WILEY

Smart Card Handbook

Second Edition

W. Rankl & W. Effing



Samsung v. Truesight
IPR2025-00123
Exhibit 1017

First published under the title *Handbuch der Chipkarten* by Carl Hanser Verlag
© Carl Hanser Verlag, Munich/FRG, 1999
All Rights reserved
Authorized translation from the 3rd edition in the original German language
published by Carl Hanser Verlag, Munich/FRG

Copyright © 2000 by John Wiley & Sons, Ltd
Baffins Lane, Chichester,
West Sussex, PO 19 1UD, England

National 01243 779777
International (+44) 1243 779777
e-mail (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on http://www.wiley.co.uk or http://www.wiley.com

Reprinted February 2001

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, 90 Tottenham Court Road, London, W1P 9HE, UK, without the permission in writing of the Publisher, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the publication.

Neither the authors nor John Wiley & Sons Ltd accept any responsibility or liability for loss or damage occasioned to any person or property through using the material, instructions, methods or ideas contained herein, or acting or refraining from acting as a result of such use. The authors and Publisher expressly disclaim all implied warranties, including merchantability of fitness for any particular purpose. There will be no duty on the authors of Publisher to correct any errors or defects in the software.

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

Other Wiley Editorial Offices

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

Wiley-VCH Verlag GmbH
Pappelallee 3, D-69469 Weinheim, Germany

Jacaranda Wiley Ltd, 33 Park Road, Milton,
Queensland 4064, Australia

John Wiley & Sons (Canada) Ltd, 22 Worcester Road
Rexdale, Ontario, M9W 1L1, Canada

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

Library of Congress Cataloguing-in-Publication Data
Rankl, W. (Wolfgang)
[Handbuch der Chipkarten. English]
Smart Card Handbook/W. Rankl, W. Effing: transalted by Kenneth Cox. – 3rd ed
p. cm.
ISBN 0 471 98875 8
1. Smart cards – Handbooks, manuals, etc. I. Effing, W. (Wolfgang) II. Title.
TK7895.S62 R3613.2000
006 – dc21

00-043346

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library
ISBN 0 471 98875 8

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

Contents

Foreword ..... **xi**

Preface to the Second Edition ..... **xv**

Symbols and Notation ..... **xvii**

Program Code Conventions ..... **xix**

Acronyms ..... **xx**

1 Introduction **1**
1.1 The History of Smart Cards 2
1.2 Application Areas 5
1.2.1 Memory cards 5
1.2.2 Microprocessor cards 6
1.2.3 Contactless cards 8
1.3 Standardization 8

2 Types of Cards **15**
2.1 Embossed Cards 15
2.2 Magnetic-strip Cards 16
2.3 Smart Cards 18
2.3.1 Memory cards 18
2.3.2 Microprocessor cards 20
2.3.3 Contactless Smart Cards 21
2.4 Optical Memory Cards 24

3 Physical and Electrical Properties **27**
3.1 Physical Properties 27
3.1.1 Card Formats 28
3.1.2 Card components and security markings 32
3.2 The Card Body 37
3.2.1 Smart Card materials 38
3.2.2 Chip modules 40
3.3 Electrical Properties 50
3.3.1 Connections 50
3.3.2 Supply voltage 51
3.3.3 Supply current 52
3.3.4 External clock 54

3.3.5 Data transfer 54
3.3.6 Activation and de-activation sequences 54
3.4 Smart Card Microcontrollers 56
3.4.1 Processor types 59
3.4.2 Memory types 61
3.4.3 Supplementary hardware 71
3.5 Contact-type Cards 75
3.6 Contactless Cards 78
3.6.1 Close-coupling cards: ISO/IEC 10536 83
3.6.2 Remote coupling cards 88
3.6.3 Proximity integrated circuit(s) cards: ISO/IEC 14443 89
3.6.4 Hands-free integrated circuit cards: ISO/IEC 15693 89

4 Information-Technological Foundations 91
4.1 Data Structures 92
4.2 SDL Notation 96
4.3 State Machines 97
4.3.1 Fundamentals of state machine theory 97
4.3.2 Practical application 97
4.4 Error Detection and Correction Codes 101
4.4.1 XOR checksums 102
4.4.2 CRC checksums 103
4.4.3 Error correction 105
4.5 Data Compression 106
4.6 Cryptology 108
4.6.1 Symmetric cryptographic algorithms 112
4.6.2 Asymmetric cryptographic algorithms 119
4.6.3 Padding 127
4.6.4 Message authentication codes and cryptographic checksums 128
4.7 Key Management 130
4.7.1 Derived keys 130
4.7.2 Key diversification 130
4.7.3 Key versions 131
4.7.4 Dynamic keys 131
4.7.5 Key parameters 133
4.7.6 Key management example 133
4.8 Hash Functions 136
4.9 Random Numbers 138
4.9.1 Generating random numbers 138
4.9.2 Testing random numbers 141
4.10 Authentication 144
4.10.1 Symmetric unilateral authentication 145
4.10.2 Symmetric mutual authentication 147
4.10.3 Asymmetric static authentication 149
4.10.4 Dynamic asymmetric authentication 150
4.11 Digital Signatures 152
4.12 Certificates 156

