Smart Card Handbook

Fourth Edition

Wolfgang Rankl and Wolfgang Effing
Giesecke & Devrient GmbH, Germany

Translated by
Kenneth Cox
Kenneth Cox Technical Translations, Wassenaar, The Netherlands

WILEY
A John Wiley and Sons, Ltd., Publication

Smart Card Handbook

Fourth Edition

Smart Card Handbook

Fourth Edition

Wolfgang Rankl and Wolfgang Effing
Giesecke & Devrient GmbH, Germany

Translated by
Kenneth Cox
Kenneth Cox Technical Translations, Wassenaar, The Netherlands

WILEY
A John Wiley and Sons, Ltd., Publication

First published under the title *Handbuch der Chipkarten: Fünfte Edition* by Carl Hanser Verlag

This edition first published 2010

First edition published 1997
Second edition published 2000
Third edition published 2003

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

Library of Congress Cataloging-in-Publication Data

Rankl, W. (Wolfgang)
[Handbuch der Chipkarten. English]
Smart card handbook / Wolfgang Rankl. – 4th ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-74367-6 (cloth)
1. Smart cards–Handbooks, manuals, etc. I. Title.
TK7895.S62R3613 2010
004.5'6–dc22
2009052095

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

ISBN 978-0-470-74367-6 (Hbk)

Typeset in 10/12pt Times by Aptara Inc., New Delhi, India
Printed in Singapore by Markono

Contents

Preface to the Fourth Edition

Preparing the fourth edition of a book with more than one thousand pages is not entirely the same as preparing the first edition of a technical book with three hundred pages. We learned this from painful experience in the course of the last two years, after we decided to write this new edition of the *Smart Card Handbook*.

Our decision was motivated by the dramatic evolution of smart card technology since the last edition of the book in 2002, which has resulted in so many fundamental changes that modifications were necessary on almost every page. With this major revision effort, we took the opportunity to migrate to a different working environment. Instead of using a certain well-known word processing program that was constantly on the verge of total collapse under the burden of this volume of material, we resolved to switch to a professional layout system. As well-known advocates of open-source software, we naturally had only one choice: LaTeX. Although we have never regretted this step, it did not exactly accelerate our project. One of the visible effects of this change for the reader is the large number of cross-references with page numbers. We also revised most of the figures and all of the tables. The result is a book that is distinctly more lucid and easier to read.

With this major revision, we have restructured the book to achieve a more logical arrangement of the various topics. This also allowed us to incorporate all the additions, changes, and special cases that have appeared in the previous editions in a structure that is once again self-contained and presents the entire subject in a clearly organized manner.

This also reflects the incipient paradigm shift in smart card technology. Until fairly recently, smart cards were largely niche products in the world of information technology, existing in a rather isolated technotope. However, in the last few years the technology of the PC and Internet worlds has made increasing inroads in the world of smart cards. As an example, we can mention cryptographically secured data transmission between smart cards and the outside world. The standard remains secure messaging, as specified by ISO/IEC 7816, but the integration of SSL and TSL protocols, long since proven in the Internet realm, is already on

the horizon. A similar situation can be seen with TCP/IP in the medium term. This will make smart cards uniquely addressable Internet devices and allow them to be integrated accordingly into the Internet infrastructure.

Another topic that made relatively large revisions necessary is the use of smart card microcontrollers with flash memory instead of mask-programmed ROM. If this evolutionary trend continues on its present course, and there is every reason to believe that it will, in only a few years there will be scarcely any ROM-based chips available for smart cards. This is accompanied by distinctly increased flexibility in operating systems and production logistics.

With regard to the overall organization of the book, we have maintained the proven approach of the previous editions. It begins with a relatively short chapter that provides a general introduction to the world of smart cards and sets the stage for the rest of the book. This is followed by several chapters devoted to the underlying aspects of the technology, which are necessary for proper understanding of this rather extensive subject. After this comes a group of chapters that deal with data transmission, commands, operating systems, smart card production, and quality assurance.

The book concludes with copious descriptions of diverse applications. We have limited the application descriptions to representative examples, since a nearly indescribable variety of new and interesting application areas have opened up for smart cards in the last few years.

At this point we would like to thank our families, friends and colleagues, whose help and encouragement made this book possible. Our particular thanks go to the following people: Bernhard Seen for his expert comments on card production; Jörn Treger for his thoroughgoing revision of the section on Java Card; Christoph Schiller for answering many questions about LaTeX; Johannes Reschreiter for his helpful information on smart cards in ski areas; Thomas Tarantino for helping with questions on card bodies; Michael Baldischweiler for his expert advice regarding USB, SWP and HCI; Peter Hildinger for reviewing the chapter on payment cards; Marcus Janke and Peter Laackmann for numerous tips and photos related to attacks on smart cards; Christopher Tarnovsky for his interesting photos of chip analysis equipment; Jürgen Hirschinger for his precise comments on the subject of testing; Harald Vater for answering many detailed questions on cryptography; Hermann Altschäfl for his practical advice on telecommunication applications; Peter van Elst and Dieter Weiß for their always prompt and knowledgeable answers to many small questions about cards; Irene Weilhart for her outstanding suggestions and expert assistance on the typography and layout of technical books; and Margarete Metzger for her astounding patience every time we postponed the delivery date yet again, and for being an ideal partner in this book project.

Our special thanks also go to the many dedicated readers of the *Smart Card Handbook*, whose questions, comments and suggestions have often led us to new and interesting insights.

Munich, June 2008

Wolfgang Rankl
[Wolfgang@wrankl.de]
[www.wrankl.de]

Wolfgang Effing
[Wolfgang.Effing@gi-de.com]

Symbols and Notation

- In accordance with ISO nomenclature, the least significant bit is designated 1.
- The most significant byte of concatenated data is at the beginning and the least significant byte is at the end. In other words, concatenated data is big-endian.
- In accordance with common usage, a byte is a series of eight bits.
- Length specifications of data, objects, and all countable quantities are represented in decimal notation.
- When used in connection with data quantities or memory quantities, the prefixes ‘kilo’, ‘mega’, and ‘giga’ have the values of 1 024 (2^{10}), 1 048 576 (2^{20}), and 1 073 741 824 (2^{30}).
- Binary values are used in a context-sensitive manner and are not explicitly identified as such.
- Smart card commands are set in uppercase characters (e.g. SELECT).
- As a rule, only good cases are shown in sequence diagrams.
- In diagrams, a solid arrow indicates a direction. By contrast, an open arrow is a pointer.
- Unless otherwise stated, all quantities are valid effective early 2008.
- In parameter coding tables for byte parameters consisting of two or more fields, the boundaries of the individual fields are marked by vertical rules.

Representation of characters and numbers

0, 1	binary value (used in a context-sensitive manner and not explicitly identified as such)
8	decimal value
'00'	hexadecimal value
"ABC"	ASCII value
b*n*	bit number *n* (e.g. b8)
B*n*	byte number *n* (e.g. B1)
D*n*	digit number *n* (e.g. D3)

References

See also ...	This is a reference to another location in the book.
[X Y]	This is a reference to additional literature listed in the Appendix or an Internet site. In case of a literature reference, X is the surname of the first-named author and Y is the last two digits of the year of publication. A reference to a website on the Internet consists of a unique abbreviated identifier and does not include a year number.

Cryptographic and data-related functions

$e = C(m)$	Compute the error detection code e of message m.
$t = T(d)$	Structure the data d using TLV coding. The result is the TLV-coded data t.
$p = P(d, v, l)$	Pad data d to an integer multiple of block length l using the value or method v. The result is the padded data p.
$c = E(p, k)$	Encrypt the plaintext p using a symmetric cryptographic algorithm and the secret key k. The result is the ciphertext c.
$p = D(c, k)$	Decrypt the ciphertext c using a symmetric cryptographic algorithm and the secret key k. The result is the plaintext p.
$a = M(m, k)$	Compute the message authentication code (MAC) of message m using the secret key k.
$s = S(m, sk)$	Sign the message m using the private key k.
$r = V(m, s, pk)$	Verify the signature s of message m using the public key pk. The result r is either true or false.
$h = H(m)$	Compute the hash value h of message m.
$C = (A, pk_A, S(A \parallel pk_A, sk_{CA}))$	Generate the certificate C of the public key pk_A of user A. This certificate is signed using the private key sk_{CA} of the certification authority CA.
$r = V(A \parallel pk_A, C, pk_{CA}))$	Verify the certificate C of the public key pk_A of user A using the public key pk_{CA} of the certification authority CA. The result r is either true or false.

Logical functions and program code

$=$	assignment operator (to be distinguished from the equality operator according to the context)
$=, \neq, <, >, \leq, \geq$	comparison operators
$+, -, \cdot, /$	arithmetic operators
$\|\|$	concatenation operator (e.g. concatenation of two data elements or data objects)

Program code

The syntax and semantics of the program code used in this book are based on current dialects of Basic. However, explanations in natural language may be used in a program listing for the sake of simplicity or clarity. Although this makes the code easier to understand for the reader, it prevents the code from being compiled automatically into machine code. This compromise is easily justified by the resulting significant improvement in readability.

:=	assignment operator
=, ! =, <, >, <=, >=	comparison operators
+, −, ∗, /	arithmetic operators
NOT	logical not
AND	logical and
OR	logical or
||	concatenation operator (e.g. coupling two byte strings)
_	end-of-line marker in a multiline instruction
// ...	comment marker
IO_Buffer	variable (set in italic)
Label:	jump destination or call target (set in bold)
GOTO ...	jump
CALL ...	function call or subroutine call
RETURN	return from a function or subroutine
IF ... THEN ...	decision, type 1
IF ... THEN ... ELSE ...	decision, type 2
SEARCH (...)	search in a list (search string in parentheses)
STATUS (...)	query the result of a previously executed function call
STOP	terminate a process
LENGTH (...)	calculate a length
EXIST	test for presence (e.g. of an objected or data element)
WITH ...	begin the declaration of a variable or an object as a reference
END WITH	end the declaration of a variable or an object as a reference

Abbreviations

μC	microcontroller
3DES	triple DES (data encryption standard) *(see glossary)*
3GPP	Third Generation Partnership Project *(see glossary)*
3GPP2	Third Generation Partnership Project 2 *(see glossary)*
3rd FF	third form factor
A-PET	amorphous polyethylene terephthalate
A3, A5, A8	GSM algorithm 3, 5, 8 *(see glossary)*
AAM	application abstract machine
ABA	American Bankers Association
ABS	acrylonitrile butadiene styrene
AC	access conditions *(see glossary)*
ACD	access control descriptor
ACK	acknowledge
ACM	accumulated call meter
ADF	application dedicated file
ADK	additional decryption key
ADN	abbreviated dialing number
AES	Advanced Encryption Standard *(see glossary)*
AFI	application family identifier
AFNOR	Association Française de Normalisation *(see glossary)*
AGE	Autobahngebührenerfassung (motorway toll collection)
AGE	automatische Gebührenerfassung (automatic toll collection)
AID	application identifier *(see glossary)*
AM	access mode
Amd.	amendment

AMPS	Advanced Mobile Phone Service *(see glossary)*
ANSI	American National Standards Institute *(see glossary)*
AoC	advice of charge
AODF	authentication object directory file
APACS	Association for Payment Clearing Services
APDU	application protocol data unit *(see glossary)*
API	application programming interface *(see glossary)*
AR	access rules
ARM	advanced RISC machine
ARR	access rule reference
ASC	application-specific command
ASCII	American Standard Code for Information Interchange
ASIC	application-specific integrated circuit
ASK	amplitude shift keying *(see glossary)*
ASN.1	Abstract Syntax Notation One *(see glossary)*
AT	attention
ATM	automated teller machine
ATQA	answer to request, type A
ATQB	answer to request, type B
ATR	answer to reset *(see glossary)*
ATS	answer to select
AUX1, AUX2	auxiliary 1, auxiliary 2
BAC	Basic Access Control
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BASIC	Beginners All Purpose Symbolic Instruction Code
BCD	binary-coded digit
Bellcore	Bell Communications Research Laboratories
BER	Basic Encoding Rules *(see glossary)*
BER-TLV	Basic Encoding Rules – tag, length, value
BEZ	Börsenevidenzzentrale(electronic purse clearing center for GeldKarte)
BGT	block guard time
BIBO	be-in / be-out
BIN	bank identification number
BIP	bearer independent protocol
bit	binary digit
BPF	basic processor functions
BPSK	binary phase-shift keying *(see glossary)*
BS	base station
BSI	Bundesamt für Sicherheit in der Informationstechnik
BWT	block waiting time
C-APDU	command APDU *(see glossary: command APDU)*
C-SET	Chip SET (secure electronic transaction)
CA	certification authority *(see glossary: certification authority)*
CAD	chip accepting device *(see glossary)*
CAFE	Conditional Access for Europe (EU project)
CAMEL	Customized Applications for Mobile Enhanced Logic

CAP	card application *(see glossary: CAP file)*
CAPI	crypto API (application programming interface)
CASCADE	Chip Architecture for Smart Card and Portable Intelligent Devices
CASE	computer-aided software engineering
CAT	card application toolkit
CAT_TP	card application toolkit transport protocol
CAVE	Cellular Authentication, Voice Privacy And Encryption
CBC	cipher block chaining
CC	Common Criteria *(see glossary)*
CCD	card coupling device
CCID	integrated circuit(s) cards interface device
CCITT	Comité Consultatif International Télégraphique et Téléphonique (now ITU) *(see glossary)*
CCR	chip card reader
CCS	cryptographic checksum *(see glossary)*
CD	committee draft
CDC	communications device class
CDF	certificate directory file
CDM	card dispensing machine
CDMA	code division multiple access *(see glossary)*
CEN	Comité Européen de Normalisation *(see glossary)*
CENELEC	Comité Européen de Normalisation Eléctrotechnique
CEPS	common electronic purse specifications *(see glossary)*
CEPT	Conférence Européenne des Postes et Télécommunications *(see glossary)*
CFB	cipher feedback
CGI	Common Gateway Interface
CHV	cardholder verification *or* cardholder verification information
CICC	contactless integrated chip card
CICO	check-in / check-out
CID	card identifier
CISC	complex instruction set computer
CLA	class
CLF	contactless front end
CLK	clock
CLn	cascade level n, type A
CMEA	Cellular Message Encryption Algorithm
CMM	capability maturity model *(see glossary)*
CMOS	complementary metal oxide semiconductor
CMS	card management system
CoD	clear on deselect
CoR	clear on reset
COS	chip operating system *(see glossary)*
COT	chip on tape *(see glossary)*
CPA	Common Payment Application
CPU	central processing unit
CRC	cyclic redundancy check *(see glossary)*

CRCF	clock rate conversion factor
CRT	Chinese remainder theorem
CRT	control reference template
Cryptoki	Cryptographic Token Interface
CSD	circuit-switched data
CT	card terminal
CT	cascade tag, type A
CT	chipcard terminal
CT	cordless telephone
CT-API	chipcard terminal API *(see glossary)*
CTDE	cryptographic token data element
CTI	cryptographic token information
CTIO	cryptographic token information object
CVM	cardholder verification method
CWT	character waiting time
D	divisor
D-AMPS	Digital Advanced Mobile Phone Service *(see glossary)*
DAD	destination address
DAM	DECT authentication module
DAM	draft amendment
DAP	data authentication pattern
DB	database
DBF	database file
DBMS	database management system
DC/SC	Digital Certificates on Smart Cards
DCODF	data container object directory file
DCS	digital cellular system
DEA	Data Encryption Algorithm *(see glossary)*
DECT	Digital Enhanced Cordless Telecommunications *(see glossary)*
DEMA	differential electromagnetic analysis
DER	Distinguished Encoding Rules *(see glossary)*
DES	Data Encryption Standard *(see glossary)*
DF	dedicated file *or* directory file *(see glossary)*
DFA	differential fault analysis *(see glossary)*
DG	data group
DIL	dual inline
DIN	Deutsche Industrienorm (German industrial standard)
DIS	draft international standard
DLL	dynamic link library
DMA	direct memory access
DO	data object
DoA	dead on arrival
DoD	Department of Defense (USA)
DOM	Document Object Model
DoS	denial of service
DOV	data over voice

DPA	differential power analysis *(see glossary)*
dpi	dots per inch
DR	divisor receive (PCD to PICC)
DRAM	dynamic random access memory *(see glossary)*
DRI	divisor receive integer (PCD to PICC)
DS	divisor send (PICC to PCD)
DSA	Digital Signature Algorithm
DSI	divisor send integer (PICC to PCD)
DSS	digital signature standard
DTD	Document Type Definition
DTMF	dual tone multiple frequency
DVD	digital versatile disc
E	end of communication, Type A
E^2PROM	electrically erasable programmable read-only memory
EAC	extended access control
EAP	Extensible Authentication Protocol
EAP-SIM	extensible authentication protocol security identity module
EBCDIC	Extended Binary Coded Decimal Interchange Code
EC	elliptic curve *or* elliptic curve cryptoalgorithm
ec	Eurocheque
ECB	electronic code book
ECBS	European Committee for Banking Standards *(see glossary)*
ECC	elliptic curve cryptosystems *(see glossary)*
ECC	error correction code *(see glossary)*
ECC	EU Citizen Card
ECDSA	Elliptic Curve Digital Signature Algorithm (DSA)
ECML	Electronic Commerce Modelling Language
ECTEL	European Telecom Equipment and Systems Industry
EDC	error detection code *(see glossary)*
EDGE	Enhanced Data Rates for GSM and TDMA Evolution *(see glossary)*
EDI	electronic data interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EEM	Ethernet emulation model
EEPROM	electrically erasable programmable read-only memory *(see glossary)*
EF	elementary file *(see glossary)*
EFF	Electronic Frontier Foundation
EFI	EF internal
EFTPOS	electronic fund transfer at point of sale
EFW	EF working
eGK	elektronische Gesundheitskarte (German electronic health care card)
EGT	extra guard time, type B
EHIC	European Health Insurance Card
EMV	Europay, MasterCard, Visa *(see glossary)*
EOF	end of frame, type B
EOP	end of packet

