing new applications. Also, from the point of view of the *security requirements* of a smart card, there is no difference between a contact and a contactless smart card. Due to the transparency of the interface, the replay and fraud of security-related data that has been transmitted is effectively ruled out by the methods defined in ISO/IEC 7816 (e.g. ‘secure messaging’), regardless of the interface used. See Figures 10.26 and 10.27.

The greatest difference between a contactless and a contact smart card is the power available. A contactless smart card in accordance with ISO 14443 has only around 5 mW available for operation at the maximum distance from the reader ($H_{\min} = 1.5 \text{ A/m}$) (Mühlbauer, 2001). A contact smart card, on the other hand, may have 7.2 mW (GSM 11.13), 50 mW (GSM 11.11) or even up to 300 mW (ISO 7816-3 Class A: 5 V,

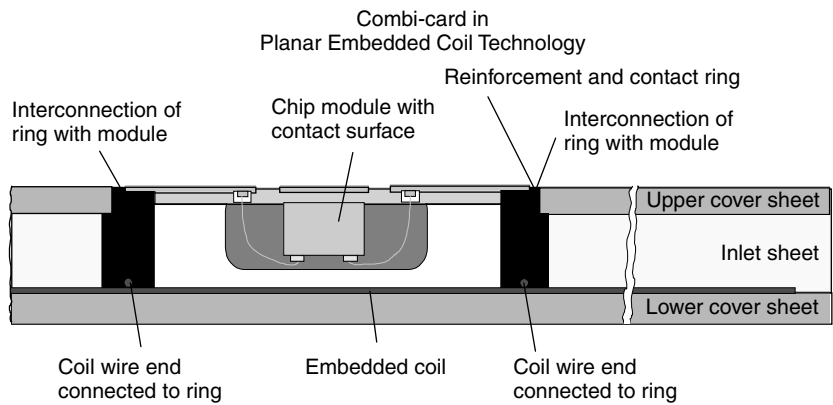


Figure 10.26 Possible layout of a dual interface smart card. The chip module is connected to both contact surfaces (like a telephone smart card) and a transponder coil (reproduced by permission of Amatech GmbH & Co. KG, Pfronten)

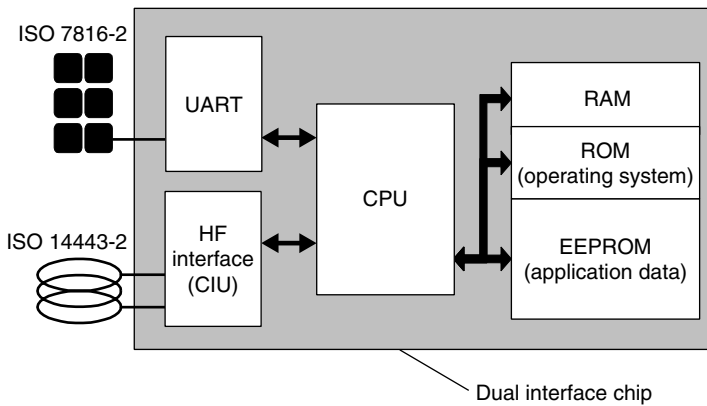


Figure 10.27 Block diagram of a dual interface card. Both smart card interfaces can be addressed independently of one another

60 mA) available depending upon its specification (Philipp, 2001). This calls for completely new concepts in the development of contactless microprocessor chips. For example, the use of a *PMU* (*power management unit*) on the chip, which can automatically separate inactive circuit parts of the chip from the power supply to save energy, is recommended. Furthermore, ultra-low-power and low-voltage technology is used in all dual interface chips so that the available power can be optimally exploited.

An explicit switching between contactless and contact operation on the chip is not necessary. In the simplest case it is sufficient to use the validity of the data received via one of the two interfaces as the evaluation criterion for further operation. Some chips provide the programmer with status flags that allow the currently active operating mode to be interrogated. Moreover, the signals (frequency, voltage) present at the HF interface or the chip contacts are evaluated.

10.2.1.1 MIFARE® plus

The block diagram in Figure 10.28 shows a very early approach to the dual interface card. This chip was developed jointly by Philips Semiconductors Gratkorn and Siemens HL (now Infineon AG) as early as 1997. Since it was not possible using the semiconductor technologies available at the time to reliably operate a microprocessor with the power available via the contactless interface, an unconventional solution was selected.