Exhibit 1017
Page 004 of 102

5 Smart Card Operating Systems 159
5.1 The Development of Smart Card Operating Systems 160
5.2 Fundamentals 162
5.3 Design and Implementation Principles 165
5.4 Program Code Structure 169
5.5 Memory Organization 172
5.6 Smart Card Files 175
5.6.1 File types 176
5.6.2 File names 179
5.6.3 File selection 183
5.6.4 EF file structures 184
5.6.5 File access conditions 188
5.6.6 File attributes 190
5.7 File Management 191
5.8 Process Control 197
5.9 Atomic Processes 198
5.10 Smart Card Operating Systems with Downloadable Program Code 200
5.10.1 Executable native code 202
5.10.2 Java Card 208
5.11 The Small-OS Smart Card Operating System 226

6 Smart Card Data Transfers 269
6.1 The Physical Transmission Layer 271
6.2 Answer to Reset (ATR) 275
6.2.1 ATR characters 277
6.2.2 Practical examples of ATRs 284
6.3 Protocol Type Selection (PTS) 287
6.4 Data Transmission Protocols 290
6.4.1 Synchronous data transmission 292
6.4.2 The T=0 transmission protocol 297
6.4.3 The T=1 transmission protocol 303
6.4.4 Comparison of asynchronous transmission protocols 313
6.5 Message Structure: APDUs 314
6.5.1 Structure of the command APDU 314
6.5.2 Structure of the response APDU 316
6.6 Secure Data Transfers 317
6.6.1 The authentic mode procedure 320
6.6.2 The combined mode procedure 322
6.6.3 Send sequence counter 323
6.7 Logical Channels 325

7 Smart Card Commands 327
7.1 File Selection Commands 331
7.2 Read and Write Commands 333
7.3 Search Commands 341
7.4 File Manipulation Commands 343
7.5 Identification Commands 345

7.6 Authentication Commands 348
7.7 Commands for Cryptographic Algorithms 353
7.8 File Management Commands 359
7.9 Database Commands: SCQL 366
7.10 Commands for Electronic Purses 369
7.11 Credit Card and Debit Card Commands 371
7.12 Commands for Completing the Operating System 373
7.13 Hardware Testing Commands 376
7.14 Application-Specific Commands 379
7.15 Transmission Protocol Commands 379

8 Security Techniques 383
8.1 User Identification 383
8.1.1 Testing a secret number 384
8.1.2 Biometric methods 390
8.2 Smart Card Security 399
8.2.1 A classification of attacks and attackers 400
8.2.2 Attacks and defense mechanisms during the development stage 406
8.2.3 Attacks and defense mechanisms during the production stage 408
8.2.4 Attacks and defense mechanisms when the card is in use 409

9 Quality Assurance and Testing 443
9.1 Card Body Tests 444
9.2 Microcontroller Hardware Tests 449
9.3 Evaluating and Testing Software 451
9.3.1 Evaluation 451
9.3.2 Testing methods for software 457
9.3.3 Dynamic tests for operating systems and applications 464

10 The Smart Card Life Cycle 471
10.1 The Five Phases of the Smart Card Life Cycle 472
10.2 Phase 1 of the Life Cycle in Detail 474
10.2.1 Generating the operating system and producing the chip 474
10.2.2 Producing a card body without integrated coils 485
10.2.3 Producing card bodies with integrated coils 490
10.2.4 Combining the card body and the chip 493
10.3 Phase 2 of the Life Cycle in Detail 495
10.4 Phase 3 of the Life Cycle in Detail 501
10.5 Phase 4 of the Life Cycle in Detail 508
10.6 Phase 5 of the Life Cycle in Detail 508

11 Smart Card Terminals 511
11.1 Mechanical Characteristics 515
11.2 Electrical Characteristics 518
11.3 Security Techniques 520
11.4 Linking a Terminal with PC/SC 522

12 Smart Cards in Payment Systems 527
12.1 Payment Transactions with Cards 528
12.1.1 Electronic payments with Smart Cards 528
12.1.2 Electronic money 533
12.1.3 Basic system architecture options 534
12.2 Prepaid Memory Cards 537
12.3 Electronic Purses 538
12.3.1 The CEN EN 1546 standard 539
12.3.2 The Mondex system 553
12.4 The Eurocheque System in Germany 558
12.5 Credit Cards with Chips 565

13 Sample Applications 571
13.1 Public Cardphones in Germany 571
13.2 Contactless Memory Cards for Air Travel 574
13.3 Health Insurance Cards 577
13.4 Electronic Toll Systems 581
13.5 The GSM Network 585
13.6 Digital Signatures 595

14 Application Design 607
14.1 General Notes and Characteristic Data 607
14.1.1 Microcontrollers 607
14.1.2 Applications 611
14.1.3 System considerations 613
14.2 Formulas for Estimating Processing Times 614
14.3 Processing Times of Typical Smart Card Commands 622
14.4 Typical Command Execution Times 623
14.5 Application Development Tools 626
14.6 The Course of a Smart Card Project 628
14.7 Design Examples for Smart Card Applications 629
14.7.1 Electronic purse system for arcade games 630
14.7.2 Access control system 633
14.7.3 Testing the genuineness of a terminal 636

15 Appendix 639
15.1 Glossary 639
15.2 Literature 666
15.3 List of Standards with Comments 672
15.4 Registration Authorities for RIDs 694
15.5 Events 694
15.6 World Wide Web Addresses 695
15.7 Characteristic Values and Tables 707
15.7.1 ATR interval 707
15.7.2 ATR data element conversion tables 707
15.7.3 Determining the data transmission rate 708
15.7.4 Sampling times 709

15.7.5 The most important Smart Card commands 710
15.7.6 Summary of utilized instruction bytes 714
15.7.7 Smart Card command encoding 716
15.7.8 Smart Card return codes 719
15.7.9 Selected chips for memory cards 722
15.7.10 Selected microcontrollers for Smart Cards 724

Index **731**

Exhibit 1017
Page 008 of 102

1

Introduction

This book has been written for students, engineers and the technically minded who would like to find out more about Smart Cards. It attempts to cover as much of this wide-ranging topic as possible, in order to provide the reader with an overview of the fundamentals of the field and the current state of its technology.