EP	endpoint
EPA	elektronische Patientenakte (electronic patient file)
EPROM	erasable programmable read-only memory *(see glossary)*
ESD	electrostatic discharge
ETS	European Telecommunication Standard *(see glossary)*
ETSI	European Telecommunications Standards Institute *(see glossary)*
etu	elementary time unit *(see glossary)*
ET	evaluation target *(see glossary)*
f	following page
F2F	face to face
FAQ	frequently asked questions
FAR	false acceptance rate
FAT	file allocation table *(see glossary)*
f_C	frequency of operating field (carrier frequency)
FCB	file control block
FCC	Federal Communications Commission
FCFS	first come, first served
FCI	file control information
FCOS	flip chip on substrate
FCP	file control parameters
FD/CDMA	frequency division / code division multiple access *(see glossary)*
FDMA	frequency division multiple access *(see glossary)*
FDN	fixed dialing number
FDT	frame delay time, type A
FEAL	Fast Data Encipherment Algorithm
FET	field effect transistor
ff	following pages
FID	file identifier *(see glossary)*
FIFO	first in, first out
FINEID	Finnish Electronic Identification Card
FIPS	Federal Information Processing Standard *(see glossary)*
FMD	file management data
FN	Fowler–Nordheim effect
FO	frame option
FPGA	field programmable gate array
FPLMTS	Future Public Land Mobile Telecommunication Service *(see glossary)*
FRAM	ferroelectric random access memory *(see glossary)*
FRR	false rejection rate
FS	file system
f_S	frequency of subcarrier modulation
FSC	frame size for proximity card
FSCI	frame size for proximity card integer
FSD	frame size for coupling device
FSDI	frame size for coupling device integer
FSK	frequency-shift keying
FTAM	file transfer, access, and management

FTL	flash translation layer *(see glossary)*
FWI	frame waiting time integer
FWT	frame waiting time
FWTTEMP	temporary frame waiting time
GF	Galois field
GGSN	gateway GPRS support node
GMT	Greenwich Mean Time
GND	ground (electrical)
GNU	GNU's not Unix
GP	Global Platform *(see glossary)*
GPL	GNU general public license
GPRS	General Packet Radio System *(see glossary)*
GPS	Global Positioning System
GSM	Global System for Mobile Communications *(see glossary)*
GSMA	GSM Association
GTS	GSM Technical Specification
GUI	graphical user interface
HAL	hardware abstraction layer *(see glossary)*
HBA	Heilberufsausweis (health professional ID card)
HBCI	Home Banking Computer Interface *(see glossary)*
HCI	host controller interface
HiCo	high coercivity
HLTA	halt command, type A
HLTB	halt command, type B
HMAC	keyed hash message authentication code (MAC)
HPC	health professional card
HSCSD	high-speed circuit-switched data
HSM	hardware security module
HSM	high-security module
HSP	High-speed Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HV	Vickers hardness
HW	hardware
I block	information block
I/O	input/output
I^2C	inter-integrated circuit
IATA	International Air Transport Association
IBAN	international bank account number
IBE	identity-based encryption
ICAO	International Civil Aviation Organization
ICC	integrated circuit card *(see glossary)*
ICCD	integrated circuit(s) card device
ICCSN	ICC serial number
ID	identifier

IDEA	International Data Encryption Algorithm
IEC	International Electrotechnical Commission *(see glossary)*
IEEE	Institute of Electrical and Electronics Engineers
IEP	inter-sector electronic purse
IFD	interface device *(see glossary)*
IFS	information field size
IFSC	information field size for the card
IFSD	information field size for the interface device
IIC	institution identification codes
IMEI	international mobile equipment identity
IMSI	international mobile subscriber identity
IMT-2000	International Mobile Telecommunication 2000 *(see glossary)*
IN	intelligent network
INF	information field
INS	instruction
INTAMIC	International Association of Microcircuit Cards
IP	Internet protocol
IPES	Improved Proposed Encryption Standard
IPR	intellectual property rights
IrDA	Infrared Data Association
ISDN	Integrated Services Digital Network *(see glossary)*
ISF	internal secret file
ISIM	IP security identity module
ISO	International Organization for Standardization *(see glossary)*
IT	information technology
ITSEC	Information Technology Security Evaluation Criteria *(see glossary)*
ITU	International Telecommunications Union *(see glossary)*
IuKDG	Informations- und Kommunikations-Gesetz (Information and Communication Act)
IV	initialization vector
IVU	in-vehicle unit
J2ME	Java 2 Micro Edition
JC	Java Card
JCF	Java Card Forum *(see glossary)*
JCP	Java Community Process
JCRE	Java Card runtime environment *(see glossary)*
JCVM	Java Card virtual machine *(see glossary)*
JDK	Java Development Kit *(see glossary)*
JECF	Java electronic commerce framework
JFFS	journaling flash file system
JIT	just in time
JSR	Java specification request
JTC1	Joint Technical Committee One
JVM	Java virtual machine
K	key
Kc	ciphering key

KCV	check value key
KD	derived key
KFPC	key fault presentation counter
Ki	individual key
KID	key identifier
KM	master key
KS	session key
KVK	Krankenversichertenkarte (health insurance card)
LA	location area
LAN	local area network
L_c	length command
LCSI	life cycle status indicator
LDS	logical data structure
L_e	expected length
LEN	length
LFSR	linear feedback shift register
LIFO	last in, first out
LLC	logical link control
LND	last number dialed
LOC	lines of code
LoCo	low coercivity
LPDU	link protocol data unit
LRC	longitudinal redundancy check
LSAM	load secure application module
lsb	least significant bit
LSB	least significant byte
M	month
M2M	machine to machine *(see glossary)*
MAC	medium access control
MAC	message authentication code *(see glossary)*
MAO	multiapplication operating system
MBL	maximum buffer length
MBLI	maximum buffer length index
MCU	microcontroller unit
MD5	message digest algorithm 5
ME	mobile equipment
MEL	Multos Executable Language
MExE	mobile station execution environment *(see glossary)*
MF	master file *(see glossary)*
MFC	multifunction card
MIME	Multipurpose Internet Mail Extensions
MIPS	microprocessor without interlocked pipeline stages
MIPS	million instructions per second
MKT	Multifunktionales Kartenterminal (multifunctional card terminal) *(see glossary)*
MLC	multilevel cell

MLI	multiple laser image
MM	moduliertes Merkmal
MMI	man–machine interface
MMS	multimedia messaging service
MMU	memory management unit
MOC	match on card
MOO	mode of operation
MOSAIC	microchip on surface and in card
MOSFET	metal oxide semiconductor field effect transistor
MoU	memorandum of understanding *(see glossary)*
MRTD	machine-readable travel document
MRZ	machine-readable zone
MS	mobile station
msb	most significant bit
MSB	most significant byte
MSC	mass storage class
MSE	MANAGE SECURITY ENVIRONMENT
MTBF	mean time between failures
MUSCLE	Movement for the Use of Smart Cards in a Linux Environment
NAD	node address
NAK	negative acknowledgment
NBS	National Bureau of Standards (USA) *(see glossary)*
NCSC	National Computer Security Center (USA) *(see glossary)*
NDA	nondisclosure agreement
NFC	near field communication
NIST	National Institute of Standards and Technology (USA) *(see glossary)*
NOK	not OK
NOP	no operation
NPU	numeric processing unit *(see glossary)*
NRZ	non return to zero
NRZI	non return to zero inverted
NSA	National Security Agency (USA) *(see glossary)*
NU	not used
NVB	number of valid bits
NVM	nonvolatile memory
OBU	onboard unit
OCF	Open Card Framework
OCR	optical character recognition
ODF	object directory file
OFB	output feedback
OID	object identifier
OMA	Open Mobile Alliance (formerly WAP)
OOK	on/off keying
OP	Open Platform *(see glossary)*
OS	operating system
OSI	Open Systems Interconnect

OTA	Open Terminal Architecture
OTA	over the air *(see glossary)*
OTASS	over the air SIM services
OTP	one-time password
OTP	one-time programmable
OTP	Open Trading Protocol
OVI	optically variable ink
P1, P2, P3	parameter 1, 2, 3
PA	power analysis
PACE	Password Authenticated Connection Establishment
PB	procedure byte
PC	personal computer
PC	polycarbonate
PC/SC	Personal Computer / Smart Card *(see glossary)*
PCB	protocol control byte
PCD	proximity coupling device *(see glossary)*
PCMCIA	Personal Computer Memory Card International Association
PCN	personal communication networks
PCS	personal communication system
PDA	personal digital assistant
PES	Proposed Encryption Standard
PET	polyethylene terephthalate
PETP	partially crystalline polyethylene terephthalate
PGP	Pretty Good Privacy
PICC	proximity ICC *(see glossary)*
PIN	personal identification number
PIX	proprietary application identifier extension
PKCS	Public Key Cryptography Standards *(see glossary)*
PKI	public key infrastructure *(see glossary)*
PLL	phase locked loop
PLMN	public land mobile network *(see glossary)*
PM	person month
POD	production on demand
POS	point of sale *(see glossary)*
POZ	POS ohne Zahlungsgarantie (type of payment transaction)
PP	protection profile *(see glossary)*
PPC	production planning and control
PPM	pulse position modulation
PPP	Point-to-point Protocol
PPS	protocol parameter selection
prEN	preliminary Europe Standard
prETS	preliminary European Telecommunication Standard
PrKDF	private key directory file
PRNG	pseudorandom number generator *(see glossary)*
PROM	programmable read-only memory
PSAM	purchase secure application module

PSK	phase shift keying
PSO	PERFORM SECURITY OPERATION
PSTN	public switched telephone network *(see glossary)*
PTS	protocol type selection
PTT	Post, Telegraph and Telephone
Pub	publication
PUK	personal unblocking key *(see glossary)*
PuKDF	public key directory file
PUPI	pseudo-unique PICC identifier
PVC	polyvinyl chloride
PWM	pulse width modulation
QFN	quad flat pack, no leads
R-APDU	response APDU *(see glossary)*
R-UIM	removable user identity module *(see glossary)*
RACE	Research and Development in Advanced Communication Technologies in Europe
RAM	random access memory *(see glossary)*
RATS	request to answer to select
Reg TP	Regulierungsbehörde für Telekommunikation und Post
REJ	reject
REQA	request command, type A
REQB	request command, type B
RES	resynchronisation
RF	radio frequency
RFC	Request for Comment
RFID	radio frequency identification
RFU	reserved for future use
RID	record identifier
RID	registered application provider identifier
RIPE	RACE Integrity Primitives Evaluation
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RISC	reduced instruction set computer
RMI	remote method invocation
RND	random number
RNDIS	remote network device interface specification
RNG	random number generator
ROM	read-only memory *(see glossary)*
RS	Reed–Solomon
RSA	Rivest, Shamir and Adleman Algorithm
RST	reset
RTE	runtime environment
S	start of communication
S-HTTP	Secure Hypertext Transfer Protocol
S^2C	SigIn–SigOut Connection
S@T	SIM Alliance Toolbox

S@TML	SIM Alliance Toolbox Markup Language
SA	security attributes
SA	service area
SAD	source address
SAGE	Security Algorithm Group of Experts
SAK	select acknowledge
SAM	secure application module *(see glossary)*
SAS	Security Accreditation Scheme
SAT	SIM Application Toolkit *(see glossary)*
SATSA	security and trust services API
SC	security conditions
SC	smart card
SCC	smart card controller
SCMS	smart card management system
SCOPE	smart card open platform environment *(see glossary)*
SCP	smart card platform
SCQL	Structured Card Query Language
SCSUG	Smart Card Security Users Group
SCWS	smart card web server
SDL	Specification and Description Language
SDMA	space division multiple access *(see glossary)*
SE	security environment *(see glossary)*
SECCOS	Secure Chip Card Operating System *(see glossary)*
SEIS	Secured Electronic Information In Society
SEL	select code
SEMA	simple electromagnetic analysis
SEMPER	Secure Electronic Marketplace for Europe (EU project)
SEPP	Secure Electronic Payment Protocol
SET	secure electronic transaction *(see glossary)*
SFGI	start-up frame guard time integer
SFGT	start-up frame guard time
SFI	short file identifier
SGSN	serving GPRS support node
SigG	Signaturgesetz *(see glossary)*
SigV	Signaturverordnung *(see glossary)*
SIM	subscriber identity module *(see glossary)*
SIMEG	subscriber identity module expert group *(see glossary)*
SKDF	secret key directory file
SLC	single-level cell
SM	secure messaging
SM	security mechanism
SMD	surface mounted device
SMG9	Special Mobile Group 9 *(see glossary)*
SMIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service *(see glossary)*
SMS-PP	Short Message Service Point to Point

SMSC	Short Message Service Center
SOF	start of frame
SOP	small outline package
SOP	start of packet
SPA	simple power analysis *(see glossary)*
SPU	standard or proprietary use
SQL	Structured Query Language
SQUID	superconducting quantum interference device
SRAM	static random access memory *(see glossary)*
SRES	signed response
SS	supplementary service
SSC	send sequence counter
SSCD	secure signature creation device
SSL	secure socket layer
SSO	single sign-on *(see glossary)*
STARCOS	Smart Card Chip Operating System (G+D)
STC	sub-technical committee
STK	SIM Application Toolkit *(see glossary)*
STT	secure transaction technology
SVC	Stored Value Card (Visa International)
SW	software
SW1, SW2	status word 1, 2
SWIFT	Society for Worldwide Interbank Financial Telecommunications
SWP	Single-wire Protocol
T	tag
TAB	tape automated bonding
TACS	Total Access Communication System
TAL	terminal application layer
TAN	transaction number *(see glossary)*
TAR	toolkit application reference
tbd	to be defined
TC	technical committee
TC	thermochrome
TC	trust center *(see glossary)*
TCOS	Telesec Card Operating System
TCP	Transport Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria *(see glossary)*
TD/CDMA	time division / code division multiple access *(see glossary)*
TDES	triple DES *(see glossary)*
TDMA	time division multiple access *(see glossary)*
TETRA	Trans-European Trunked Radio *(see glossary)*
TLS	transport layer security
TLV	tag length value *(see glossary: TLV format)*
TMSI	temporary mobile subscriber identity
TOE	target of evaluation *(see glossary)*
TPD	trusted personal device *(see glossary)*

TPDU	transmission protocol data unit *(see glossary)*
TRNG	true random number generator *(see glossary: random number generator)*
TS	technical specification
TSCS	The Smart Card Simulator
TTCN	Tree And Tabular Combined Notation
TTL	terminal transport layer
TTL	transistor–transistor logic
TTP	trusted third party *(see glossary)*
UART	universal asynchronous receiver transmitter *(see glossary)*
UATK	UIM Application Toolkit
UCS	Universal Character Set *(see glossary)*
UDP	User Datagram Protocol
UI	user interface
UICC	universal integrated chip card *(see glossary)*
UID	unique identifier
UIM	user identity module *(see glossary)*
UML	Unified Modeling Language *(see glossary)*
UMTS	Universal Mobile Telecommunication System *(see glossary)*
URL	uniform resource locator *(see glossary)*
USAT	USIM Application Toolkit *(see glossary)*
USB	Universal Serial Bus *(see glossary)*
USIM	Universal Subscriber Identity Module *(see glossary)*
USSD	unstructured supplementary services data
UTF	UCS transformation format
UTRAN	UMTS radio access network
VAS	value-added services *(see glossary)*
Vcc	supply voltage
VCD	vicinity coupling device
VEE	Visa Easy Entry *(see glossary)*
VICC	vicinity integrated chip card
VLSI	very large scale integration
VM	virtual machine *(see glossary)*
VOP	Visa Open Platform *(see glossary)*
Vpp	programming voltage
VSI	vertical system integration
W3C	World Wide Web Consortium
WAE	wireless application environment
WAN	wide area network
WAP	Wireless Application Protocol *(see glossary)*
WCDMA	wideband code division multiple access *(see glossary)*
WDP	Wireless Datagram Protocol
WfSC	Windows for Smart Cards
WG	working group
WIG	wireless Internet gateway
WIM	wireless identification module *(see glossary)*

WML	Wireless Markup Language *(see glossary)*
WORM	write once, read multiple
WSP	wafer-scale package
WSP	Wireless Session Protocol
WTAI	Wireless Telephony Application Interface
WTLS	Wireless Transport Layer Security
WTP	Wireless Transport Protocol
WTX	waiting time extension
WTXM	waiting time extension multiplier
WUPA	wake-up command, type A
WUPB	wake-up command, type B
WWW	World Wide Web *(see glossary)*
XML	Extensible Markup Language *(see glossary)*
XOR	logical exclusive OR operation
Y	year
ZKA	Zentraler Kreditausschuss *(see glossary)*

1
Introduction

This book is intended for students, engineers, and technically minded persons who want to learn more about smart card technology. It attempts to cover this broad topic as completely as possible, in order to provide the reader with a general understanding of the fundamentals and the current state of the technology.

We have put great emphasis on a practical approach. The wealth of illustrations, tables and references to real applications is intended to help the reader become familiar with the subject much faster than would be possible with a strictly technical approach. Consequently, this book is intended to be practically useful instead of academically complete. This is also the reason for making the descriptions as illustrative as possible. In places where we were faced with a choice between academic accuracy and ease of understanding, we have tried to strike a happy medium. Where this was not possible, we have given the preference to ease of understanding.

The book is structured such that it can be read in the usual way, from front to back. We have tried to avoid forward references as much as possible. The structure and content of the individual chapters are formulated to allow them to be read individually without any loss of understanding. A comprehensive index and a glossary allow this book to be used as a reference work. If you wish to know more about a specific topic, the references in the text and the annotated directory of standards will help you find the relevant documents.

Unfortunately, a large number of abbreviations have become established in smart card technology, as in so many other areas of technology and everyday life. This makes it particularly difficult for newcomers to become familiar with the subject. We have tried to minimize the use of these cryptic and frequently illogical abbreviations. Nevertheless, we have often had to choose a middle way between internationally accepted smart card terminology used by specialists and common terms more easily understood by laypersons. If we have not always succeeded, the extensive list of abbreviations should at least help overcome any barriers to understanding, 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 abbreviations.

An important feature of smart cards is that their properties are strongly based on international standards. This is also essential for interoperability, which is a fundamental requirement in most applications. Unfortunately, these standards are often difficult to understand, and in some problematic places they require outright interpretation. Sometimes only the members of the relevant standardization group can explain the intended meaning of certain sections. In such

Smart Card Handbook: Fourth Edition Wolfgang Rankl and Wolfgang Effing

cases, *The Smart Card Handbook* attempts to present the meaning generally accepted in the smart card industry. Nevertheless, the relevant standards remain the ultimate authority, and in such cases they should always be consulted.