At the heart of this chip is an 8 Kbyte EEPROM memory, the Common EEPROM, in which the application data was stored. In a similar manner to a dual port RAM, this common EEPROM can be accessed via two interfaces that are completely separate from each other from the point of view of circuitry. The inactive interface at any time is completely separated from the power supply of the chip, so that the power available in contactless operation is used optimally.

The contactless interface is based upon a *state machine*, which forms a contactless MIFARE® memory card. From the point of view of a contactless reader this dual interface card thus behaves like a memory card with a segmented EEPROM memory,

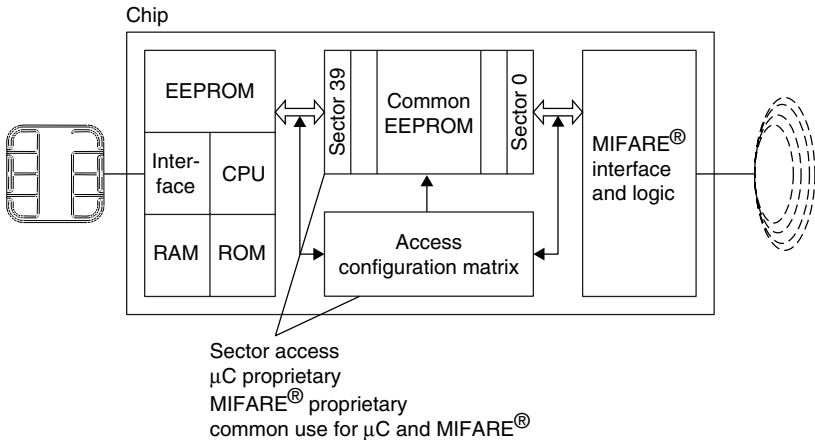


Figure 10.28 Block diagram of the MIFARE®-plus 'dual interface card' chip. In contactless operating mode the common EEPROM is accessed via a MIFARE®-compatible state machine. When operating via the contact interface a microprocessor with its own operating system accesses the same memory (reproduced by permission of SLE 44R42, Infineon AG, Munich)

in which the arrangement of the individual segments and memory blocks are identical to that of a conventional MIFARE® card (see Section 10.1.3.5).

The contact interface, on the other hand, is based upon a *microprocessor* with its own *smart card operating system*. The above-mentioned memory segmentation is once again present when the microprocessor accesses the common EEPROM. The operating system can therefore only read and write the common EEPROM in blocks within the corresponding sectors.

In addition, the write and read rights for individual memory blocks of the common EEPROM can be configured separately for the contactless and contact interface. These access rights are set in, and monitored by, the Access Configuration Matrix. This also facilitates the realisation of hierarchical security concepts.

10.2.1.2 Modern concepts for the dual interface card

Figure 10.29 shows the block diagram of a modern dual interface card. This card is based upon a 8051 microprocessor with a *smart card operating system*. The contactless interface is formed by a CIU (*contactless interface unit*), which can be configured by the CPU via register addresses or can also facilitate a status interrogation of the CIU.

A modern CIU automatically performs the transfer of a data block from and to a reader and thereby automatically performs the necessary coding or decoding of the data stream according to the specifications in the standard ISO/I EC14443-2 and ISO/I EC14443-3. Often it also performs the automatic calculation and verification of the transmitted CRCs.

To send a data block, the operating system only needs to store the data block to be sent in the RAM memory of the chip and load the corresponding memory address and block length into the configuration register of the CIU. The CPU is no longer actively involved in the initiated data transfer and can thus be switched into *power down mode*