We have put great emphasis on the practical approach. The wealth of pictures, tables and references to real applications is designed to help the reader become familiar with the subject rather faster than would be possible with a strictly scientific presentation. Hence, the book makes no claims to be scientifically complete, but rather to be useful in practice. This is also the reason why the explanations have been kept as concrete as possible. At many points, we had to choose between scientific accuracy and ease of understanding, and we have tried to strike a happy medium between the two. Where this proved impossible, we have always preferred comprehensibility.

The book is designed so that it can be read in the usual way, from front to back. We have tried as much as possible to avoid forward references. The designs of the individual chapters, in terms of structure and content, allow them to be read separately without any loss of understanding. The comprehensive index and the glossary allow this book to be used as a reference work. If you want to know more about a specific topic, the cross-references in the text and the annotated index of standards will help you find the relevant text.

At this point, we must mention one small proviso. This book deals mainly with microprocessor cards in the credit card format. As far as space permits, we have also described memory cards and card terminals.

A large number of acronyms have unfortunately become entrenched in the field of Smart Card technology, as they have in so many other areas of technology and in everyday life. This makes it particularly hard for the newcomer to gain familiarity with the subject. We have tried to minimize the use of these cryptic and often illogical abbreviations. Nevertheless, in many cases we have had to choose a middle way between the internationally accepted Smart Card jargon used by specialists and the vernacular terms that are more easily understood by the layman. If we have not always been successful, at least the very comprehensive list of acronyms at the front of the book should help to overcome any barriers to comprehension, which we hope will be short-lived. An extensive glossary at the end of the book explains the most important technical concepts and supplements the list of acronyms.

Active learning is indisputably much more effective and interesting than passive learning. Thus, for example, you can learn a new language more quickly and easily by

spending some time in a country in which the language is spoken. Our Smart Card simulation program for PCs, which has become well known since its introduction with the second edition, will be available shortly in a new and improved version. It is now 'freeware' and can be found on the Internet site of the publisher [Wiley]. Good luck and good learning!

1.1 The History of Smart Cards

The proliferation of plastic cards started in the USA in the early 1950s. The low price of the synthetic material PVC allowed robust, long-lasting cards to be produced. These were much more suitable for use in everyday life than the paper and cardboard cards previously used, which could not adequately withstand mechanical stress and climatic effects.

The first all-plastic payment card for general use was issued by the Diners Club in 1950. It was intended for an exclusive class of individual, and thus also served as a status symbol, allowing the holder to pay with his or her 'good name' rather than with cash. Acceptance of these cards was initially restricted to the more select restaurants and hotels, which led to this type of card being referred to as a 'travel and entertainment' card.

The entry of Visa and Mastercard into the field led to a very rapid proliferation of plastic money, at first in the USA, with Europe and the rest of the world following a few years later.

Today, credit cards allow the traveler to shop without cash anywhere in the world. The cardholder is never without means of payment, yet he or she avoids exposure to the risk of loss through theft or other hazards that are difficult to anticipate, particularly whilst travelling. Using a credit card does away with the tedious task of exchanging currency when travelling abroad. These unique advantages have helped credit cards to become rapidly established worldwide. Many hundreds of millions of cards are produced and issued annually.

At first, the cards' functions were quite simple. They initially served as data carriers that were secure against forgery and tampering. General information, such as the card issuer's name, was printed on the surface, while personal data elements, such as the cardholder's name and the card number, were embossed. Furthermore, many cards had a signature field, in which the cardholder could sign his or her name for reference. In these first-generation cards, protection against forgery was provided by visual features, such as security printing and the signature field. Consequently, the system's security depended quite fundamentally on the quality and conscientiousness of the retail staff accepting the cards. However, this was not an overwhelming problem, due to the card's initial exclusivity. With increasing proliferation in card use, these rather basic features no longer proved sufficient, all the more so since threats from organized crime were growing apace.

Increasing handling costs for the merchants and banks made a machine-readable card necessary, while at the same time the card issuers' losses due to customer insolvency and fraud grew from year to year. It became apparent that both the security measures against fraud and tampering, as well as the basic functions of the cards, had to be extended and improved.

The first improvement consisted of a magnetic strip on the back of the card. This allowed digital data to be stored on the card in machine-readable form, as a supplement to the visual data. This made it possible to minimize the use of paper receipts, which were

Exhibit 1017
Page 010 of 102

previously essential. However, the customer's signature on a paper receipt, as a form of personal identification, still remains a requirement in classical credit card applications.

New applications can however be devised in which paper receipts are unnecessary. This would allow a long-standing goal to finally be achieved, which is the replacement of paper-based transactions by electronic data processing. Identification of the card user, which up to now has been accomplished using signatures, must be accomplished in a different manner to make this possible. The use of a secret personal identification number (PIN) that is compared to a reference number has become generally accepted. The reader is surely familiar with this technique, which is used for bank machines (automated teller machines).