1.1 THE HISTORY OF SMART CARDS

The proliferation of plastic cards began in the USA in early 1950s. The low price of the synthetic material PVC made it possible to produce robust, durable plastic cards that were much more suitable for everyday use than the paper and cardboard cards previously used, which could not adequately withstand mechanical stresses 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 individuals, and thus also served as a status symbol, allowing the holder to pay with his or her 'good name' instead of cash. Initially, only the more select restaurants and hotels accepted these cards, so this type of card came to be known as a 'travel and entertainment' card.

The entry of Visa and MasterCard into the field led to a very rapid proliferation of 'plastic money' in the form of credit cards. This occurred first in the USA, with Europe and the rest of the world following a few years later.

Today, credit cards allow travelers to shop without cash everywhere in the world. A cardholder is never at a loss for means of payment, yet he or she avoids exposure to the risk of loss due to theft or other unpredictable hazards, particularly while traveling. Using a credit card also eliminates the tedious task of exchanging currency when traveling abroad. These unique advantages helped credit cards become rapidly established throughout the world. Billions of cards are produced and issued annually.

At first, the functions of these cards were quite simple. They served as data storage media that were secure against forgery and tampering. General data, such as the card issuer's name, was printed on the surface, while personal data, such as the cardholder's name and the card number, was embossed. Many cards also had a signature panel where 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 panel. Consequently, the system's security depended largely on the experience and conscientiousness of the employees of the card-accepting organization. However, this did not represent an overwhelming problem, due to the card's initial exclusivity. With the increasing proliferation of card use, these rather rudimentary functions and security technology were no longer adequate, particularly since threats from organized criminals were growing apace.

Increasing handling costs for merchants and banks made a machine-readable card necessary, while at the same time, losses suffered by card issuers as the result of customer insolvency and fraud grew from year to year. It became apparent that the security features for protection against fraud and manipulation, as well as the basic functions of the card, had to be expanded and improved.

The first improvement consisted of a magnetic stripe on the back of the card, which allowed digital data to be stored on the card in machine-readable form as a supplement to the visual information. This made it possible to minimize the use of paper receipts, which were previously essential, although the customer's signature on a paper receipt was still required in traditional credit card applications as a form of personal identification. However, new approaches that rendered paper receipts entirely unnecessary could also be devised. This made it possible to

finally achieve the long-standing objective of replacing paper-based transactions by electronic data processing. This required a different method to be used for user identification, which previously employed the user's signature. The method that has come into widespread general use involves a secret personal identification number (PIN) that is compared with a reference number in a terminal or a background system. Most people are familiar with this method from using bank cards in automated teller machines. Embossed cards with a magnetic stripe and a PIN code are still the most commonly used type of payment card.

However, magnetic-stripe technology has a crucial weakness, which is that the data stored on the stripe can be read, deleted and rewritten at will by anyone with access to a suitable magnetic card reader/writer. It is thus unsuitable for storing confidential data. Additional techniques must be used to ensure confidentiality of the data and prevent manipulation of the data. For example, the reference value for the PIN can be stored in the terminal or host system in a secure environment, instead of on the magnetic stripe in unencrypted form. Most systems that employ magnetic-stripe cards thus use online connections to the system's host computer for reasons of security, even though this generates significant costs for the necessary data transmission. In order to minimize costs, it is necessary to find solutions that allow card transactions to be executed offline without endangering the security of the system.

The development of the smart card, combined with the expansion of electronic data processing systems, has created completely new possibilities for devising such solutions.

In the 1970s, rapid progress in microelectronics made it possible to integrate nonvolatile data memory and processing 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 by Kunitaka Arimura in Japan. However, real progress in the development of smart cards began 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 necessary 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 at a reasonable cost.

The basic inventions in smart card technology originated in Germany and France, so it is not surprising that these countries played the leading roles in the development and marketing of smart cards.

The great breakthrough was achieved in 1984, when the French PTT (postal and telecommunication services authority) successfully carried out a field trial with telephone cards. In this field trial, smart cards immediately proved to meet all expectations with regard to high reliability and protection against manipulation. Significantly, this 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 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 several technologies. Magnetic-stripe cards, optical-storage (holographic) cards and smart cards were used in comparative tests.

Smart cards proved to be the winners in this pilot study. In addition to a high degree of reliability and security against manipulation, smart card technology promised the greatest

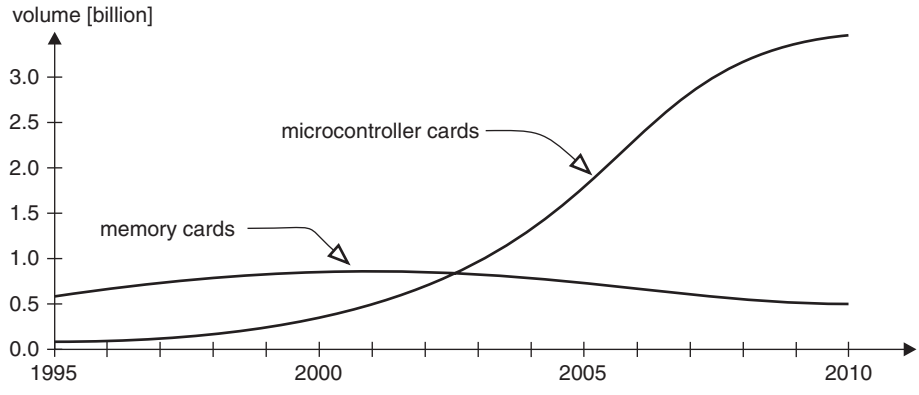

Figure 1.1 Worldwide production figures for memory cards and processor cards. The numbers are estimated values, since the various sources differ considerably. Average values have been used here

degree of flexibility for future applications. Although the older but less expensive EPROM technology was used in the French telephone card chips, newer EEPROM chips were used from the start in German telephone cards. The latter type of chip does not need an external programming voltage. An unfortunate consequence is that the French and German telephone cards are mutually incompatible. 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 rose to nearly 60 million in 1990, and to several hundred million worldwide in 1997.

Germany experienced similar progress, with a time lag of about three years. These systems were marketed throughout the world after the successful introduction of the smart card public telephone in France and Germany. Telephone cards incorporating chips are currently used in more than 50 countries. However, the use of telephone cards in their original home countries (France and Germany), as well as in highly industrialized countries in general, has declined dramatically in the last decade due to the widespread availability of inexpensive mobile telecommunication networks and the general use of mobile telephones.

The integrated circuits used in telephone cards are relatively small, simple and inexpensive memory chips with specific security logic that allows the card balance to be reduced while protecting it against manipulation. Microprocessor chips, which are significantly larger and more complex, were first used in large numbers in telecommunication applications, specifically for mobile telecommunication. The production trends of smart cards with memory chips (memory cards) and smart cards with microprocessor chips (microcontroller cards) in recent years are shown in Figure 1.1.

In 1988, the German Post Office acted as a pioneer in this area by introducing a modern processor card using EEPROM technology as an authorization card for the analog mobile telephone network (C-Netz). The reason for introducing such cards was an increasing incidence of fraud with the magnetic-stripe cards used up to that time. For technical reasons, the analog mobile telephone network was limited to a relatively small number of subscribers (around one million), so it was not a true mass market for processor cards. However, the positive experience gained from using smart cards in the analog mobile telephone system was decisive for the introduction of smart cards in the digital GSM network. This network was put into service in

1991 in various European countries and has presently expanded over the entire world, with more than three billion subscribers in nearly every country of the world.

Progress was significantly slower in the bank card area, in part due to the more stringent security requirements and higher complexity of bank cards compared with 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 crucial for the proliferation of bank cards as developments in semiconductor technology.

With the widespread use of electronic data processing in the 1960s, the discipline of cryptography experienced a sort of quantum leap. Modern, high-performance hardware and software made it possible to implement complex, sophisticated mathematical algorithms in single-chip processors, which allowed previously unparalleled levels of security to be achieved. Moreover, this new technology was available to everyone, in contrast to the previous situation in which cryptography was a covert science in the private reserve of the military and secret services.

With these modern cryptographic algorithms, the strength of the security mechanisms in electronic data processing systems could be mathematically calculated. It was no longer necessary to rely on a highly subjective assessment of conventional techniques, whose security essentially rests on the secrecy of the methods 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 could safely store secret keys and execute cryptographic algorithms. In addition, smart cards are so small and easy to handle that they can be carried and used everywhere by everybody in everyday life. It was a natural idea to attempt to use these new security features for bank cards, in order to come to grips with the security risks arising from the increasing use of magnetic-stripe cards.

The French banks were the first to introduce this fascinating technology in 1984, after completion of a pilot project with 6000 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, using a multifunctional payment card incorporating a chip. However, the Zentrale Kreditausschuss (ZKA), which is the coordinating 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 capability, an electronic purse, and optional value-added services 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 making payments was the adoption of the EMV specification, a product of the joint efforts of Europay, MasterCard and Visa. The first version of this specification was published in 1994. It provides a detailed description of the operation of credit cards incorporating processor chips, and it ensures the worldwide compatibility of the smart cards of the three largest credit card organizations. Hundreds of millions of EMV cards are presently in use worldwide.

With a delay of around ten years relative to normal contact smart cards, the technology of contactless smart cards has developed to the point of market maturity. With contactless cards, an electromagnetic field is used to supply power to the cards and exchange data with the terminal, without any electrical contact. The majority of currently issued EMV cards use this technology to enable fast, convenient payment for small purchases.

In the 1990s, it was anticipated that electronic purses, which store money in a card and can be used for offline payment, would prove to be another driver for the international proliferation

of smart cards for payment transactions. The first such system, called Danmønt, was put into service in Denmark in 1992. There are presently more than twenty national systems in use in Europe alone, many of which are based on the European EN 1546 standard. The use of such systems is also increasing outside of Europe. Payment via the Internet offers a new and promising application area for electronic purses. However, a satisfactory solution to the difficulties involved in using the public Internet medium to make payments securely but anonymously throughout the world, including small payments, has not yet been found. Smart cards could play a decisive role in such a solution.

The anticipated pioneering success of electronic purses has failed to materialize up to now. Most installed systems remain far below the original highly optimistic expectations, which among other things can be attributed to the fact that fees for online transactions have decreased dramatically, with the result that one of the key advantages of electronic purse systems – cost savings resulting from offline capability – has largely vanished. Today the electronic purse function is often included as a supplementary application in multifunction smart cards for payment transactions.

Another potentially important application for smart cards is as personal security devices for electronic signatures, which are slowly becoming established in several European countries after the legal basis for their use was created in 1999 when the European Parliament adopted an EU directive on digital signatures.

Another application has resulted the issuing of smart cards to nearly all the citizens of several countries. These smart cards serve as health insurance cards, which are issued to the insured persons and which contribute to cost savings in the billing of services to health insurance organizations. In most cases, the first cards to be issued were simple memory cards containing only the personal data of the insured person necessary for identification, but the patient cards now in common use contain complex security microcontrollers that also make it possible to store prescriptions and patient files, and to use electronic signatures to enable secure access to centrally stored data via the Internet.

The high functional flexibility of smart cards, which even allows programs for new applications to be added to a card already in use, has opened up completely new application areas, extending beyond the boundaries of traditional card uses.

As already mentioned, the technology of contactless smart cards has reached a level of maturity that enables economical mass production. For this reason, contactless smart cards are used as electronic tickets for local public transport in many cities throughout the world. In addition, this technology has established a firm position in electronic passports. Although electronic passports do not have the same size or shape as a credit card, which is standardized as an ID-1 card, under the cover they have the same circuitry as a contactless smart card, consisting of a security microcontroller connected to an antenna coil for contactless data exchange.

Intensive efforts are presently underway at the European level to achieve standardization of a contactless electronic card to be issued to all citizens, which will have an ID1 form factor (the same as a credit card) and is intended to be used as a personal identification card, among other things.

Although the history of smart cards and their applications goes back more than 25 years, a steady stream of promising new applications is still being developed. The increasing, almost omnipresent networking of our world creates major problems with regard to the security, confidentiality, and anonymity of personal data. Smart cards as personal security devices, with their ability to store and encode data securely, can make a major contribution to solving these problems.

1.2 CARD TYPES AND APPLICATIONS

As can be seen from the historical summary, the potential applications of smart cards are extremely diverse. With the steadily increasing storage and processing capacities of available integrated circuits, the range of potential applications is constantly expanding. Since it is impossible to describe all of these applications in detail within the confines of this book, a few typical examples must serve to illustrate the basic properties of smart cards. This introductory chapter is only meant to provide an initial overview of the functional versatility of these cards. Some typical application areas with their memory and processing capacities are shown in Figure 1.2, and several typical applications are described in detail in later chapters.

To make this overview easier to follow, it is helpful to divide smart cards into two categories: memory cards and processor cards.

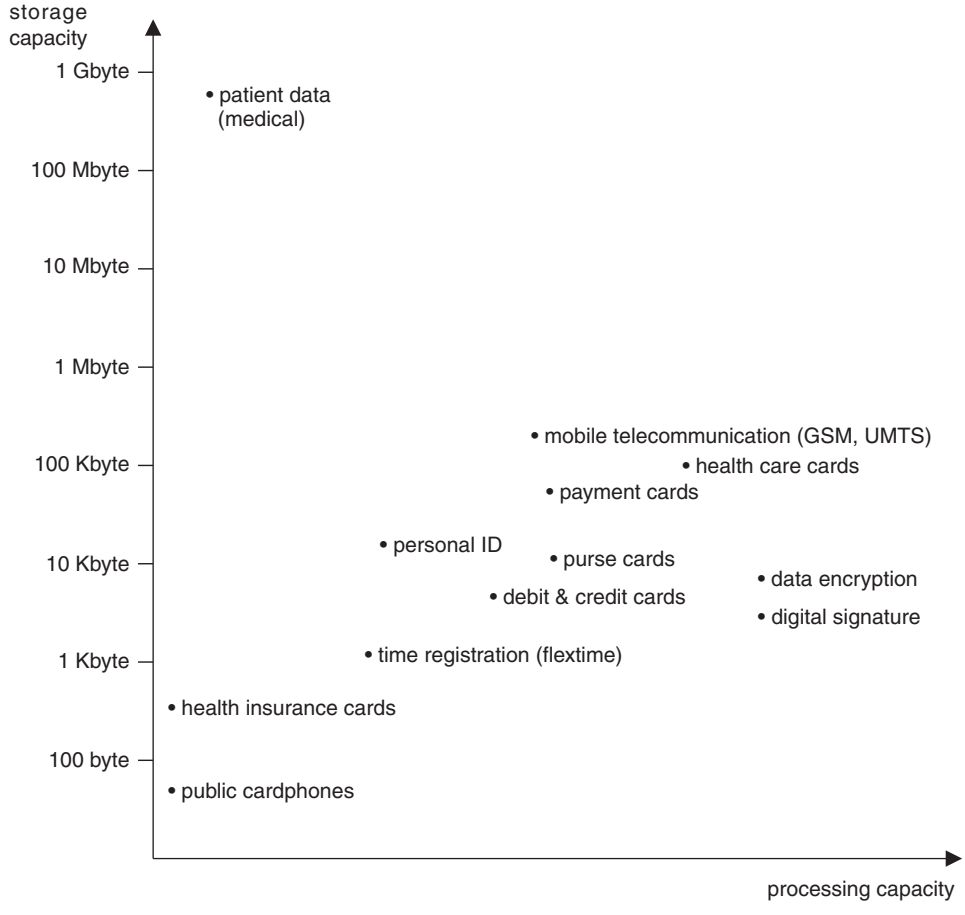

Figure 1.2 Typical smart card application areas, and the required memory capacity and arithmetic processing capacity

1.2.1 Memory cards

The first smart cards used in large quantities were memory cards for telephone applications. These cards are prepaid, with the value stored electronically in the chip being decreased by the amount of the calling charge each time the card is used. Naturally, it is necessary to prevent the user from subsequently increasing the stored value, which could easily be done with a magnetic-stripe card. With such a card, all the user would have to do is record the data stored at the time of purchase and rewrite it to the magnetic stripe after using the card. The card would then have its original value and could be reused. This type of manipulation, known as buffering, is prevented in smart phone cards by security logic in the chip that makes it impossible to erase a memory cell once it has been written. Decreasing the card balance 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, vending machines of all types, cafeterias, swimming pools, car parks and so on. The advantage of this type of card lies in its simple technology (the surface area of the chip 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 German health insurance card, which has been issued since 1994 to all persons enrolled in the national health insurance plan. The information previously written on the patient's card is now stored in the chip and printed or laser-engraved on the card. Using a chip for data storage makes the cards machine-readable using simple equipment. However, the next generation of German health insurance cards will have a security microcontroller and significantly expanded functionality.

In summary, we can say that memory cards have limited functionality. Their integrated security logic makes it possible to protect stored data against manipulation. They are suitable for use as prepaid cards or identification cards in systems where low cost is a primary consideration.

1.2.2 Processor cards

As already mentioned, processor cards were first used as bank cards in France. Their ability to store secret keys securely and to execute modern cryptographic algorithms made it possible to implement highly secure offline payment systems.

As the processor embedded in the card is freely programmable, the functionality of processor cards is restricted only by the available memory and the computing power of the processor. The only limits to the designer's imagination when implementing smart card systems are thus technological, and they are extended enormously with each new generation of integrated circuits.

As the prices of processor cards steadily decline due to mass production and ongoing technological progress, more and more new applications are developed. The use of smart cards with mobile telephones has been especially important for their international proliferation.

After being successfully tested in the German national C-Netz (analog mobile telephone network) for use in mobile telephones, smart cards were specified as the access medium for the European digital mobile telephone system (GSM). In part, this was because smart cards allowed a high degree of security to be achieved for accessing the mobile telephone network.

At the same time, they provided new possibilities and thus major advantages in marketing mobile telephones, since they made it possible for network operators and service providers to sell telephones and services separately. Without smart cards, mobile telephones would certainly not have spread so quickly across Europe or developed into a worldwide standard.

Other potential applications for processor cards include identification cards, access control systems for restricted areas and computers, secure data storage, electronic signatures, electronic purses, and multifunctional cards incorporating several applications in a single card. Modern smart card operating systems also allow new applications to be loaded into a card after it has been issued to the user, without endangering the security of the various applications. This new flexibility opens up completely new application areas.

For example, personal security modules are indispensable if Internet commerce and payments are to be made trustworthy. Such security modules can securely store personal keys and execute high-performance cryptographic algorithms. This task can be handled elegantly by a processor card with a cryptographic coprocessor.

In summary, we can say that the essential advantages of processor cards are large storage capacity, secure storage of confidential data, and the ability to execute cryptographic algorithms. These advantages make a wide range of new applications possible, in addition to the traditional bank card application. The potential of smart cards is by no means yet exhausted, and furthermore, it is constantly being expanded by progress in semiconductor technology.