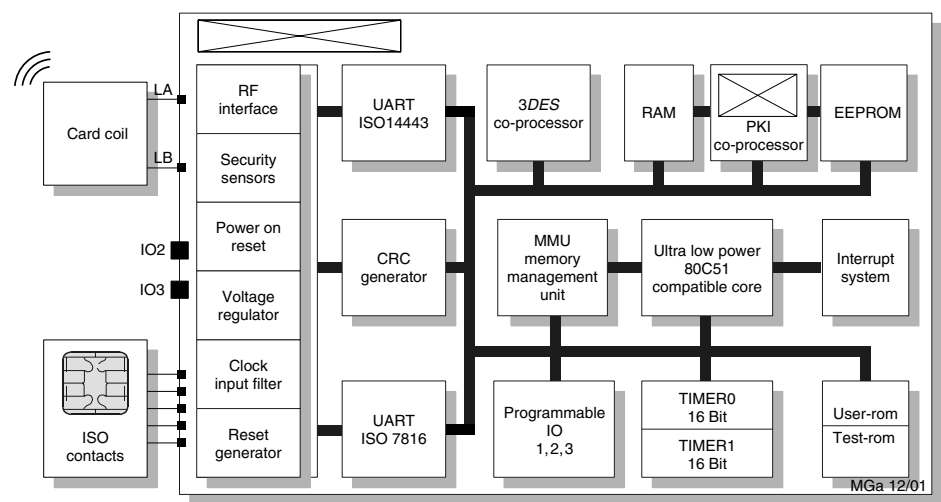


Figure 10.29 Block diagram of the dual interface card chip ‘MIFARE ProX’ (reproduced by permission of Philips Semiconductors Gratkorn, A-Gratkorn)

(*power saving mode*) for the duration of the data transfer (Mühlbauer, 2001). When a data block is received, the data from the CIU is then automatically stored in the chip’s RAM and the *CRC* of the received block is verified.

Short transaction times represent a particularly important requirement for contactless applications. For ticketing applications a maximum transaction time of 100ms is a generally accepted value. In order to facilitate the calculation of cryptographic functions within this short time interval, many dual interface chips have *cryptographic coprocessors*. In banking applications, symmetrical encryption algorithms such as *DES* (data encryption standard) and triple DES are normally used (Figure 10.30). *Encryption*

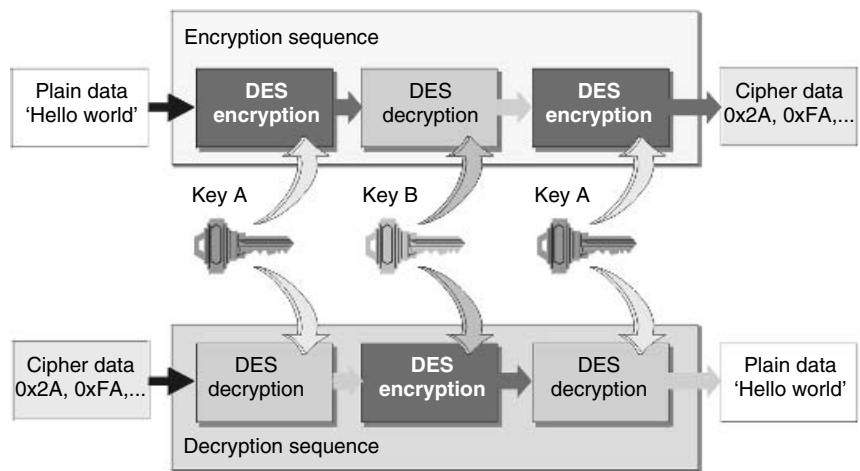


Figure 10.30 Calculation of the 3DES (triple DES). Encryption (above) and decryption (below) of a data block (reproduced by permission of Philips Semiconductors Gratkorn, A-Gratkorn)

and *decryption* by software is time consuming and therefore not practical in a contact-less application. DES encryption can be calculated several hundreds of times quicker using a coprocessor than is possible with the software solution (Mühlbauer, 2001). The CPU need only enter the data to be encrypted and the key in the correct register (DDAT and DKEY in Figure 10.31) and start the calculation by means of a control register (DCNTRL).

Asymmetric key algorithms ('public key' procedures such as RSA) will become increasingly important in future. Typical applications are electronic signatures (digital signature) or the validity testing of electronic documents (certification). Therefore, the first dual interface chips already have coprocessors for asymmetric algorithms (e.g. Fame PKI in Figure 10.29).

10.3 Memory Technology

After the state machine or microprocessor, the most important component of a data carrier is the memory that user data is read from or written to. Read-only data is defined at the manufacturing stage by the chip mask (exposure mask) or permanently burnt into the memory by a laser. The use of a laser also makes it possible to programme *unique numbers* (*serial numbers* that are issued only once) or consecutive numbers into the data carrier.

If data is to be written to the data carrier, then RAM, EEPROM or FRAM cells are also incorporated into the chip. However, only EEPROM and FRAM cells can store the written data for long periods (typical retention periods are 10 years) without a power supply.