The embossed card with a magnetic strip is still the most commonly used type of payment card. Magnetic strip technology suffers from a crucial weakness, however, in that the data stored on the strip can be read, deleted and rewritten at will by anyone with access to the appropriate equipment. It is thus unsuitable for the storage of confidential data. Additional techniques must be used to ensure confidentiality and to protect against tampering. For example, the reference value for the PIN can be stored either in the terminal or in the host system in a secure environment, instead of on the magnetic strip. Most systems that employ magnetic-strip cards thus have on-line connections to the system's host computer for security reasons. However, this generates considerable data transmission costs. In order to reduce costs, solutions must be sought that allow card transactions to be executed off-line without putting the system's security at risk.

The development of the Smart Card, combined with the expansion of electronic data processing, has created completely new possibilities for solving this problem. Enormous progress in microelectronics in the 1970s made it possible to integrate data storage and arithmetic logic on a single silicon chip measuring a few square millimeters. The idea of incorporating such an integrated circuit into an identification card was contained in a patent application filed by the German inventors Jürgen Dethloff and Helmut Grötrupp as early as 1968. This was followed in 1970 by a similar patent application, made by Kunitaka Arimura in Japan. However, the first real progress in the development of Smart Cards came when Roland Moreno registered his Smart Card patents in France in 1974. It was only then that the semiconductor industry was able to supply the required integrated circuits at acceptable prices. Nevertheless, many technical problems still had to be solved before the first prototypes, some of which contained several integrated circuit chips, could be transformed into reliable products that could be manufactured in large numbers with adequate quality and reasonable prices. Since the basic inventions in Smart Card technology come out of Germany and France, it is not surprising that these countries played the leading role in the development and marketing of Smart Cards.

The great breakthrough was achieved in 1984, when the French PTT (postal and telecommunications services) successfully carried out a field trial with telephone cards. In this field trial, the Smart Cards immediately proved to meet all expectations with regard to protection against tampering and high reliability. Significantly, the breakthrough for Smart Cards did not come in an area where traditional cards were already used, but in a new application. Introducing a new technology in a new application has the great advantage that compatibility with existing systems does not have to be taken into account, so that the capabilities of the new technology can be fully exploited.

A pilot project was conducted in Germany in 1984–85, using telephone cards based on a variety of technologies. Magnetic-strip cards, optical-storage (holographic) cards and Smart Cards were used in comparative tests. The Smart Card proved to be the winner in this pilot

study. In addition to a high degree of reliability and security against tampering, Smart Card technology promised the greatest flexibility in future applications. While the older but less expensive EPROM technology was used in the French telephone card chips, newer EEPROM chips were used from the start in the German telephone cards. The latter type of chip does not need a programming voltage supply. However, the unfortunate consequence is that the French and German telephone cards are mutually incompatible. It appears that even after the introduction of the Euro, French and German telephone cards will for a short time still not be usable in each other's countries of origin.

Further developments followed the successful trials of telephone cards, first in France and then in Germany, with breathtaking speed. By 1986, several million 'smart' telephone cards were in circulation in France alone. The total number reached nearly 60 million in 1990 and several hundred million worldwide in 1997. Germany experienced a similar development, with a time lag of about three years. These systems were marketed throughout the world after the successful introduction of the public Smart Card in France and Germany. Telephone cards incorporating chips are currently used in over 50 countries.

Progress was significantly slower in the field of bank cards, which is partly due to their greater complexity in comparison to telephone cards. These differences are described in detail in the following chapters. Here we would just like to remark that the development of modern cryptography has been just as critical for the proliferation of bank cards as the developments in semiconductor technology.

With the general expansion of electronic data processing in the 1960s, the field of cryptography experienced a sort of quantum leap. Modern hardware and software permitted the implementation of complex and demanding mathematical algorithms, which made possible a degree of security unparalleled until then. Moreover, this new technology was available to everyone, whereas cryptography had previously been a covert science in the private reserve of the military and secret services.

With these modern cryptographic procedures, the strength of the security mechanisms in electronic data processing systems could be mathematically calculated. It was no longer necessary to rely on the very subjective assessment of conventional techniques, whose security essentially rested on the secrecy of the procedures used.

The Smart Card proved to be an ideal medium. It made a high level of security (based on cryptography) available to everyone, since it can safely store secret keys and also execute cryptographic algorithms. In addition, Smart Cards are so small and easy to handle that they can be carried and used everywhere by everyone in everyday life. It was a natural idea to try to employ these new security features for bank cards, in order to come to grips with the security risks associated with the increasing utilization of magnetic-strip cards.

The French banks were the first to introduce this fascinating technology in 1984, following a trial with 60,000 cards in 1982–83. It took another 10 years before all French bank cards incorporated chips. In Germany, the first field trials took place in 1984–85 with a multifunctional payment card incorporating a chip. However, the *Zentrale Kreditausschuß* (ZKA), which is a committee of the leading German banks, did not manage to issue a specification for multifunctional Eurocheque cards incorporating chips until 1996. In 1997, all German savings associations and many banks issued the new Smart Cards. In the previous year, multifunctional Smart Cards with POS functions, an electronic purse and optional additional applications were issued in all of Austria. This made Austria the first country in the world to have a nationwide electronic purse system.

An important milestone for the future worldwide use of Smart Cards for financial transactions was the completion of the EMV specification, which was a product of the joint effort of Europay, Mastercard and Visa. The first version of this specification was published in 1994. It contained detailed descriptions of credit cards incorporating microprocessor chips, and it guaranteed the mutual compatibility of the future Smart Cards of the three largest credit card organizations.