1.2.3 Contactless cards

The rapid progress of integrated circuit technology has led to a dramatic decrease in the power consumption of smart card microcontrollers. As a result, contactless cards, in which energy and data are transferred without any electrical contact between the card and the terminal, have become mature, inexpensive mass-produced products in the form of memory cards as well as processor cards. Although contactless processor cards are limited to operation at a distance of up to ten centimeters from the terminal due to their relatively high power consumption, contactless memory cards can be used up to a meter away from the terminal. This means that contactless memory cards do not necessarily have to be held in the user's hand in use, but can remain in the user's purse or wallet. Contactless cards are thus particularly suitable for applications in which people or items should be identified quickly. Sample applications include access control, local public transport, ski passes, airline tickets, and luggage identification.

However, there are also applications where operation over a long distance could cause problems and should be prevented. A typical example is an electronic purse. A declaration of intent on the part of the cardholder is normally required to complete a financial transaction. This confirms the amount of the payment and the cardholder's agreement to pay. With a contact card, this declaration takes the form of inserting the card in the terminal and confirming the indicated amount using the keypad. If contactless payments over relatively long distances were possible, a swindler could remove money from the electronic purse without the knowledge of the cardholder. Dual-interface cards offer a possible solution to this problem. These cards combine 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, according to what is desired.

There is considerable interest in using contactless cards for local public transport. If the functionality of smart cards used in payment systems, which are generally contact cards, is

expanded to enable them to act as electronic tickets with a contactless interface, transport system operators can utilize the infrastructure and cards of the credit card industry.

1.3 STANDARDIZATION

The prerequisite for the worldwide use of smart cards in everyday life, such as their present worldwide use in the form of SIM cards, health insurance cards, bank cards and passports, was the generation of national and international standards. Due to the special significance of such standards, in this book we repeatedly refer to currently applicable standards and those that are in preparation.

A smart card is normally part of a complex system. This means that the interfaces between the card and the rest of the system must be precisely specified and coordinated. Of course, this could be done for each system on a case-by-case basis, without regard to other systems. However, this would mean that a different type of smart card would be needed for each system. Users would thus have to carry a separate card for each application. In order to avoid this, an attempt has been made to generate application-independent standards that allow multifunctional cards to be developed. Since the smart card is usually the only component of the system that the user holds in his or her hand, it is enormously important for user awareness and acceptance of the entire system. However, from a technical and organizational perspective the smart card is usually only the tip of the iceberg, since complex systems (which are usually networked) are often hidden behind the card terminal, and it is these systems that make the customer benefits possible in the first place.

Let us take telephone cards as an example. In technical terms, they are fairly simple objects. By themselves, they are almost worthless, except perhaps as collector's items. Their true benefit, which is to allow public telephones to be used without coins, can be realized only after umpteen thousand card phones have been installed throughout a region and connected to a network. The large investments required for this can only be justified if the long-term viability of the system is ensured by appropriate standards and specifications. Standards are also an indispensable prerequisite for multifunctional smart cards that can be used for several different applications, such as phoning, an electronic purse, an electronic ticket, and so on.

What are standards?

This question is not as trivial as it may appear at first glance, especially because the terms 'standard' and 'specification' are often used interchangeably. A standard requires the consensus of all interested parties, while a specification has looser requirements with regard to consensus and open consultation. To make things clear, let us consider the ISO/IEC definition of a standard:

> A document that is produced by consensus and adopted by a recognized organization, and which, for general and recurring applications, defines rules, guidelines or features for activities or their results, with the objective of achieving an optimum degree of regulation in a given context.

Here it should be noted that standards are based on the established results of science, technology and experience, and their objective is to promote the optimization of benefits for society. International standards should thus help make life easier and increase the reliability and usefulness of products and services.

In order to avoid confusion, ISO/IEC have also defined the term 'consensus' as general agreement, characterized by the absence of continuing objections to essential elements on the part of any significant portion of the interested parties, and achieved by a procedure that attempts to consider the views of all relevant parties and to address all counter-arguments. Here it should be noted that consensus does not necessarily mean unanimity.

Although unanimity is not required for consensus, the democratic process naturally takes a lot of time in many cases, especially because it is necessary to consider not only the views of the technical specialists, but also the views of all involved and affected parties, since the objective of a standard is the promotion of optimum benefits 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 limited group of interested parties, such as commercial firms, generates its own specification ('industry standard') in order to accelerate the launch of a new system. This is particularly true in the field of information technology, which is characterized by especially fast development and correspondingly short innovation cycles. Although industry standards and specifications have the advantage that they can be developed significantly faster than 'true' standards, they carry the risk of ignoring the interests of the parties that are not involved in their development. For this reason, ISO uses the 'fast track' procedure to allow important, publicly accessible specifications to be quickly published as ISO standards after the fact.

What does ISO/IEC mean?

The relevant ISO/IEC standards are especially significant for smart cards because they are based on a broad international consensus and define the fundamental properties of smart cards. What lies behind the abbreviations 'ISO' and 'IEC'? 'ISO' stands for the International Organization for Standardization, while 'IEC' stands for the International Electrotechnical Commission.

The International Organization for Standardization (ISO) is a worldwide association of around 100 national standards organizations, with one per country. ISO was founded in 1947 and is a nonnational 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 activities of ISO are agreements that are published as ISO standards.

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

As already noted, 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. Germany is represented in ISO by the DIN organization. The member organizations have four basic tasks, as follows:

- Informing potentially interested parties in their own countries about relevant activities and opportunities for international standardization,
- Fashioning agreed national opinions and representing these opinions in international negotiations,
- Providing secretarial services for the ISO committees in which the country has a particular interest,

- Paying the country's financial contribution to support the activities of the central ISO organization.

The IEC (International Electrotechnical Commission) is an international standardization organization whose scope of responsibility is electrical technology and electronics. The first card standards, which did not include parts on the subject of electronics, were issued by ISO. After the introduction of smart cards, a difference of focus arose between the ISO and the IEC. In order to avoid duplication of effort, standards are developed in a joint technical committee (JTC 1, Joint Technical Committee for Information Technology) and published as ISO/IEC standards.

How is an ISO standard generated?

The need for a standard is reported to a national standards organization by a special interest group, such as an association or a industrial sector committee. The national organization then proposes this to ISO as a new working topic. If the proposal is accepted by the responsible working group, which consists of technical experts from countries that are interested in the topic, the first thing that is done is to define the application area of the future standard.

After agreement has been reached on the technologies and applications to be defined in the standard, the details of the standard are discussed and negotiated between the various countries. This is the second phase in the development of a 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' (DIS).

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

To prevent standards from becoming outdated as the result of ongoing development, 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 CEN

As already mentioned, ISO is not the only international standardization organization. In order to avoid duplication of effort, ISO cooperates closely with the IEC in certain areas. The areas of responsibility are defined as follows: the IEC is responsible for electrical technology and electronics, while ISO is responsible for all other areas. Combined working groups are formed to deal with topics of common interest, and these groups produce combined ISO/IEC standards. Most standards for smart cards belong to this category.

ISO and the Comité Européen de Normalisation (CEN) (European Standardization Committee) have also agreed on rules for the development of standards that are recognized as both European and international standards. This leads to time and cost savings.

The major industrial countries are represented in all relevant committees, and they generally also maintain 'mirror' committees in the form of national working groups and voting committees. The ISO website [ISO] provides an overview of the structure of ISO and its standardization projects. Smart card standards are developed by JTC 1/SC17 ('Cards and Personal Identification'). This working group also provides an overview of recently published standards and standards in progress.

At CEN, the topic of smart cards is handled by the TC 224 committee ('Personal identification, electronic signature and cards, and their related systems and operations').

The activities of CEN complement those of ISO. As much as possible, ISO standards are taken as the basis for CEN standards. If necessary, they are augmented with specifically European sections. In many cases, the number of options is reduced to simplify their implementation for purely European applications. The CEN working groups also produce standards for specific European applications that would not be able to achieve a consensus with ISO in a given form or at a given time.

An additional European standardization body, the European Telecommunications Standards Institute (ETSI), has made a significant contribution to the widespread international use of smart cards with its standard for SIM cards. ETSI generates standards for information and telecommunication technologies, which include mobile telecommunication and Internet technology.

ETSI is recognized by the European Commission as a European standardization organization. The members of ETSI are not the national standardization committees, but instead nearly 700 member organizations worldwide, which essentially represent the industrial sector, telecommunication companies, user groups, and research organizations. The smart card standards are prepared by the Technical Committee for Smart Card Platform (TC SCP). The TS 51.011 family of standards (formerly GS 51.011) specifies the interface between the smart card (called the subscriber identity module, SIM, in the GSM system) and the mobile telephone. This family of standards is based on the ISO/IEC standards. With the international expansion of GSM systems outside Europe, the ETSI standards have achieved global significance for the smart card industry.

After more than thirty years of standardization effort, the most important basic ISO standards for smart cards are now complete. They form the basis for further, application-oriented standards, which are currently being prepared by ISO and CEN.

These standards are based on prior ISO standards in the 7810, 7811, 7812 and 7813 families, which define the properties of identification cards in the ID-1 format. These standards include embossed cards and cards with magnetic stripes, which we all know in the form of credit cards.

Compatibility with these existing standards was a criterion from the very beginning in the development of standards for smart cards (which are called 'integrated circuit(s) cards', ICC, in the ISO standards), in order to provide a smooth transition from embossed cards and magnetic-stripe cards to smart cards. Such a transition is possible because all functional components, such as embossing, magnetic stripes, contacts and interface components for contactless interfaces, can be integrated into a single card. Of course, a consequence of this is that the integrated circuits, which are sensitive electronic components, are exposed to high stresses during the embossing process and recurrent impact stresses when the embossed characters are printed onto paper. This makes heavy demands on the packaging of the integrated circuits and the manner in which they are embedded in the card.

A summary of the currently available standards, with brief descriptions of their contents, can be found in the Appendix.[1]

In the last few years, an increasing number of specifications have been prepared and published by industrial organizations and other nonpublic groups, with no attempt being made to incorporate them in the standardization activities of ISO. The reason most often given for this approach is that the way ISO operates is too slow to keep pace with the short innovation cycles of the information technology and telecommunication industries. Some examples of consortiums that generate specifications relevant to smart cards are Java Card Forum, Open

[1] See also Section 25.4, 'Directory of Standards and Specifications', on page 999

Mobile Alliance (OMA), Global Platform, and NFC Forum. In many cases, only a few interest groups are involved in drafting these industry standards, so there is a risk that the interests of smaller companies, and especially the interests of the general public, may be ignored in the process. Fortunately, the most important consortiums work closely together with standardization organizations and try to include the most important specifications in the standardization process later on. It is a major challenge to the future of ISO and IEC to devise processes that make it possible to safeguard general interests without hampering the pace of innovation.

2
Card Types

Smart cards are the youngest member of the family of identification cards using the ID-1 format defined in ISO/IEC standard 7810, 'Identification Cards – Physical Characteristics'. This standard specifies the physical properties of identification cards, including their material properties such as flexibility and temperature resistance, as well as the dimensions of three different card formats: ID-1, ID-2, and ID-3. The ISO 7816-1 family of smart card standards is based the ID-1 card format, which is commonly used for the payment cards used by millions of people.

This chapter provides an overview of a variety of cards in ID-1 format because many applications have a special interest in combining several functions, especially when the cards used in an existing system (such as magnetic-stripe cards) are intended to be replaced by smart cards. In such cases, it is usually not possible to replace the existing infrastructure (such as magnetic-stripe card terminals) by a new technology overnight.

The solution to this problem usually consists of issuing cards with magnetic stripes as well as chips for use during a transition period. Such cards can be used with both types of terminals (old and new). Naturally, new functions that are only possible with a chip cannot be used with a terminal that only supports magnetic-stripe cards.

Similar considerations apply to the transition from contact smart cards to contactless smart cards. In many cases, the infrastructure must be able to support both types of cards during an extended transition period. Form factors other than ID-1 have now become established in some applications where compatibility with magnetic-stripe cards is not necessary. SIM cards in ID-000 format are one example. Naturally, the information regarding electrical properties and functions also applies to these other form factors.

2.1 EMBOSSED CARDS

Embossing is the oldest technique for adding machine-readable features to identification cards. The embossed characters on the card can be transferred to paper using simple, inexpensive devices, and they can easily be read visually (by humans). The nature and location of the embossing are specified in the ISO/IEC 7811 standard ('Identification Cards - Recording Techniques'). This standard, which is divided into five parts, deals with magnetic stripes as well as embossing.

Smart Card Handbook: Fourth Edition Wolfgang Rankl and Wolfgang Effing

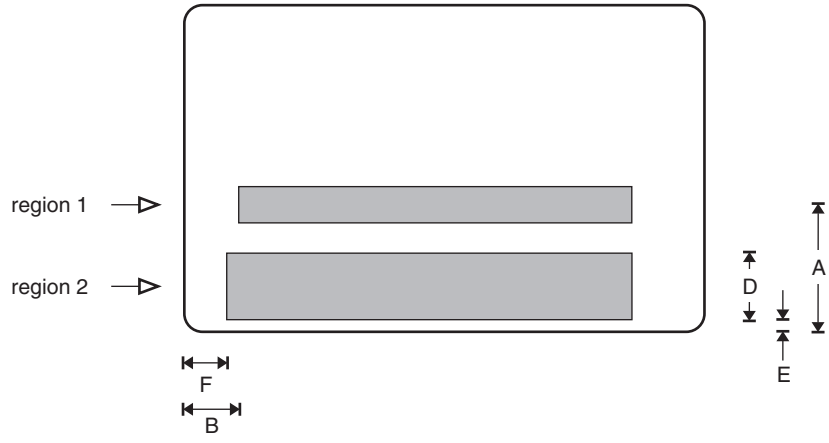

Figure 2.1 Embossing regions according to ISO 7811. Region 1 is intended for the identification number (19 characters), while region 2 is intended for the name and address (4 lines of 27 characters each). The following dimensions are specified in the standard: A: 21.42 ± 0.12 mm; B: 10.18 ± 0.25 mm; D: 14.53 mm; E: 2.41–3.30 mm; F: 7.65 mm ± 0.25 mm

Two different embossing regions are defined, as shown in Figure 2.1. Region 1 is reserved for the card identification number, which identifies the card issuer as well as cardholder. Region 2 is reserved for additional cardholder data, such as the cardholder's name and address.

At first glance, transferring information by printing from embossed characters may appear quite primitive. However, the simplicity of this technique has made worldwide use of credit cards possible, even in developing countries. Utilization of this technology requires neither electrical power nor a connection to a telephone network.

2.2 MAGNETIC-STRIPE CARDS

The essential disadvantage of embossed cards is that their use creates a flood of paper receipts, which are expensive to handle and process. One remedy to this problem is to digitally encode the card data on a magnetic stripe located on the back of the card.

The magnetic stripe is read by pulling it across a read head, either manually or automatically. After this, the read data can be used in the system without any human intervention. One of the properties of magnetic stripes is the strength of the magnetic field (measured in oersteds) necessary to modify the data on the magnetic stripe. With low-coercivity (*loco*) magnetic stripes, the required magnetic field strength is 300 to 650 oersted, while with high-coercivity (*hico*) magnetic stripes the required magnetic field strength is 1250 to 4000 oersted. High-coercivity magnetic stripes have the advantage that they cannot be erased accidentally, such as by a nearby magnet, but they require special write heads.

Parts 2, 6, 7 and 8 of ISO/IEC standard 7811 specify the properties of the magnetic stripe, the coding method, and the locations of the magnetic tracks. The magnetic stripe may have up to three tracks. as illustrated in Figure 2.2 on the next page. Tracks 1 and 2 are specified to be read-only tracks, while track 3 may also be written to. The specified contents of the data tracks are listed in Table 2.1 on page 18, while typical contents and their positions are listed in Table 2.2 on page 18.

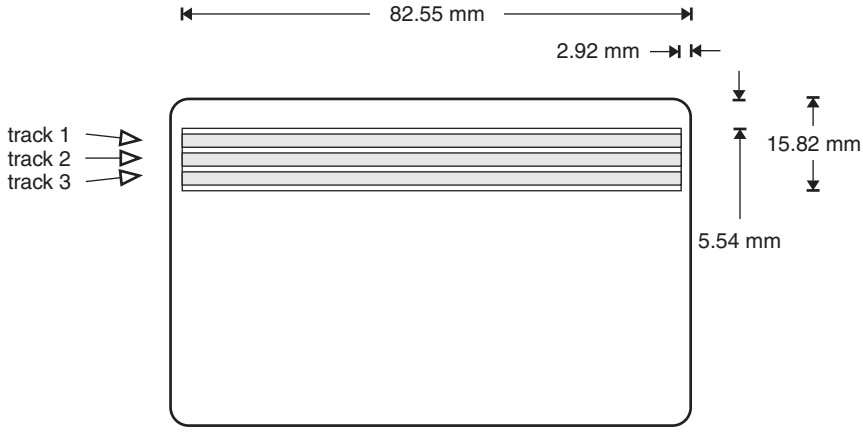

Figure 2.2 Magnetic stripe location on an ID-1 card. The data region of the magnetic stripe is intentionally not extended to the edges of the card, since the use of hand-operated card readers causes rapid wear at the ends of the stripe

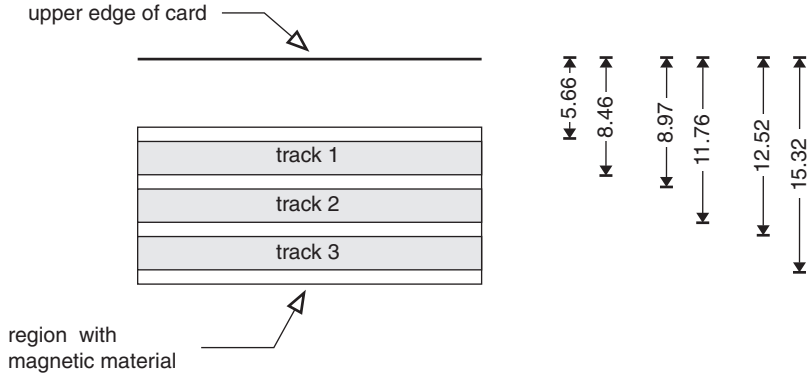

Figure 2.3 Locations of the data tracks on an ID-1 card (all dimensions in mm)

Although the storage capacity of the magnetic stripe is fairly small (around 1000 bits), it is more than sufficient for storing the information contained in the embossing. Additional data can be read and written on track 3, such as the most recent transaction data in the case of a credit card. The track locations are shown in Figure 2.3.