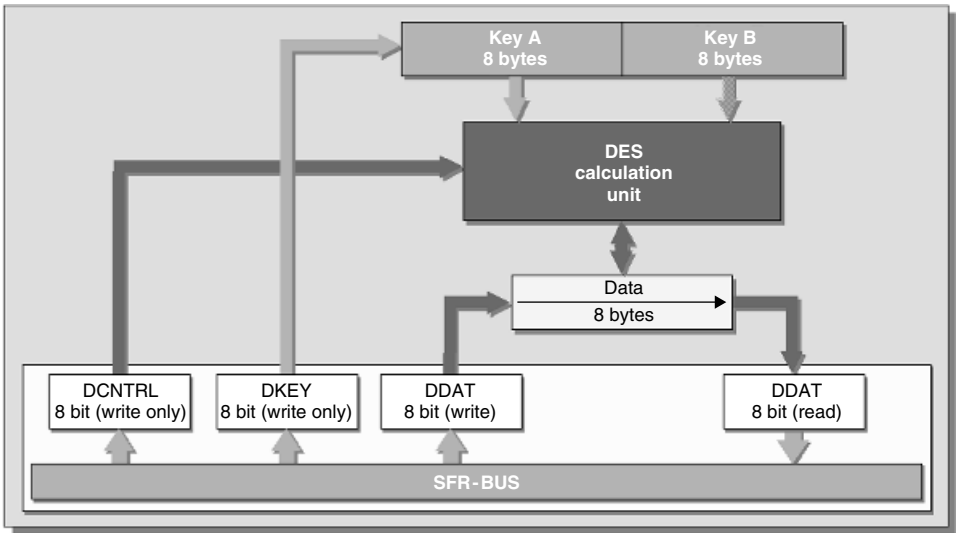


Figure 10.31 Block diagram of a DES coprocessor. The CPU key and data can be transferred to the coprocessor by means of its own SFR (special function register) (reproduced by permission of Philips Semiconductors Gratkorn, A-Gratkorn)

10.3.1 RAM

RAM is memory that can be used for the storage of temporary data. When the power supply is removed, the stored data is lost forever. In transponders, RAM is mainly used for the temporary storage of data that exists briefly during operation in the interrogation zone of a reader. In active transponders that have their own battery, RAMs with battery backups are sometimes used for the long-term storage of data.

The main component of the (S)RAM memory cell is a D-flip-flop. Figure 10.32 shows the block diagram for a single memory cell. Each memory cell has the connections DI (Data Input), WE (Write Enable) and DO (Data Out). If data is only to be read from the memory cell, it is sufficient to activate the selected cell with logic 1 levels at the allocated address connections Y_i and X_i .

To write data to the memory cell, the WE connection must also be switched to the 1 level. If there is a 1 level at C1 input data is written to the flip-flop.

10.3.2 EEPROM

The operating principle of an EEPROM cell is based upon the ability of a capacitor (condenser) to store electric charge over long periods. An EEPROM therefore represents a tiny capacitor that can be charged or discharged. A charged capacitor represents a logic '1', a discharged capacitor represents a logic '0'.

In its simplest form, an EEPROM cell basically consists of a modified field effect transistor on a carrier material (substrate) made of silicon. The EEPROM cell contains an additional gate between the control gate of the field effect transistor and the substrate, which is not connected to an external power supply, and which is positioned at a very short distance ($\sim 10\text{nm}$) from the carrier material. This so-called *floating gate* can be charged or discharged via the substrate using the tunnel effect, and therefore represents a capacitor. For the tunnel effect to exist there must be a sufficiently large potential difference at the thin insulating tunnelling oxidation layer between the floating gate and the substrate (Figure 10.33).

The flow of current between source and drain can be controlled by the stored charge of the floating gate. A negatively charged floating gate gives rise to a high threshold

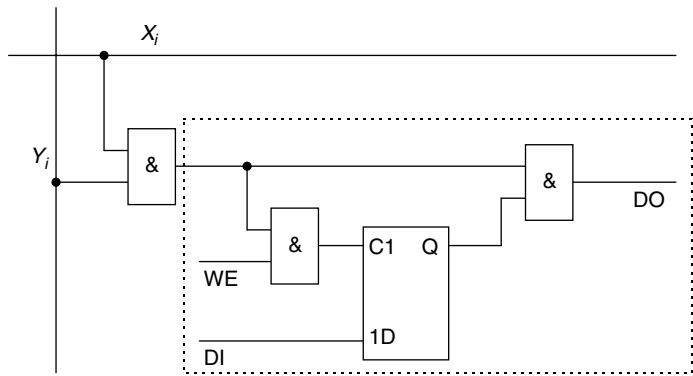


Figure 10.32 Simplified functional block diagram of a (S)RAM cell