Electronic purse systems have proven to be an additional drawing card for the international use of Smart Cards for financial transactions. The first such system, called Danmønt, was put into operation in Denmark in 1992. There are currently more than 20 national systems in use in Europe alone, many of which are based on the preliminary European standard prEN 1546. The use of such systems is also increasing outside of Europe. Even in the USA, where Smart Card systems have hardly taken root up to now, a Smart Card purse system was tried out by Visa during the 1996 Olympic Summer Games in Atlanta. Payments via the Internet offer a new and promising area for the use of electronic purses. However, the problems associated with making small payments securely but anonymously throughout the world via the public Internet have not yet been solved in a satisfactory manner. Smart Cards could play a decisive role in the solution of these problems.

Yet another application has meant that almost every German citizen these days owns a Smart Card. When health insurance cards incorporating chips were introduced, more than 70 million Smart Cards were issued to all persons covered by the national health insurance plan.

The Smart Card's high degree of functional flexibility, which even allows a card already in service to be reprogrammed for new applications, has opened up completely new areas of use that extend beyond traditional card applications.

1.2 Application Areas

As can be seen from the historical summary, possible applications for the Smart Card are extremely diverse. They are also constantly being extended with the increasing arithmetic power and storage capacity of available integrated circuits. Within the confines of this book, it is impossible to describe all these applications in detail. Instead, a few typical examples must serve to illustrate the Smart Card's fundamental properties. This introductory chapter is only meant to provide an initial overview of the card's functional flexibility. Chapter 13 describes several sample applications in detail.

To make this summary easier to follow, it is helpful to divide Smart Cards into two categories: memory cards and microprocessor cards.

1.2.1 Memory cards

The first Smart Cards used in large quantities were memory cards for telephone applications. These cards are prepaid, and the value stored electronically in the chip is decreased by the amount of the charge each time it was used. Naturally, it is necessary to prevent the user from subsequently increasing the stored value, which could easily be done with a magnetic-strip card. All the user would have to do is note the data stored at the time of purchase and rewrite them to the magnetic strip after using the card. The card would then

have its original value and could be reused. This type of tampering, known as 'buffering', is prevented in Smart Cards by security logic in the chip. This makes it impossible to erase a memory cell once it has been written. The reduction in the card's value by the number of charge units used is thus irreversible.

This type of Smart Card can naturally be used not only for telephone calls, but also whenever goods or services are to be sold against prior payment without the use of cash. Examples of possible uses include local public transport, all kinds of vending machines, cafeterias, swimming pools, car parks and so on. The advantage of this type of card lies in its simple technology (the chip's surface area is typically only a few square millimeters), and hence its low cost. The disadvantage is that the card cannot be reused once it is empty, but must be discarded as waste unless it ends up in a card collection.

Another typical application of memory cards is the health insurance card, which has been issued in Germany since 1994 to all persons covered by the national health insurance plan. The information that previously was written on the patient's card is now stored in the chip and also printed or laser-engraved on the card. Using a chip for storage makes the cards machine-readable using simple equipment.

In summary, memory-type Smart Cards have limited functionality. Their integrated security logic makes it possible to protect stored data against tampering. They can be used as cash-equivalent cards or identification cards in systems where low cost is a primary consideration.

1.2.2 Microprocessor cards

As already mentioned, the first application of microprocessor cards was in the form of French bank cards. Their ability to store private keys securely and to execute modern cryptographic algorithms made it possible to implement highly secure off-line payment systems.

Since the microprocessor built into the card is freely programmable, the functionality of microprocessor cards is restricted only by the available storage space and the capacity of the arithmetic unit. The only limits to one's imagination when implementing Smart Card systems are thus technological ones, and these are extended enormously with each new generation of integrated circuits.

Following a drastic reduction in the cost of Smart Cards in the early 1990s, as a result of mass production, new applications have been introduced year after year. The use of Smart Cards with cellular telephones has been especially important for their international proliferation.

After being successfully tested in the German national C network (analogue cellular telephone network) for use in portable end-user equipment, the Smart Card was prescribed as the access medium for the European digital cellular phone system (GSM). On the one hand, the Smart Card enabled a high degree of security to be achieved for accessing the cellular telephone network. At the same time, it offered new possibilities and thus big advantages in the marketing of cellular telephones, since it offered network operators and service providers a way to separate the sale of the telephone from the sale of services. Without the Smart Card, cellular telephones would certainly not have spread across Europe so quickly or have developed into a worldwide standard.