The main drawback of magnetic-stripe technology is that the stored data can be altered very easily. Manipulating embossed characters requires at least a certain amount of manual dexterity, and such manipulations can readily be detected by a trained eye. By contrast, the data recorded on the magnetic stripe can easily be altered using a standard read/write device, and it is difficult to prove such changes afterward. In addition, magnetic-stripe cards are often used in automated equipment such as cash dispensers, in which visual inspection is not possible. A potential criminal, having obtained valid card data, can easily use duplicated cards in such unattended machines without having to forge the visual security features of the cards.

Table 2.1 The data tracks of a magnetic-stripe card as specified in ISO/IEC 7811

Property	Track 1	Track 2	Track 3
Data volume	79 characters max.	40 characters max.	107 characters max.
Data coding	6-bit alphanumeric	4-bit BCD	4-bit BCD
Data density	210 bit/inch (8.3 bit/mm)	75 bit/inch (3 bit/mm)	210 bit/inch (8.3 bit/mm)
Writing	not allowed	not allowed	allowed

Table 2.2 Example magnetic stripe data content and coding of a typical credit card

Track	Position	Data
1	2–17	credit card number
1	19–44	surname of the cardholder
1	46–47	expiry year
1	48–49	expiry month
2	1–16	credit card number
2	18–19	expiry year
2	20–21	expiry month

Manufacturers of magnetic-stripe cards have developed various techniques to protect the data recorded on the magnetic stripe against forgery and duplication. For example, German Eurocheque cards contain an invisible, unalterable code in the body of the card, which effectively makes it impossible to alter or duplicate the data on the magnetic stripe.[1] However, such techniques require a special sensor in the card terminal, which considerably increases the cost of the terminal. For this reason, none of these techniques has so far become established internationally.

2.3 SMART CARDS

Smart cards are the latest innovation in the family of identification cards in ID-1 format. Their characteristic feature is an integrated circuit embedded in the card body, which has components for transmitting, storing and processing data. The data can be transmitted by contacts on the surface of the card or by an electromagnetic field without using contacts.

Smart cards offer several advantages compared with magnetic-stripe cards. For example, the maximum storage capacity of a smart card is many times greater than that of a magnetic-stripe card. Chips with memory capacities in the megabyte range are now available, and the maximum capacity increases with each new chip generation. Only optical memory cards, which are described in the next section, and smart cards with supplementary NAND flash memory have greater capacity.

[1] See also Section 3.5.13, ‘Moduliertes Merkmal’, on page 48

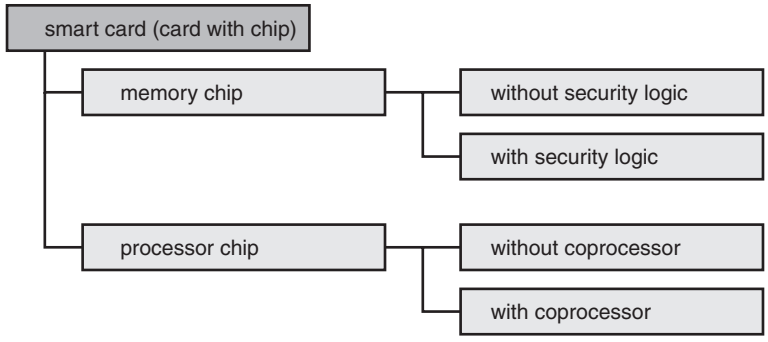

Figure 2.4 Classification of smart cards by chip type

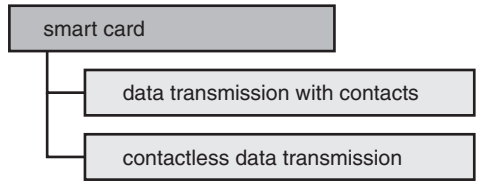

Figure 2.5 Classification of smart cards by data transmission method

However, one of the most important advantages of smart cards is that their stored data can be protected against unauthorized access and manipulation. The data can only be accessed via a serial interface that is controlled by the operating system or security logic, which means that confidential data can be stored in the card in a manner that prevents it from ever being read from outside the card. Such confidential data can be processed only internally by the chip's processing unit. In principle, hardware and software mechanisms can both be used to restrict use of the memory functions (reading, writing, and erasing data) and subject them to specific conditions. This makes it possible to construct a variety of security mechanisms, which can also be tailored to the specific requirements of a particular application.

In combination with the ability to compute cryptographic algorithms, this allows smart cards to be used to implement convenient security modules that can be carried by users at all times, for example in a purse or wallet. Some additional advantages of smart cards are their high reliability and long life compared with magnetic-stripe cards, whose useful life is generally limited to two to three years.

The fundamental properties and functions of smart cards are specified in the ISO/IEC 7816 family of standards, which are described in detail in subsequent chapters. Smart cards can be divided into two groups that differ in both functionality and price: memory cards and processor cards (see Figure 2.4).

Smart cards can also be classified on the basis of their data transmission method (see Figure 2.5). Data can be transmitted using mechanical contacts or wirelessly using electromagnetic coupling. Memory cards and processor cards are both available in contact and contactless forms.

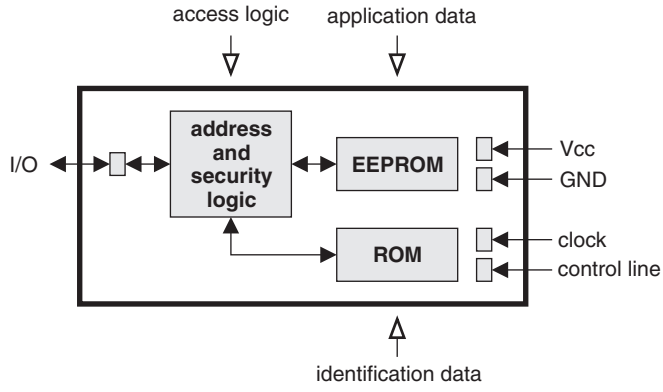

Figure 2.6 Typical architecture of a contact memory card with security logic. The figure shows only basic energy and data flows and is not a detailed schematic diagram

2.3.1 Memory cards

Figure 2.6 shows the architecture of a memory card in block diagram form. The data needed by the application is stored in nonvolatile memory, which is usually EEPROM. Access to the memory is controlled by the security logic, which in the simplest case consists only of write protection or erase protection for the memory or certain memory regions. However, there are also memory chips with more complex security logic that can also perform simple encryption. Data is transferred to and from the card via a serial interface. Part 3 of the ISO/IEC 7816 standard defines a special synchronous transmission protocol that enables an especially simple and inexpensive implementation in the chip. However, some smart cards employ the I^2C bus, which is widely used for serial-access memories.

The functionality of memory cards is usually optimized for a particular application. Although this severely restricts the flexibility of these cards, it makes them quite inexpensive. Typical applications for memory cards are prepaid telephone cards and simple health insurance cards.

2.3.2 Contactless memory cards

Contactless memory cards have come into widespread use in recent years. Standard cards compliant with ISO/IEC 14443 have an operating range of up to 10 cm. The usable memory capacity ranges from several hundred bytes to a few kilobytes. The memory can be partitioned into several sectors that are independently protected against unauthorized reading, writing, and erasing. This enables a single card to support several different applications. Each card has a unique serial number stored in ROM, as well as authentication logic using a challenge–response method. A typical architecture for contactless memory cards is shown in Figure 2.7 on the next page.

Typical applications for contactless memory cards are contactless ticketing in local transport systems and identification cards for companies, official bodies, or universities. Electronic purse functionality, such as for a company cafeteria or university cafeteria, can also be implemented on such cards. Contactless technology compliant with ISO/IEC 14443 is also used extensively now in radio-frequency identification (RFID) tags.

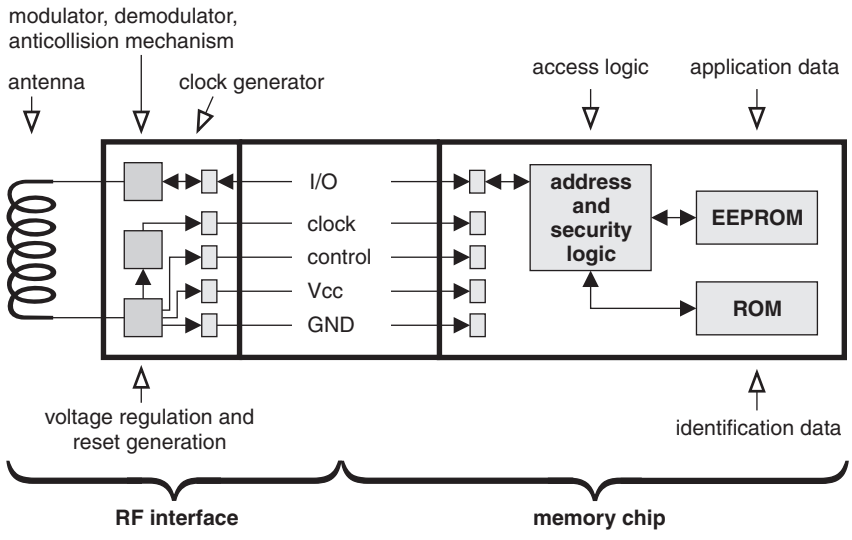

Figure 2.7 Typical architecture of a memory card with security logic and a contactless interface. The figure shows only basic energy and data flows and is not a detailed schematic diagram

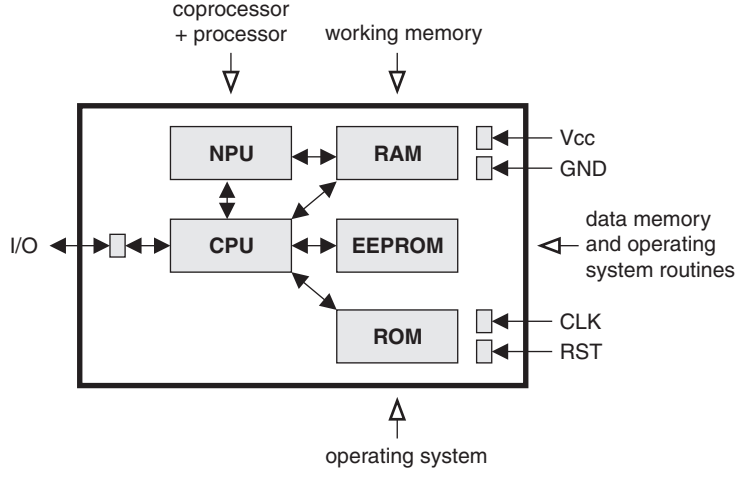

Figure 2.8 Typical architecture of a contact processor card with a coprocessor and mask-programmed ROM. The figure shows only basic energy and data flows and is not a detailed schematic diagram

2.3.3 Processor cards

The principal component of a processor card, which is formally known as a microprocessor card, is the processor (CPU), which us usually surrounded by four other functional blocks: mask ROM, EEPROM, RAM, and an I/O port. Figure 2.8 shows the typical architecture of this type of device.

The mask ROM contains the chip's operating system, which is permanently stored in memory when the chip is manufactured. The content of the ROM is thus identical for all chips

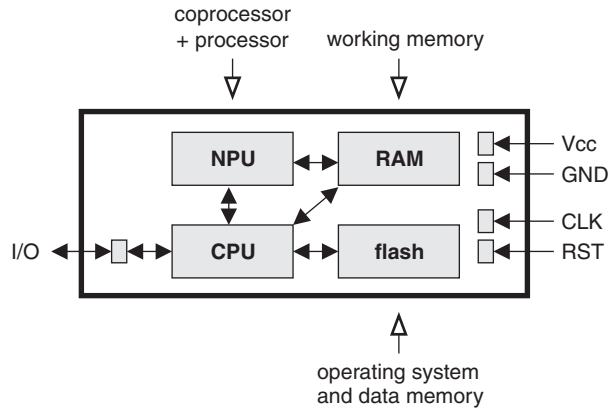

Figure 2.9 Typical architecture of a contact processor card with a coprocessor and flash memory. The figure shows only basic energy and data flows and is not a detailed schematic diagram

of a production batch, and it cannot be changed during the chip's lifetime. The EEPROM is the chip's nonvolatile memory. Data and program code can be written to and read from the EEPROM under control of the operating system. The RAM is the processor's working memory. This memory is volatile, so all data stored in it is lost when the chip is de-energized. In its simplest form, the serial I/O interface consists only of a single register used to transfer data bit by bit.

Processor cards are very versatile in use. In the simplest case, they contain a program optimized for a single application, which means that they can only be used for this particular application.

However, modern smart card operating systems allow several different applications to be integrated in a single card. In this case, the ROM contains only the basic components of the operating system, with the application-specific components being loaded into the EEPROM only after the card has been manufactured. Recent developments also allow application programs to be loaded into a card after it has already been personalized and issued to the cardholder. Special hardware and software measures are used ensure that the different security conditions of the individual applications are not violated. Semiconductor manufacturers can supply microprocessor chips with high processing power, large memory capacity and sophisticated security logic that are specially optimized for this purpose.

In a trend that parallels that of technological progress in other areas, such as digital cameras and MP3 players, mask-programmed ROM and EEPROM are increasingly being supplanted by flash (short for flash EEPROM) in newer types of processor cards. Flash memory has the advantage of distinctly greater flexibility in production and personalization compared with ROM, which cannot be modified after manufacturing. Flash memory enables capabilities such as adapting the operating system to the wishes of the customer and loading it into the cards after manufacturing. Figure 2.9 shows the architecture of a contact processor card with flash memory.

The dramatic increase in the memory capacity of processor cards in recent years, which shows no signs of ending, has increasingly highlighted the limitations imposed on the data transmission rate by the serial interface. Consequently, new interfaces and transmission protocols have been developed to accommodate the new requirements. For instance, ETSI standardized the USB interface for SIM cards in 2007. Another new interface is the Single

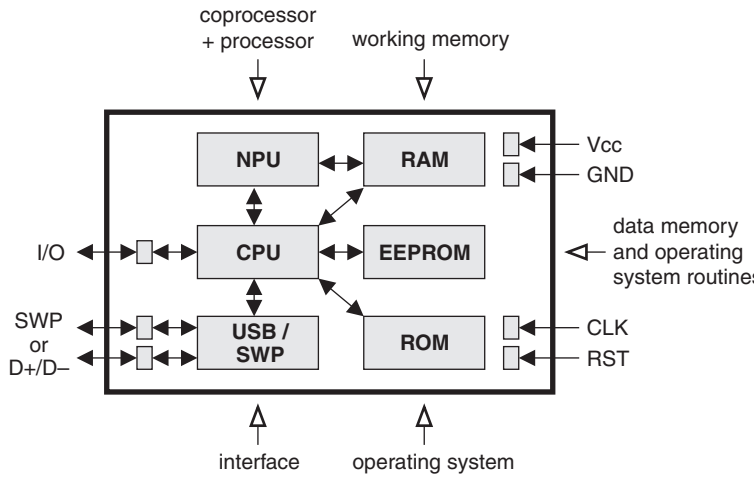

Figure 2.10 Typical architecture of a contact processor card with a coprocessor, T = 0/ T = 1 interface, USB interface, and SWP interface. The figure shows only basic energy and data flows and is not a detailed schematic diagram

Wire Protocol (SWP), which links the SIM card to an NFC controller in a mobile telephone. In the future, more and more processor cards will support several I/O interfaces in parallel, as illustrated in Figure 2.10.

2.3.4 Contactless processor cards

Contactless smart card technology enables a variety of interesting new applications for card issuers and card users. For instance, contactless cards do not have to be inserted into a card reader, but instead only have to be held close to a reader, since contactless processor cards have a working range of up to 10 cm. This is a great advantage in applications such as access control systems that control whether a door opens or a turnstile turns. A major application area for this is local public transport, which requires reliable recognition of a large number of people in the shortest possible time.

A further interesting variation on using contactless cards involves utilizing the surface of the reader. With this option, the card is not inserted into a slot, but instead simply held against a marked area on the surface of the card reader. In addition to ease of use, this solution is attractive because it significantly reduces the risk of vandalism, such as pressing chewing gum or superglue into the card slot.

For card marketing, contactless technology offers the advantage that no technical components are visible on the surface of the card, so the graphic design of the card is not constrained by magnetic stripes or contacts. However, this advantage comes at the price of more complex terminals with correspondingly higher prices.

Contactless card technology has now matured to the point that high-quality products are available at prices that are not significantly higher than those of comparable contact cards. Up to now, contactless cards have been used primarily in local public transport systems, in which they serve as electronic tickets that enable modern electronic fare management.

Although most currently operating systems still use single-function cards, which typically contain inexpensive memory chips with hard-wired security logic, there is an increasing

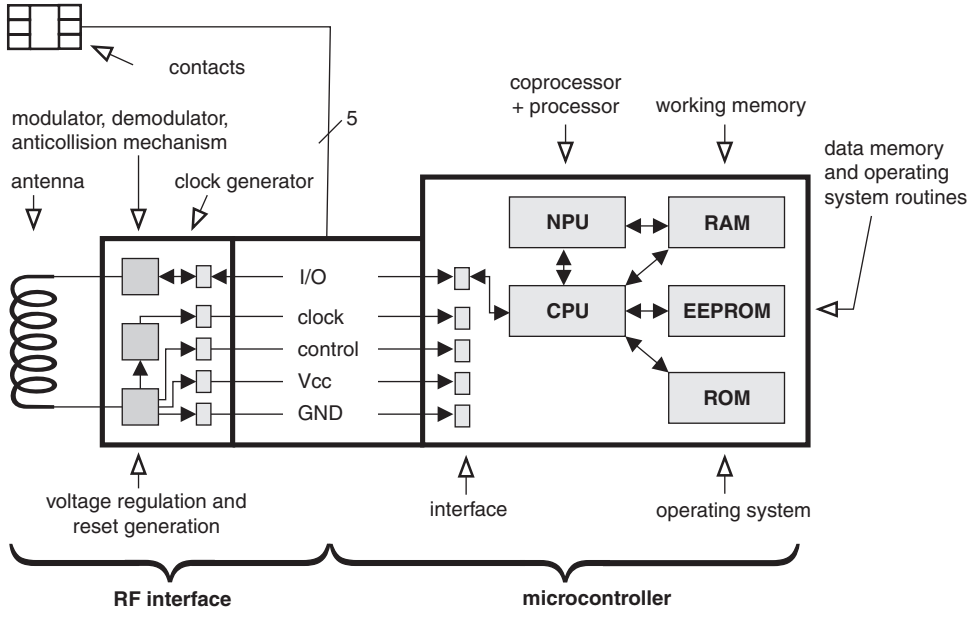

Figure 2.11 Typical architecture of a processor card with a coprocessor, a contactless interface, and a contact interface. The latter interface is not present in a purely contactless processor card. The figure shows only basic energy and data flows and is not a detailed schematic diagram

demand for adding value-added services to electronic tickets or incorporating electronic ticket functionality in payment cards. Consequently, multifunction cards with integrated processors are being used more and more often, with the payment function usually implemented with conventional contact technology in order to utilize the existing payment card infrastructure. These cards have contacts as well as contactless coupling elements and are called dual-interface cards, as illustrated in Figure 2.11. The technology and operating principles of contactless smart cards are described in detail in Chapter 10, 'Contactless Data Transmission', on page 283.