Exhibit 1017
Page 014 of 102

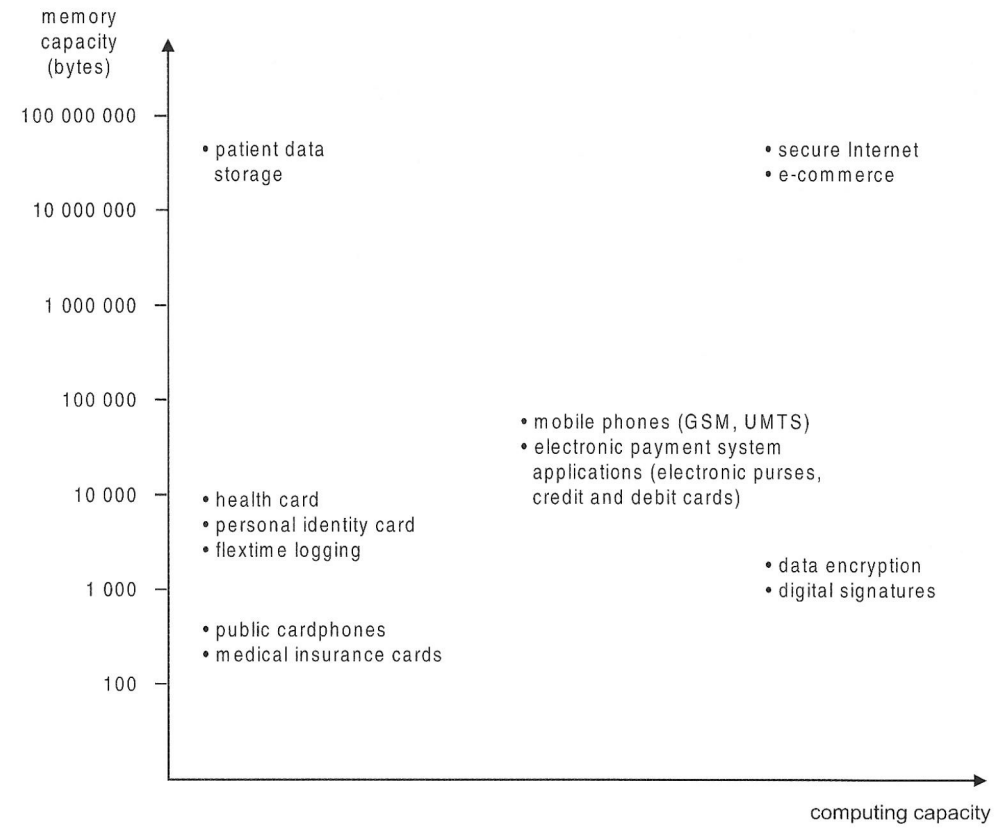


Figure 1.1 Typical Smart Card application areas, showing the required storage capacity and arithmetic processing capacity

Possible applications for microprocessor cards include identification cards, access control for restricted areas and computers, protected data storage, electronic signatures and electronic purses, as well as multifunctional cards incorporating several applications in a single card. Presently, Smart Card operating systems are being developed that allow new applications to be loaded into a card after it has been issued to the user, without compromising the security of the various applications. Completely new application areas are made possible with this new flexibility. For example, personal security modules are indispensable if Internet trade and payments are to be made trustworthy. Such security modules would securely store personal keys and could execute high-performance cryptographic algorithms. These tasks can be performed in an elegant manner by a microprocessor with a cryptographic coprocessor. Specifications for secure applications of Smart Cards with the Internet are currently being developed throughout the world. Within a few years, we can expect to see every PC equipped with a Smart Card interface.

In summary, the essential advantages of microprocessor cards are their high storage capacity, their ability to securely store confidential data and their ability to execute cryptographic algorithms. These advantages make a wide range of new applications possible, in addition to the card's traditional use as a bank card. The Smart Card's potential is by no means yet exhausted, and in fact, it is constantly being extended by progress in semiconductor technology.

Exhibit 1017
Page 015 of 102

1.2.3 Contactless cards

Contactless cards, in which energy and data are transferred without any electrical contact between the card and the terminal, have achieved the status of commercial products in the last few years. Presently, both memory cards and microprocessor cards are available as contactless cards. Although contactless microprocessor cards can usually work at a distance of only a few centimeters away from the terminal, contactless memory cards can be used up to a meter away from the terminal. This means that such cards do not necessarily have to be held in the user's hand during use, but can remain in the user's purse or briefcase, for example.

These cards are thus particularly suitable for applications in which persons or objects should be quickly identified. Sample applications are:

- access control,
- local public transportation,
- ski passes,
- airline tickets,
- baggage identification.

There are, however, applications in which operation over a long distance could cause problems, and thus should be prevented. A typical example is an electronic purse. A declaration of intention on the part of the card holder is normally required to complete a financial transaction. This confirms the amount of the payment and the agreement of the cardholder to pay. With a contactless card, this declaration takes the form of inserting the card in the terminal and confirming the indicated amount. If contactless financial transactions over relatively long distances were possible, a 'con artist' could transfer money out of the electronic purse without the knowledge of the card holder. Dual-interface cards (sometimes called 'combicards') offer a possible solution to this problem. These cards unite contact and contactless interfaces in a single card. Such a card can communicate with the terminal via either its contact interface or its contactless interface, as desired.

There is great interest in contactless cards in the field of local public transportation. If the present Smart Cards used for financial transactions, which as a rule are contact-type cards, were to have their functionality extended to include acting as electronic tickets with contactless interfaces, then transportation agencies could make use of the existing infrastructure and cards of the credit card industry.

1.3 Standardization

The prerequisite for the worldwide extension of Smart Cards into everyday life, similar to their current use in Germany in the form of telephone cards, health insurance cards and bank cards, has been the creation of national and international standards. Due to the special significance of such standards, in this book we repeatedly refer to existing standards and those that are in preparation. Why are standards so important for the expansion in the use of Smart Cards?

A Smart Card is normally one component of a complex system. This means that the interfaces between the card and the rest of the system must be exactly specified and matched to teach other. Of course, it is possible to do this for every system on a case-by-

case basis, without regard to other systems. This would however mean that a different Smart Card would be needed for each different system. The user would thus have to carry a separate card for every application. In order to avoid this, an attempt has been made to develop application-independent standards that make possible multifunctional cards. Since the Smart Card usually represents the component of the system that the user holds in his or her hand, it is of enormous importance for the recognition and acceptance of the entire system. Nonetheless, from a technical and organizational perspective, the Smart Card is usually merely the tip of the iceberg, since complex systems (which are usually networked) are quite often hidden behind the card terminal, and it is these systems that make the service possible in the first place.