2.3.5 Multi-megabyte cards

The growing popularity of flash memory as a replacement for hard disk drives in the PC realm is reflected in the smart card realm. It has become technically possible to produce processor cards with a memory capacity ranging from a few megabytes to somewhere in the gigabyte range. The standard T = 0 and T = 1 protocols specified in ISO/IEC 7816 are far too limited to cope with such large memory sizes. Consequently, such cards also have a USB or MMC interface.

In their simplest form, these cards are implemented as three-chip solutions. This does not require the development of new integrated circuits; instead, three standard ICs are wired together on a printed circuit board. The disadvantage of this approach is that three individual chips are more expensive in mass production than a design integrated in a single chip. In addition, the interconnections between the chips provide an additional target for attacks. For these reasons, two-chip and single-chip solutions can be expected increasingly often in the future, as shown in Figure 2.12 on the facing page.

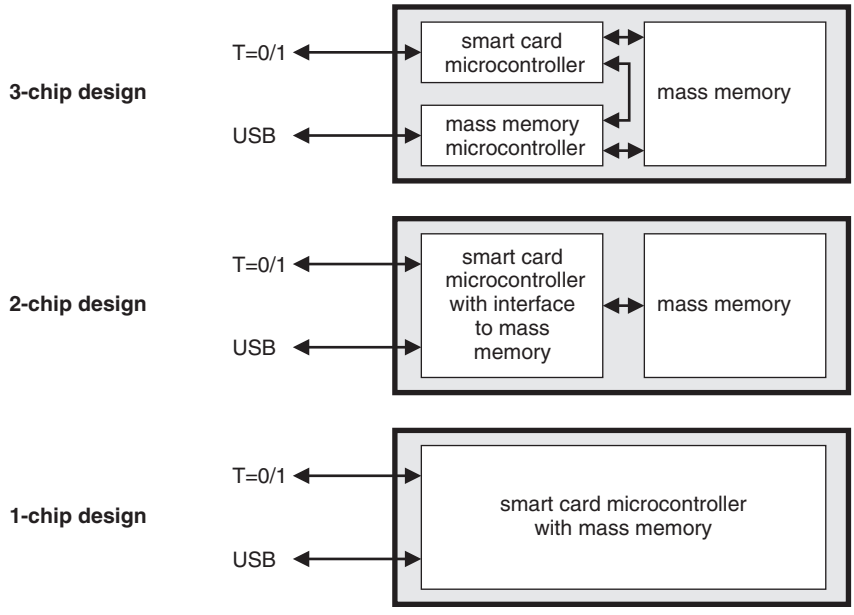

Figure 2.12 Three options for connecting NAND flash mass memory to a smart card microcontroller with a T = 0 /T = 1 interface and a USB interface

2.3.6 Security tokens

A security token is a hardware component containing a security chip, such as a smart card microcontroller, and it is usually connected to a USB port. A typical security token architecture is shown in Figure 2.13 on the next page. A USB security token thus combines the advantages of a smart card with the connection convenience of the USB interface, without any need for a card reader. Currently available USB security tokens usually contain several integrated circuits, such as a security chip and a memory chip. As the USB interface is specified as a new I/O interface for high data transmission rates in the latest smart card standards, there are already some smart card security microcontrollers available with an integrated USB interface. This enables economical, high-security single-chip solutions for security tokens. They differ from smart cards with the same functionality only in their physical form, as can be seen in Figure 3.47 on page 59.

There are also security tokens with no direct connection to a PC. In addition to the security microcontroller, these security tokens usually have a keypad for PIN entry and a display to show a pseudorandom number used for authentication between the token and a server (one-time password). These one-time password tokens are also available in the form of small hardware components or smart cards with integrated displays.

2.4 OPTICAL MEMORY CARDS

Optical memory cards utilize optical memory technology, such as is used on CDs. Data on optical memory cards is protected against read errors by conventional methods, such as

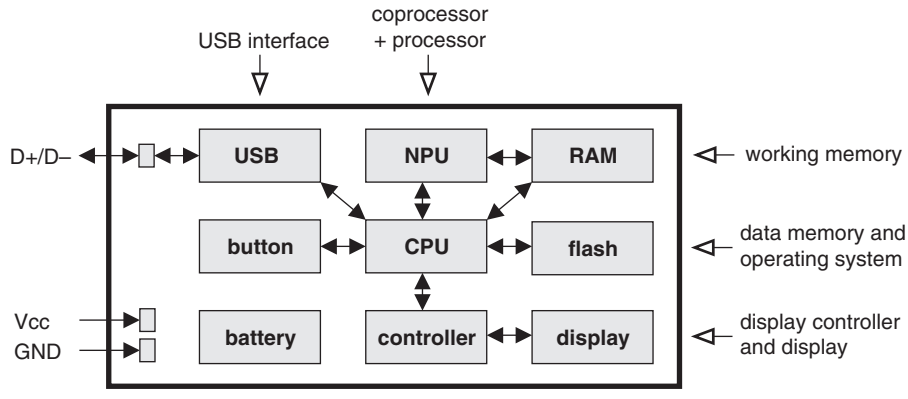

Figure 2.13 Typical architecture of a token with a coprocessor, display and USB interface, used for purposes such as generating one-time passwords. The figure shows only basic energy and data flows and is not a detailed schematic diagram

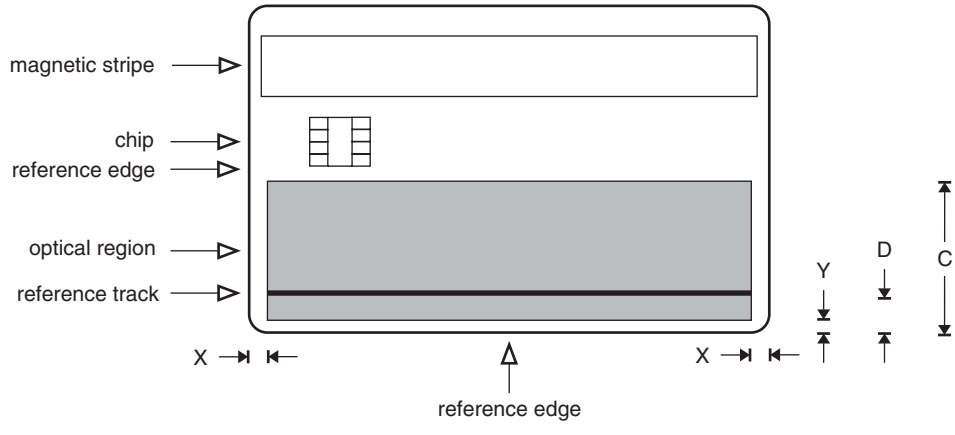

Figure 2.14 Location of the optical storage area on an ID-1 card according to ISO/IEC 11694-2. The following dimensions are specified in the standard: C: 9.5–49.2 mm; D: 5.8 ± 0.7 mm; X: 3 mm max. with MMI or 1 mm max. with PPM; Y: Y < D and ≥ 1 mm with PWM or 4.5 mm max. with PWI (PWM = pulse width modulation; PPM = pulse position modulation)

checksums, which of course reduces their useful memory capacity. The ISO/IEC 11693 and ISO/IEC 11694 standards define the physical characteristics of optical memory cards and the linear data recording technology.

Combining the large storage capacity of optical memory cards with the intelligence of smart cards opens up interesting new possibilities. For example, data can be written to the optical memory in encrypted form, with the key stored securely in the private memory of the chip. This protects the optically stored data against unauthorized access. Figure 2.14 shows the layout of a typical optical smart card with contacts, a magnetic stripe, and an optical data storage area. As you can see, the area available for optical storage is reduced by the chip

Figure 2.15 A typical optical memory card with a net storage capacity (including error correction) of approximately 4 MB. The raw storage capacity (without error correction) is approximately 6 MB

contacts, which naturally restricts the total storage capacity. The magnetic stripe is located on the back the card. An actual optical memory card is shown in Figure 2.15.

The prices of optical memory cards are comparable to those of smart cards. However, reading and writing devices for optical memory cards are much more expensive than comparable devices for smart cards, which has severely restricted their use up to now. Optical memory cards are used in areas such as health care for storing patient data, where their large memory capacity allows even X-ray images to be stored on the card. The previously described multimegabyte cards now provide memory capacity that is comparable to or even greater than that of optical memory cards. Whether optical memory cards will nevertheless manage to establish a position in the market remains to be seen.

3
Physical Properties

The card body of a smart card inherits its fundamental properties from its predecessor, the familiar embossed card, which still dominates the market in the credit card sector. Technically speaking, such cards are simple plastic structures that are personalized by being embossed with a variety of user features, such as the name and customer number of the cardholder.

Later versions of these cards were provided with a magnetic stripe to enable simple machine processing. When the idea of adding chips to cards first arose, this existing type of card was used as the basis and a module with a memory chip or processor chip was embedded in the body of the card. Many standards relating to the card's physical properties are thus not specific to smart cards, but apply equally well to magnetic-stripe and embossed cards.

If you hold a smart card in your hand, the first thing you notice is its format. After this, you might see that it has set of contacts, although a contactless smart card may not have any visible electrical interface. The next feature to catch your eye might be a magnetic stripe, embossing or a hologram. All of these features and functional components are part of the physical properties of a smart card.

Most of the physical properties are actually purely mechanical in nature, such as the format of the card and its resistance to bending or twisting. These properties are familiar to every user from personal experience. In practice, however, physical properties such as sensitivity to temperature or light and resistance to moisture are also important.

The interaction between the body of the card and the implanted chip must always be considered, since only the combination of the two components makes a functional card. For instance, a card body designed for use at high ambient temperatures is of little benefit if its embedded microcontroller does not share this property. These two components must individually and collectively meet all of the relevant requirements, since otherwise high failure rates can be expected in use.

3.1 CARD FORMATS

Small cards with the typical smart card dimensions of 85.6 by 54 mm have been in use for a very long time. Almost all smart cards are still produced in this format, which is also the most

Smart Card Handbook: Fourth Edition Wolfgang Rankl and Wolfgang Effing

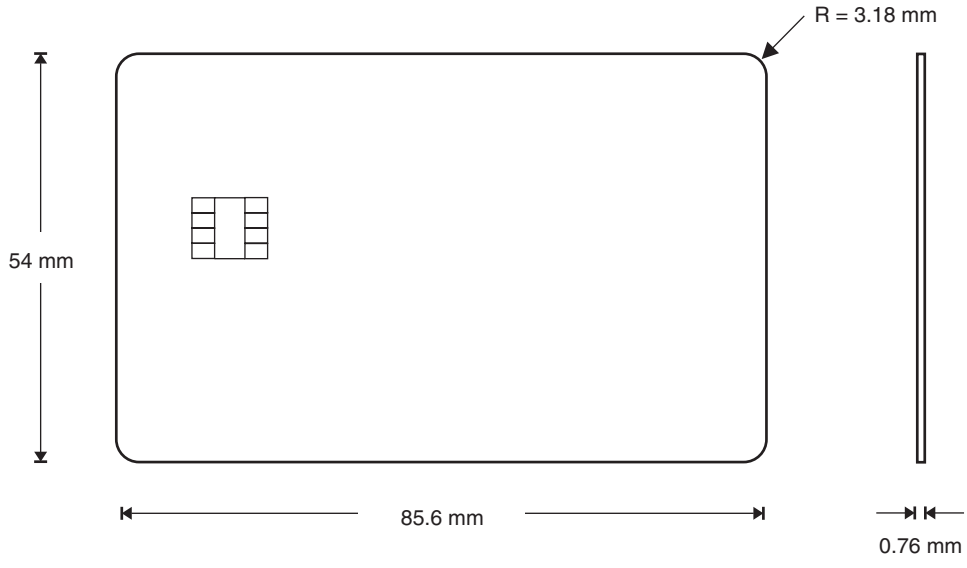

Figure 3.1 The ID-1 format as specified in ISO 7810. Thickness: 0.76 ± 0.08 mm; corner radius: 3.18 ± 0.30 mm. The indicated dimensions show the size of the card excluding tolerances

familiar.[1] It is designated ID-1, and its size is specified in the ISO 7810 standard (see Figure 3.1). An example of an ID-1 card is show in Figure 3.8 on page 34.

The ID-s standard originated in 1985 and thus has nothing to do with smart cards as we know them today, as can easily be seen from the abbreviation 'ID', which stands for 'identification'. This standard simply describes an embossed plastic card with a magnetic stripe that is intended to be used for the identification of a person. When it was written, no one had thought of putting a chip in the card. The presence of a chip and location of its contacts on the card were only defined several years later in other standards.

With the diversity of cards available today, which are used for all possible purposes and have a wide range of dimensions, it is often difficult to determine whether a particular card is actually an ID-1 smart card. In addition to the embedded chip, one of the best identifying features is the thickness of the card. If this measures 0.76 mm and the card has an embedded microcontroller, it can be regarded as a smart card in the sense of the ISO standard.

The conventional ID-1 format has the advantage of being very easy to handle. The card's format is specified such that it is not too large to be carried in a wallet, but not so small that it is easily lost. In addition, the card's flexibility makes it more convenient than a rigid object.

Nevertheless, this format does not always meet the demands of modern miniaturization. Mobile telephones typically weigh less than 200 g and are only half the size of a packet of tissues. It thus became necessary to define a smaller format in addition to the ID-1 format, in order to address the needs of small terminal devices.

This led to the development of additional card formats, all of which can be produced by stamping them from ID-1 cards or breaking them free from an ID-1 card. The cards used in

[1] Telecommunication cards are also produced in ID-000 format now. See also Section 14.4.4, 'Direct plug-in production', on page 588

Figure 3.2 A smart card in plug-in format, from which the user can break out a card in mini-UICC format

mobile telephones can be very small because they are usually plugged into the device only once and remain there forever. The ID-000 format was defined to suit this purpose, and it bears the descriptive name 'plug-in'. This format is only used in mobile telephones and as a security module in terminals.

However, cards in ID-000 format are inconvenient to handle in production and by end users, which led to the development of an additional format. This format is designated ID-00 or 'mini-card'. Its dimensions are approximately halfway between those of ID-1 and ID-000 cards. This type of card is more convenient to handle and less expensive to produce because it can be stamped from the ID-1 format. The ID-00 format was defined in the mid-1990s, but it has not yet become established either nationally or internationally.

Starting around 2003, ongoing miniaturization of mobile telephones led to the demand for a card format even smaller than the plug-in format. This was discussed for a long time under the working name 'Third Form Factor' (3FF), a term that is still often used for this new card size. The official ETSI name is 'mini-UICC', which designates a smart card format that is only slightly larger than a module with eight contacts. Mini-UICC cards can also be obtained by breaking them free from a larger ID-1 or plug-in card, as illustrated in Figure 3.2. They are already being produced in quantity for various network operators.

Developments in the payment card sector have paralleled the constant miniaturization of mobile telecommunication cards. Visa specified the Visa Mini card format in 2005. Cards in this format can also be produced by breaking them free from cards in standard ID-1 format, as illustrated in Figure 3.9 on page 35. This makes it possible to manufacture cards in the new format without modifying existing production lines for ID-1 cards. MasterCard has also defined a format with a similar size, which is called 'mc2'. Figure 3.12 on page 36 shows the two card formats in comparison.

The formats are defined in the relevant standards in a way that simplifies measuring the card dimensions, as illustrated in Figures 3.4 and 3.5 on the following page and Figure 3.9 on page 35. For example, the height and width of an ID-1 card must be such that it fits between two concentric rectangles (ignoring the rounded corners). The outer rectangle has a width of 85.72 mm (3.375 inch) and a height of 54.03 mm (2.127 inch). The inner rectangle has a width of 85.46 mm (3.365 inch) and a height of 53.92 mm (2.123 inch). The thickness must be 0.76 mm (0.03 inch), with a tolerance of $\pm$0.08 mm ($\pm$0.003 inch). The corner radii and card body thickness are dimensioned conventionally. Based on these definitions, the dimensions of an ID-1 card can be represented as shown in Figure 3.3 on the following page.