Let us take as an example telephone cards, which technically speaking are fairly simple objects. By themselves, they are almost worthless, except perhaps as collector's items. Their true function, which is to allow the use of public telephones without coins, can be realized only after umpteen thousand cardphones have been installed to cover a whole region and have been connected to a network. The large investments required for this can only be justified if appropriate standards and specifications guarantee the long-term future of the system. Standards are an indispensable prerequisite for multifunctional Smart Cards, which can be used for various applications, such as telephony, electronic purses, electronic tickets and so on.

What are standards?

This question is not as trivial as it may appear at first glance, since the terms 'standard' and 'specification' are often used fairly indiscriminately. To make things clear, let us consider the ISO/IEC definition:

> **Standard**: a document that is produced by consensus and adopted by a recognized institution, and which, for general and recurring applications, defines rules, guidelines or features for activities or their results, whereby the objective is to achieve an optimum degree of regulation in a given context.
>
> *Note:* standards should be based on the established results of science, technology and experience, and their objective should be the promotion of optimized benefits for society.

International standards should thus help to make life easier and to increase the reliability and usefulness of products and services.

In order to avoid confusion, ISO/IEC have also defined the term 'consensus' as follows:

> **Consensus**: general agreement, characterized by the absence of continuing objections to essential components on the part of any significant part of the interested parties, and achieved by a procedure that attempts to take into consideration the views of all relevant parties and to deal with all counter-arguments.
>
> *Note:* consensus does not necessarily mean unanimity.

Although unanimity is not required, the democratic process of consensus naturally takes time. This is in particular due to the fact that not only the views of the technicians, but also

the views of all relevant parties must be examined, as the objective of a standard is the promotion of optimum advantages for the whole of society. Hence, the preparation of an ISO or CEN standard usually takes several years. A frequent consequence of the slowness of this process is that a small group of interested parties, such as commercial firms, produces its own specifications ('industry standards') in order to hasten the development of new systems. This is especially true in the field of information technology, which is characterized by especially fast development and correspondingly short innovation cycles. Although industry standards have the advantage that they can be developed significantly faster than 'general' standards, they contain hidden risks in that their development takes place without giving consideration to certain important interest groups. These are the parties that are not involved in defining their specifications. For this reason, ISO attempts to create opportunities for incorporating already existing, important publicly accessible specifications into the standardization process.

What does ISO mean?

The relevant ISO standards are especially significant for Smart Cards, since these standards define the basic properties of Smart Cards. What however lies behind the word 'ISO'?

The International Organisation for Standardisation (ISO) is a worldwide association of around 100 national standards agencies, with one per country. ISO was founded in 1948 and is a non-national organization. Its task is to promote the development of standards throughout the world, with the objective of simplifying the international exchange of goods and services and developing cooperation in the fields of science, technology and economy. The results of the work of ISO are agreements that are published as ISO standards.

'ISO' is, by the way, not an acronym. The acronym of the official name would of course be 'IOS'. The name 'ISO' is instead derived from the Greek word *isos*, which means 'equal' or 'the same'. The prefix *iso-*, derived from the Greek *isos*, is commonly used in the three official languages of ISO (English, French and Russian), as well as in many other languages.

As already mentioned, the members of ISO are the national standards bodies of the individual countries, and only one such body per country is allowed to be a member. The member organizations have four basic tasks, as follows:

- to inform potentially interested parties in their own countries about relevant activities and possibilities of international standardization,
- to form national opinions on a democratic basis and to represent these opinions in international negotiations,
- to set up a secretariat for ISO committees in which the country has a particular interest,
- to pay the country's financial contribution to support the central ISO organization.

How does an ISO standard come to be?

The need for a standard is usually reported to the national standards organization by an industrial sector. The national organization then proposes this to ISO as a new working theme. If the proposal is accepted by the responsible working group, which consists of technical experts from countries that are interested in the theme, the first thing that happens is that the objective of the future standard is defined.

After agreement has been achieved regarding the technical aspects to be considered in the standard, the detailed specifications of the standard are discussed and negotiated

between the various countries. This is the second phase in the development of the standard. The objective of this phase is to arrive at a consensus of all participating countries, if possible. The outcome of this phase is a 'Draft International Standard'.

The final phase consists of a formal vote on the proposed standard. Acceptance of the standard requires the approval of two thirds of the members of ISO that have actively participated in drafting the standard, as well as three quarters of all members that participate in the vote. Once the text has been accepted, it is published as an ISO standard.

To prevent standards from becoming outdated due to ongoing developments, ISO rules state that standards should be reviewed, and if necessary revised, after an interval of at most five years.

Cooperation with the IEC and the CEN

ISO is not the only international standards organization. In order to prevent duplication of effort, ISO co-operates closely with the IEC (International Electrotechnical Commission). The areas of responsibility are defined as follows: the IEC covers the fields of electrical technology and electronics, while ISO is responsible for all other fields. Combined working groups are formed to deal with themes of common interest, and these groups produce combined ISO/IEC standards. Most standards for Smart Cards belong to this category.

ISO and the European standardization committee CEN (*Comité Européen de Normalisation*) also agree on rules for the development of standards that are recognized as both European and international standards. This results in time and cost savings.

International standardization of Smart Cards

The development of international standards for Smart Cards takes place under the aegis of ISO/IEC and/or the CEN. The German standards association DIN is represented in all relevant committees. It also maintains 'mirror' committees in the form of national working and voting committees. Figure 1.2 gives an overall view of the structure of the relevant ISO working groups and the standards that are entrusted to them.