The ID-000 format as specified in TS 51.011 and TS 102 221 is also defined using two concentric rectangles. As this format originated in Europe (based on the GSM mobile telephone system), the basic dimensions are metric. The dimensions of the outer rectangle are 25.10 mm (width) by 15.10 mm (height). The inner rectangle has a width of 24.90 mm and a height

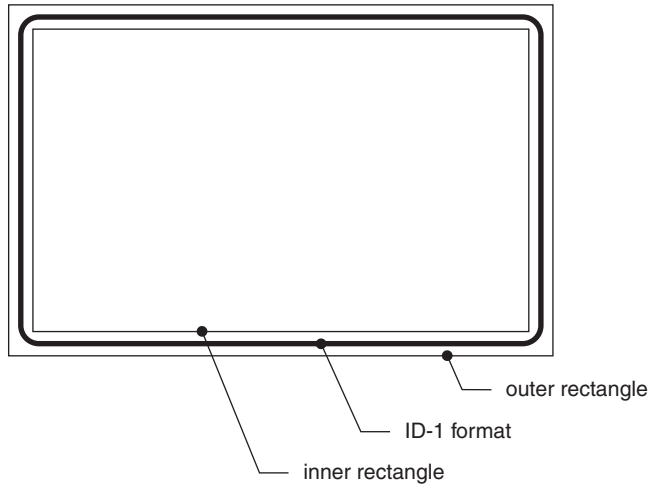

Figure 3.3 Dimensions of the ID-1 card format as specified by ISO/IEC 7810

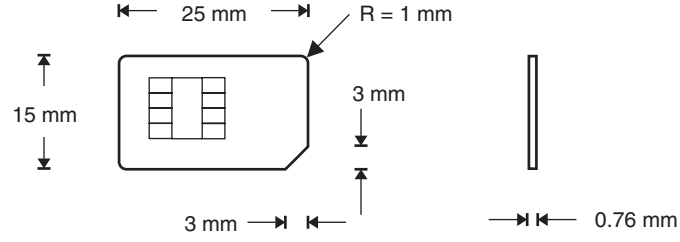

Figure 3.4 The ID-000 format. Thickness: 0.76 ± 0.08 mm; corner radius: 0.8 ± 0.10 mm; diagonal corner 2.5 ± 0.1 mm. The indicated dimensions show the size of the card excluding tolerances

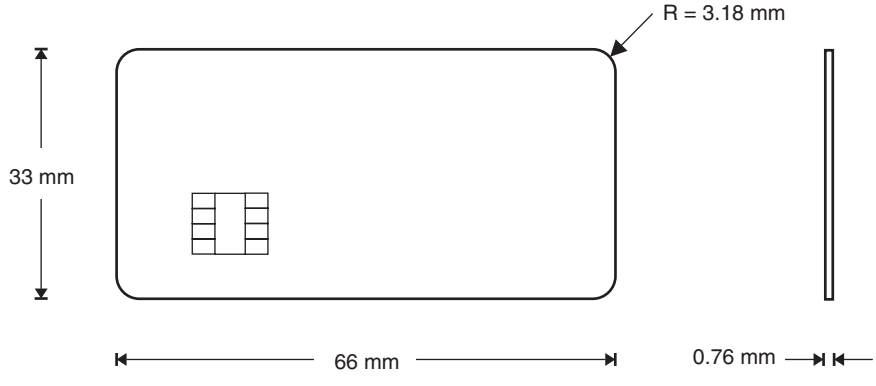

Figure 3.5 The ID-00 format. Thickness: 0.76 ± 0.08 mm; corner radius: 3.18 ± 0.30 mm. The indicated dimensions show the size of the card excluding tolerances

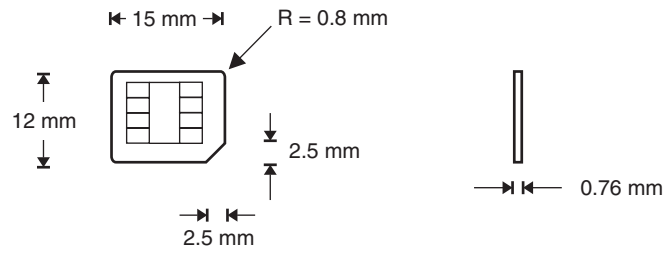

Figure 3.6 The mini-UICC format. Thickness: 0.76 ± 0.08 mm; corner radius: 0.8 ± 0.10 mm; diagonal corner 2.5 ± 0.8 mm. The indicated dimensions show the size of the card excluding tolerances

of 14.90 mm. The bottom right-hand corner of a plug-in card is beveled at angle of 45° to facilitate correct insertion of the card into the card holder.

The ID-00 format is also based on metric measurements, and its maximum and minimum dimensions are again defined by two concentric rectangles. The outer rectangle has a width of 66.10 mm and a height of 33.10 mm. The inner rectangle has a width of 65.90 mm and a height of 32,90 mm.

The mini-UICC format is the smallest possible smart card format that still allows reliable module embedding. Its dimensions are also based on the metric system and specified such that a mini-UICC card can be produced by breaking it free from an ID-000 card.

In the payment sector, the need to define a new form factor in order to create a differentiating feature relative to competitive products arose around 2003. The new card should also be suitable for carrying on a key ring, for which purpose it is required to have a hole. The result is the Visa Mini format, which is issued by the Visa credit card company. It has a width of 65.5 mm and a height of 40 mm, with a thickness of 0.76 mm, as illustrated in Figure 3.9.

To further differentiate the various card types, cards with a wide variety of dimensions are issued in the payment sector in particular, as illustrated in Figures 3.10 and 3.11 on page 35. Here the most important consideration is that these cards must also be usable in the existing infrastructure. This primarily involves magnetic stripes and embossing. The advantage of contactless smart cards becomes quite evident here, since they can take almost any desired form as long as a microcontroller and antenna can be fitted in the card body.

The ID-1, ID-00, ID-000, mini-UICC and Visa Mini formats can be produced from the larger card formats by stamping. This is especially important for card manufacturers, since it allows the production process to be designed for a single, standard format (ID-1).

For instance, card manufacturers commonly produce card blanks in only one format (preferably ID-1), embed modules in them and fully personalize them. Depending on the specific application area of the produced cards, they can then be converted to the desired format in a subsequent production operation.

Alternatively, the format may be modified later by the customer. This has become common practice with cards for mobile telephones. The customer receives an ID-1 card that is prepunched so it can be converted onto an ID-000 card by breaking it free from the larger card. In another technique, the ID-000 card is stamped entirely free from the ID-1 body and attached to the surrounding portion of the ID-1 card by adhesive tape on the side without contacts. The customer can thus convert it into a card with the appropriate format for the intended use, while the manufacturer has only to produce and ship one card format. The same approach is used if the customer needs to be able to convert the card into the smallest currently available format: mini-UICC.

Figure 3.7 Example of a mobile telephone card in ID-1 format, which the customer can convert into an ID-000 or mini-UICC card if necessary by breaking free the smaller-format version (Reproduced with permission from Giesecke & Devrient)

Figure 3.8 Example of a payment card in ID-1 format, which the customer can convert into a Visa Mini card if necessary by breaking free the smaller-format card (Reproduced with permission from Giesecke & Devrient)

However, the usual card format has some disadvantages for certain applications. In such cases, other form factors can be used, such as a USB plug with an integrated smart card microcontroller, as illustrated in Figure 3.13 on page 36. Generally speaking, the logical behavior of such smart card variants is fully equivalent to that of the usual forms.

There are also methods available for integrating smart card functionality with other components on a printed circuit board if necessary. This is typically done by fitting the smart card microcontrollers in conventional IC packages and using automated equipment to fit them on circuit boards. Some examples of SMD modules for smart card chips are shown in Figure 3.14 on page 37. The SOP8 package is often used for this purpose due to its very compact size, which is usually an important requirement in such applications. The SOP8 package has a length of 5.0 mm and a width of 4.4 mm. Its width including solder leads is 6.2 mm, with a component height of 1.5 mm. Other packages are also used, such as QFN (quad flat pack, no leads).

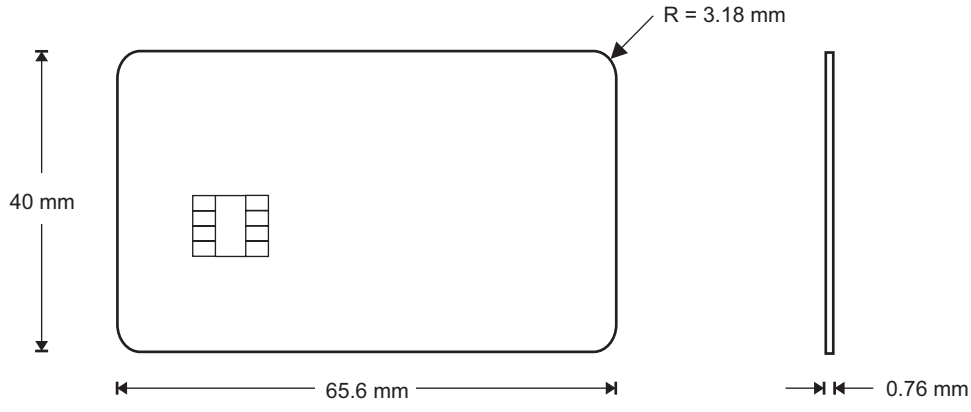

Figure 3.9 The Visa Mini format. This card is based on the ID-1 format specified in ISO 7810 and has a thickness of 0.76 ± 0.08 mm; the corner radius is 3.18 ± 0.30 mm The indicated dimensions show the size of the card excluding tolerances

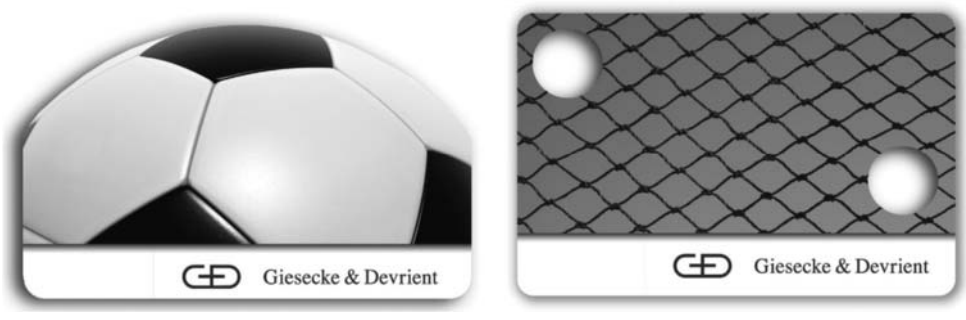

Figure 3.10 Two examples of smart cards with special shapes. They are produced as ID-1 cards and then converted to the final shape by stamping (Reproduced with permission from Giesecke & Devrient)

Figure 3.11 Examples of smart cards with special shapes. The card on the left has rounded corners, while the card on the right can be made smaller by breaking off part of the card (Reproduced with permission from Giesecke & Devrient)

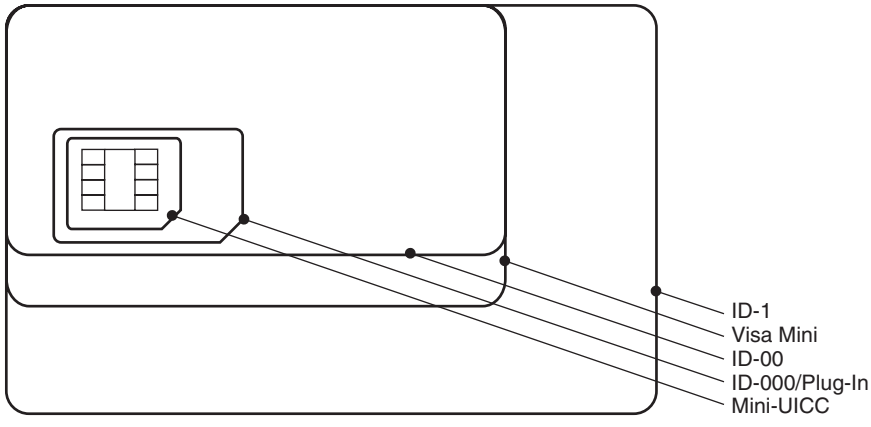

Figure 3.12 Relative sizes of the ID-1, ID-00 and ID-000 formats

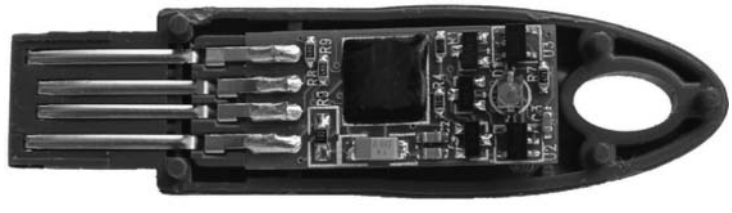

Figure 3.13 Example of an alternative smart card form factor. This photo shows a USB plug with a soldered-in smart card microcontroller and the necessary interface components, which has been opened up to reveal its internal components

3.2 CONTACT FIELD

The main difference between a smart card and other types of cards is the embedded microcontroller. If electrical power and data are transferred by direct electrical connection to the microcontroller, the card must also have electrical contacts. They consist of six or eight gold-plated contacts, which can be seen on every standard smart card. The location of these contacts on the card body and the contact dimensions are specified by the ISO 7816-2 standard, the first version of which dates from 1988.

In France, a national standard generated by AFNOR was already in use long before ISO 7816-2 was issued. It specifies a slightly higher location for the contacts than the ISO standard. This location is also included in the ISO standard as a 'transitional contacts location', although the standard recommends that this location not be used in the future. However, there are still cards in France with this contact location, so it is not likely that it will disappear all that quickly.

The absolute location of the contact field is in the upper left corner of the card body, as is illustrated in Figure 3.15 on the next page.

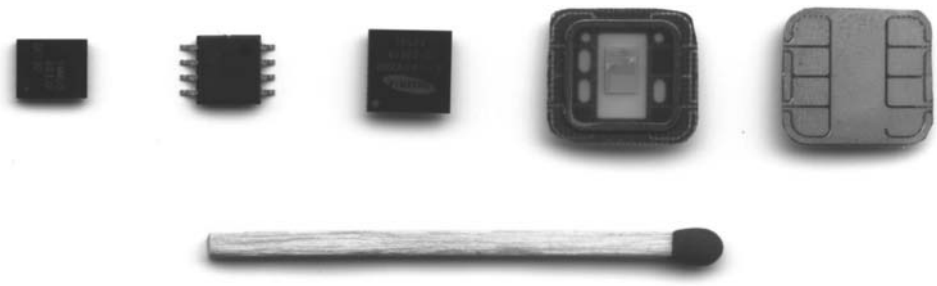

Figure 3.14 Examples of various types of SMD modules used to package smart card microcontrollers. The first and third components from the left are QFN packages, while the second component is an SOP8 package. For comparison, the front and back sides of a conventional module are shown at the right

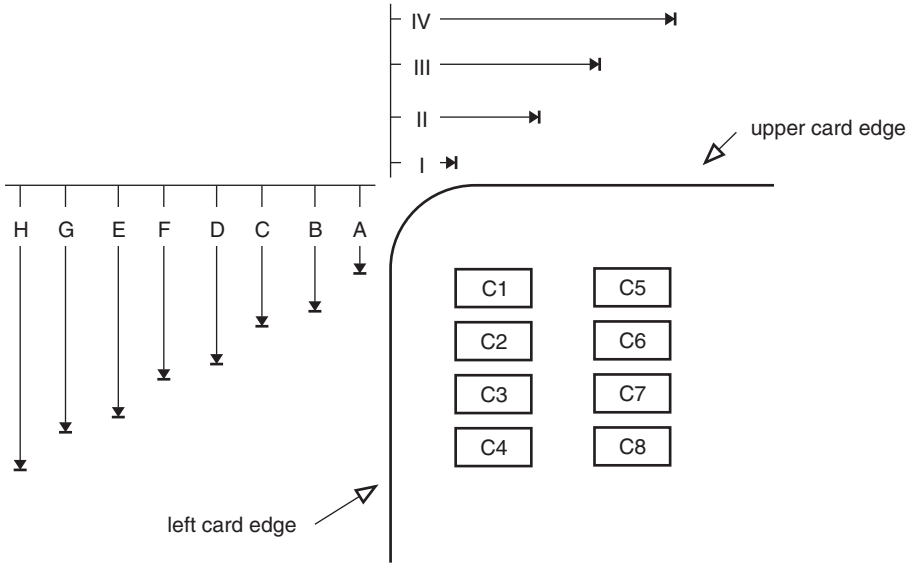

Figure 3.15 Location of the contacts on the card body (drawing not to scale). The following minimum and maximum distances are standardized: I max: 10.25 mm; II min: 12.25 mm; III max: 17.87 mm; IV min: 19.87 mm; A max: 19.23 mm; B min: 20.93 mm; C max: 21.77 mm; D min: 23.47 mm; E max: 24.31 mm; F min: 26.01 mm; G max: 26.85 mm; H min: 28.55 mm

The minimum dimensions of any contact are 1.7 by 2 mm (height by width), as shown in Figure 3.16 on the next page. The maximum dimensions of any contact are not specified, but they are of course limited by the fact that the individual contacts must be electrically isolated from each other.

The location of the module in the card body is specified in the standard. The locations of the magnetic stripe area and the area reserved for embossing are also specified precisely (see ISO 7811). All three of these components may be present on a single card. However, in this case the following mutual relationships must be taken into account: (a) if only a chip and an embossing field are present, they may be located on the same side or on opposite sides of the card; (b) if a magnetic stripe is also present, it and the embossing area must be located on opposite sides of the card. Figure 3.17 on the next page shows the various options.

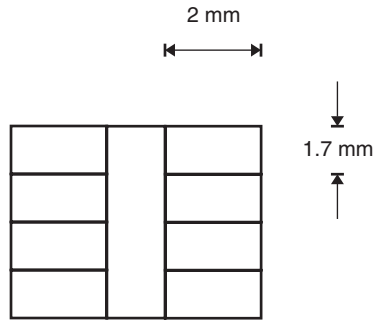

Figure 3.16 Minimum contact dimensions as specified in ISO 7816-2

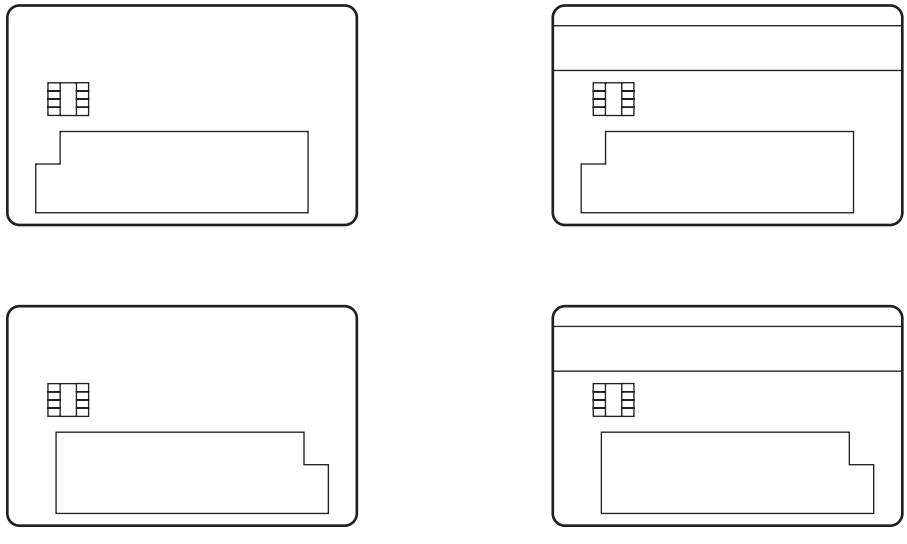

Figure 3.17 The various possible arrangements of the card components (chip, embossing field and magnetic stripe) according to the ISO 7816-2 standard

3.3 CARD BODY

The materials, construction and production of the card body are effectively determined by the card's functional components (see Figure 3.18 on page 40), as well as by the stresses to which it is subjected during use. Typical functional components of a card include:

- magnetic stripe
- signature panel
- embossing
- imprinting of personal data via laser beam (text, photo, fingerprint)
- hologram

- security printing
- invisible authentication features (e.g. fluorescence)
- chip with contacts or antenna

Clearly, even a relatively small card with a thickness of only 0.76 mm must sometimes have a large number of functional components. This places severe demands on the quality of the materials used and the manufacturing process.