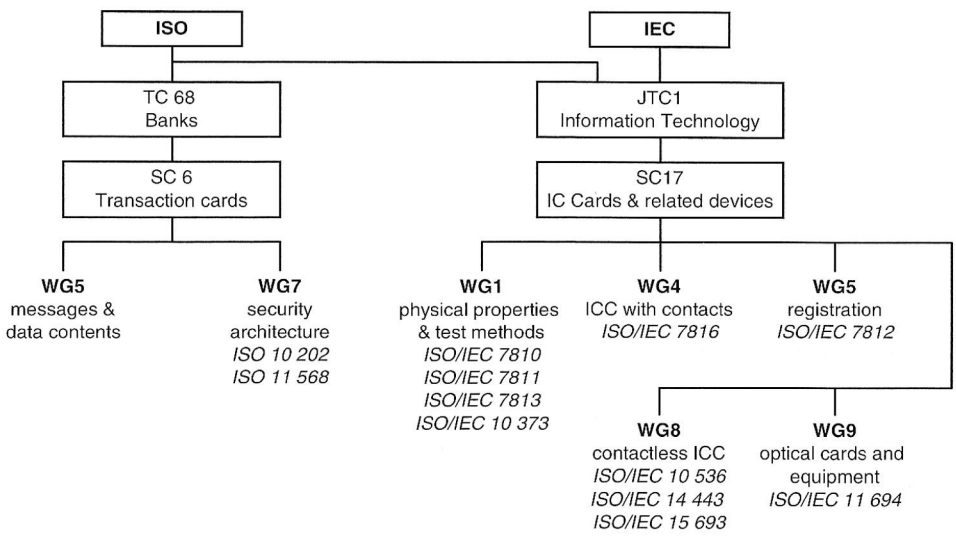


Figure 1.2 Overview and organization of the working groups involved in developing international Smart Card standards

As can be seen, there are two technical committees that are concerned with the standardization of Smart Cards. The first of these is ISO TC68/SC6, which is responsible for the standardization of cards used for financial transactions, while the second is ISO/IEC JTC1/SC17, which is responsible for general applications. This division has historical roots, since the first international applications were for identification cards used for financial transactions. The number of applications has naturally increased enormously since then, so that the general standards, which are looked after by the SC17 committee, have taken on greater significance. The standards relating specifically to financial transactions can thus be regarded as a subset of the general standards. Brief descriptions of the standards listed in Figure 1.2, including their current status, can be found in the Appendix.

The general subject of Smart Cards is dealt with by the CEN TC 224 committee ('Machine-readable Cards, Related Device Interfaces and Procedures'). Figure 1.3 provides an overview of the working groups and the standards that they look after.

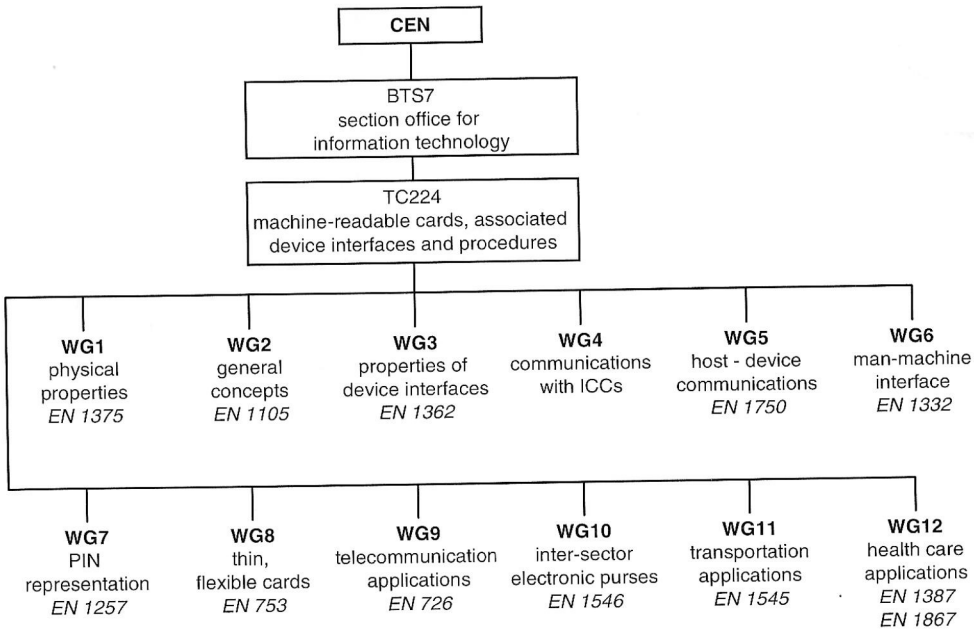


Figure 1.3 Overview and hierarchy of the working groups for European Smart Card standardization

The efforts of the CEN supplement those of ISO. ISO standards are taken over as CEN standards where possible, which requires that they be translated into the three official CEN languages (English, French and German). They may also be extended or reduced to comply with specifically European conditions, as necessary. In addition to these activities, the CEN working groups produce application-oriented standards, which as such would not be possible with ISO. Brief descriptions of the standards listed in Figure 1.3 can be found in the Appendix.

After more than fifteen years of standardization, the most important fundamental ISO standards for Smart Cards are now complete. They form the basis for further, more application-oriented standards, which are currently being prepared by ISO and the CEN.