The minimum requirements relating to card robustness are specified in ISO standards 7810, 7813 and 7816 Part 1. The requirements essentially relate to the following areas:

- mechanical robustness of the card and contacts
- temperature resistance
- surface profile of the card
- electrostatic discharge
- electromagnetic susceptibility
- ultraviolet radiation
- X-ray radiation

The ISO/IEC 10373 standard specifies test methods for many of these requirements, to enable users and card manufacturers to objectively test card quality. The bending and twisting tests are particularly important for smart cards, since the chip, which is as fragile and brittle as glass, is a delicate foreign object in the elastic card. Special structural features are required to protect it against the mechanical stresses produced by bending and twisting the card. Chapter 15, 'Quality Assurance', on page 633 contains a detailed list of tests and the methods used to perform them.

3.4 CARD MATERIALS

A variety of materials are used for card bodies. Their main characteristics are listed in Table 3.1 on page 41, and the structural formulas of the most important materials are shown in Figure 3.19 on the next page. The first material employed for ID cards, which is still widely used, is polyvinyl chloride (PVC), an amorphous thermoplastic material. It is the least expensive of all the available materials, easy to process, and suitable for a wide range of applications. It is used worldwide for credit cards. Its drawbacks are a limited lifetime due to physical deterioration and limited resistance to heat and cold. PVC is used in sheet form to manufacture cards, since injection molding is not possible. PVC is considered to be environmentally hazardous because the feedstock, vinyl chloride, is a known carcinogen. In addition, hydrochloric acid and (under unfavorable conditions) possibly dioxins are released when it is burned. In addition, heavy-metal compounds are often used as stabilizers. Nonetheless, PVC is still by far the most widely used material for cards. This is primarily due to its low cost and good processing characteristics. However, it is used less and less each year due to its undesirable environmental properties. Many card issuers have now decided not to use PVC for reasons of environmental policy.

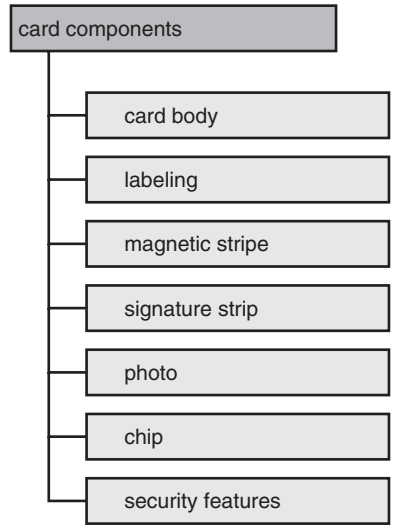

Figure 3.18 Classification of card components

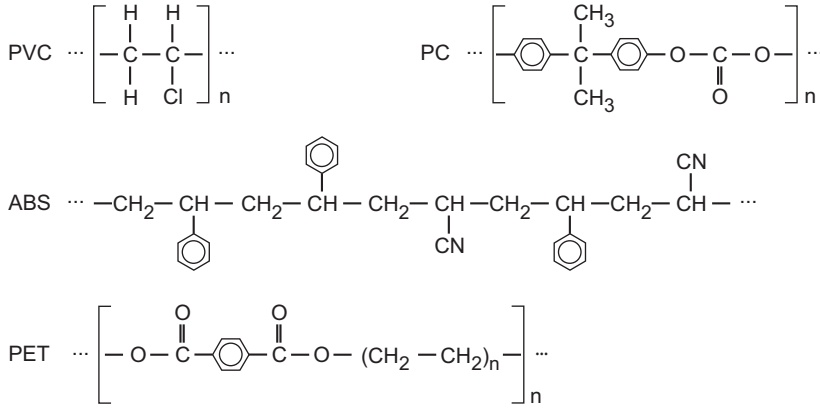

Figure 3.19 Structural formulas of the most important plastics used for card bodies

To avoid the drawbacks of PVC, acrylonitrile butadiene styrene (ABS) has been used for some time to make cards. It is also an amorphous thermoplastic that is distinguished by its high strength and resistance to temperature extremes. Consequently, it is commonly used for mobile telephone cards, which for obvious reasons may be subjected to relatively high temperatures. ABS can be processed readily in sheet form or by injection molding, and it does not have any known environmental drawbacks.

Polycarbonate (PC), which incidentally is also the substrate material of CDs and DVDs, is used for applications where high strength and durability are required. Due to its high thermal stability, relatively high temperatures are needed to apply holograms or magnetic stripes using the hot-stamp process. This can easily cause problems due to the limited thermal

Table 3.1 Summary of the characteristics of the usual card body materials. The relative cost is based on the cost of PVC

Properties	PVC	ABS	PC	PET
Primary use	Credit cards	Mobile phone cards	ID cards	Health insurance cards
Principal feature	Inexpensive	Thermally stable	Durable	Environmentally friendly
Card production	Sheet only	Sheet and injection molding	Sheet and injection molding	Sheet and injection molding
Heat tolerance	65–90°C	75–100°C	160°C	Up to 80°C
Cold tolerance	Moderate	High	Moderate	Moderate
Mechanical stability	Good	Good	Good	Very good
Embossing	Good	Poor	Good	Good
Printing	Good	Moderate	Moderate	Good
Hot stamping (e.g. for holograms, etc.)	Good	Good	Difficult	Good
Laser engraving	Yes	Poor	Good	Good
Typical lifetime	2 years	3 years	5 years	3 years
Cost	1	2	7	2.5
Environmental aspects	Burning may release dioxins Stabilizers contain heavy metals		Burning does not release hazardous materials	Currently the most environmentally friendly card material Burning does not release hazardous materials
Special aspects	Negative public image Low thermal stability		Low scratch resistance	

stability of the materials being applied. The main drawbacks of polycarbonate are its low resistance to scratching and high cost relative to other card materials. A further drawback is that phosgene and chlorine are needed for the production of polycarbonate, and both of these materials are environmentally problematical. Polycarbonate cards can be easily recognized by the characteristic 'tinny' sound they produce when dropped on a hard surface.

An environmentally friendly material that is mainly used as a PVC substitute is polyethylene terephthalate (PET), which has been used for a fairly long time as a packaging material. It is commonly known as polyester. This thermoplastic material is used in smart cards in both its amorphous form (A-PET) and its crystalline form (PETP). Both types are suitable for processing in sheet form or by injection molding. However, PETP is difficult to laminate, which makes additional processing steps necessary in the manufacturing process.

Repeated attempts have been made to find new or better materials for card bodies in addition to the four usual materials (PVC, ABS, PC and PET). One example is cellulose acetate, which although having good environmental properties has up to now proven to be poorly suited to the mass production of cards. Truly different materials, such as paper, have been frequently discussed, but as yet they have never been used in any significant quantity. The requirements imposed on cards in terms of cost, durability and quality are after all very high, and they can presently only be met by plastics.

Although it does not represent a true alternative to plastic card bodies, an interesting (or at least remarkable) field trial was carried out in 1996–97 in Denmark by Danmønt.[2] Around 6 000 smart cards with a card body made from laminated and printed birch (eight laminations, each 0.1 mm thick) were issued. Although these cards did not pass the various tests specified in ISO 10373, such as the bending and twisting tests, and they were naturally not suitable for embossing, around 90 % of their users responded positively and said that they experienced no problems with their cards. Unfortunately, laminated birch cards are not especially innovative from an environmental perspective because the layers must be laminated with a synthetic glue and the usual printing processes are still necessary.

3.5 CARD COMPONENTS AND SECURITY FEATURES

Smart cards are primarily used to provide authorization for specific actions or identify the cardholder, so security features on the card body are often needed in addition to the embedded chip. To enable the authenticity of the card to be checked by humans as well as by machines, many security features are based on visual elements. However, some security features employ a modified smart card microcontroller and thus can only be checked by a computer. In contrast to the security features used with microcontrollers, the usual features for human verification of card authenticity are not based on cryptographic methods (such as mutual authentication). Instead, they are primarily based on secret materials and production methods or technological processes whose mastery requires a large amount of effort and considerable expertise or is technically difficult.

Particularly with regard to new card components, there is considerable potential for innovations in the near future because one of the possible evolution paths of smart cards is in the direction of additional integrated components such as a keypad, display, solar cell, and battery, as illustrated in Figures 3.20 and 3.21 on the next page.

3.5.1 Guilloche patterns

A somewhat more complicated technique is to insert a foil printed with color guilloche patterns under the transparent outer foil of the card. Guilloche patterns are decorative patterns consisting of very fine interwoven lines, usually circular or oval, such as are found on some bank notes and share certificates (see Figure 3.22 for an example). These patterns have such fine structures that they can presently only be produced by special printing processes and are thus difficult to copy.

[2] [a la Card 97]

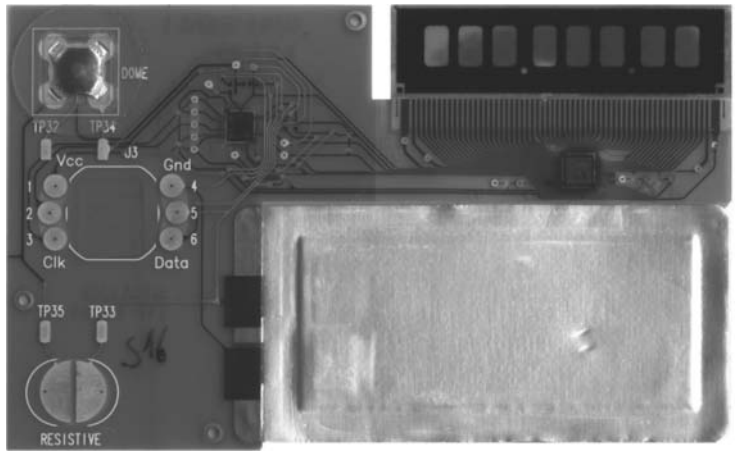

Figure 3.20 Inlay foil for a super smart card. A pushbutton switch is located at the upper left, with the connections for the actual smart card microcontroller below. A display is located at the upper right, with the display controller below. The rectangular component at the bottom right is the battery that powers the card (Reproduced with permission from Giesecke & Devrient)

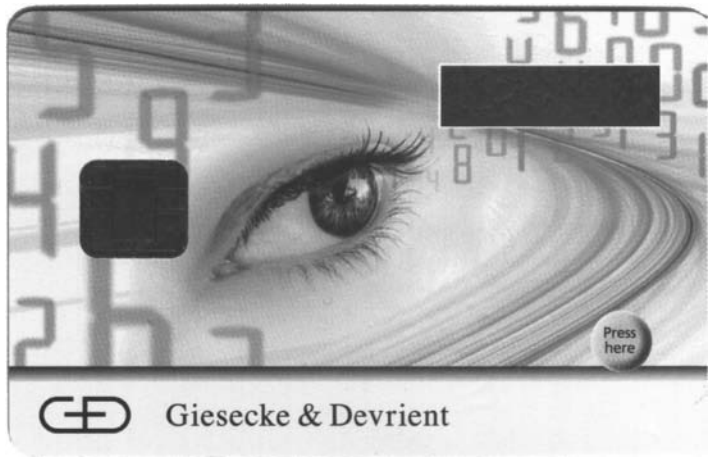

Figure 3.21 Inlay foil for a super smart card for contactless and contact communication. A pushbutton switch for confirming transactions is at the bottom right, and a display for showing the purse balance and other data is at the upper right (Reproduced with permission from Giesecke & Devrient)

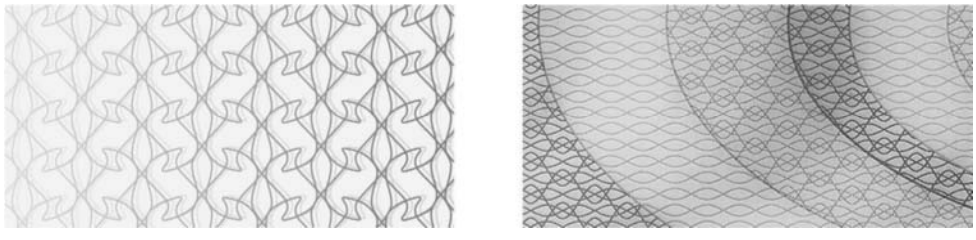

Figure 3.22 Examples of originally multicolored guilloche patterns (highly enlarged). They cannot be printed using ordinary commercial printing processes (Reproduced with permission from Giesecke & Devrient)

3.5.2 Signature panel

A very simple way to identify the cardholder is to use a signature panel bonded to the card, as is common with credit cards. Once such a panel has been signed, it cannot be altered, so it is erasure-proof. A very fine colored pattern printed on the panel makes any attempt to glue something on top of the panel immediately apparent. The signature panel is permanently bonded to the card body by using a hot-glue process to attach a printed paper strip to the card. Alternatively, the signature panel can be part of the top layer of the card body, laminated into the card when it is assembled.

3.5.3 Microtext

Another technique that is based on the security provided by fine printed structures is microtext lines. They look like simple lines to the naked eye, but they can be recognized as text under a loupe (see Figure 3.23 for an example). Like guilloche patterns, microtext cannot be photocopied.

Figure 3.23 A highly enlarged example of microtext, which cannot be printed using ordinary commercial printing processes (Reproduced with permission from Giesecke & Devrient)

3.5.4 Ultraviolet text

To avoid affecting the visible layout of the card, control characters or control numbers can be printed on the card using ink that is only visible under ultraviolet light.

3.5.5 Barcode

For storing a small amount of data, a barcode can be printed on the surface of the card using laser printing or thermal-transfer printing. The advantage of barcodes is that they can be read automatically at close range using optical equipment. The barcodes used on smart cards include not only the widely use one-dimensional type, but also two-dimensional barcodes in the form of stacked or matrix barcodes. A two-dimensional barcode, such as PDF 417, can easily encode up to 1000 bytes. If an integrated Reed–Solomon code is used for error correction, the data can be recovered even if up to 25 % of the barcode area is unreadable.

3.5.6 Hologram

A hologram integrated in the card is a security feature that is now familiar to all card users (see Figure 3.24 for an example). The security of holograms is primarily based on the fact that they are produced by only a few companies in the world and their availability is restricted.

Figure 3.24 Example of a hologram attached to a substrate printed with guilloche patterns (originally multicolor) (Reproduced with permission from Giesecke & Devrient)

The holograms used for smart cards are called 'embossed' holograms, since they must be recognizable under diffuse reflected daylight illumination. For this reason, they are also called white-light reflection holograms. By contrast, a conventional transmission hologram requires coherent laser light for proper viewing. Supplementary security features that can only be seen with laser light are sometimes incorporated in the hologram. In order to produce an embossed hologram, a master hologram must first be generated using the conventional holographic recording method. A master embossing stamp is then prepared from the master hologram using a transfer process. The embossing stamp contains the microstructures that will produce the subsequent embossed holograms. Daughter stamps are made from the master stamp using electroplating processes, and these daughter stamps are used to emboss the hologram structure in plastic films. These films are then vapor-coated with aluminum to produce the well-known white-light reflection holograms.

The hologram is permanently bonded to the card body and cannot be removed without destroying it. The bonding can be performed using either lamination or the roll-on method. With the latter method, a hologram located on a carrier film is pressed onto the card by a heated roller. The carrier film is then pulled off, and the hologram remains permanently welded to the plastic card body. A third option is the hot-stamp method, which is similar to the roll-on method but uses a heated stamp instead of a heated roller.

3.5.7 Kinegram

Kinegrams have same structure as holograms, but they show different images when viewed at different angles. Kinegrams are just as hard to forge as holograms, and they have the advantage that they are more readily recognized and thus can be checked more quickly.

3.5.8 Multiple laser image (MLI)

A multiple laser image is a sort of kinegram that is very similar to a simple hologram. It is based on an array of lenses embossed in the surface of the card, some of which are blackened by a laser. The main difference between an MLI and a hologram is that card-specific information is shown in the small MLI image. For instance, this technique can be used to mark an individual card with the cardholder's name in the form of a kinegram.

A small trick (which incidentally also works with all personalization features of this sort) is used to ensure that the authenticity of the MLI is also checked when the card is verified manually. Some of the information necessary for the verification process (such as the expiry date), which must be read during the verification process, is stored in the MLI. As a result, the person who verifies the card more or less automatically checks the authenticity of the feature by reading this information. This would not necessarily happen if the feature were not merged into the verification process in this manner.

3.5.9 Embossing

Another way to add user data to a card is to emboss characters on the card, as shown for example in Figure 3.25. This is done by hammering metal letter punches against the card with considerable force. In principle, this works the same way as a mechanical typewriter. Nowadays there is only one reason for using embossing, but it is very important in practice: the characters of embossed cards can be copied relatively easily onto preprinted forms using carbon paper. On the global scale, this is still the most widely used method of paying with a credit card.

It is very easy to manipulate embossed characters, since the plastic can be flattened by moderately heating the embossed characters (using an iron, for example). Different characters can them be embossed in place of the original ones. To prevent this sort of manipulation, some

Figure 3.25 An example of a credit card with embossing and an antenna for contactless communication. This is a functional sample without issuer-specific printing (Reproduced with permission from Giesecke & Devrient)

of the embossed characters are often placed in the hologram, which will be destroyed if it is heated.

3.5.10 Laser engraving

Darkening a special plastic layer by charring it with a laser beam is called laser engraving (see Figure 3.26), or simply lasing. In contrast to embossing, this is a secure way to write information on an individual card, such as the cardholder's name and the card number. It is secure because the necessary equipment and the knowledge of how to use it are not readily available.

Two different methods are used for laser engraving: vector engraving and raster engraving. In the vector method, the laser beam is directed along its path without interruption. This is very well suited to writing characters and has the advantage of being quick. With the raster method, by contrast, a large number of adjoining points are blackened to produce an image, similar to the operation of an inkjet or dot-matrix printer. This method is primarily used to place a picture on the card. Although it has the advantage of high resolution, which allows details to be reproduced well, it has the disadvantage of being very time-consuming. For instance, it takes approximately ten seconds to laser engrave a standard-quality passport photograph.

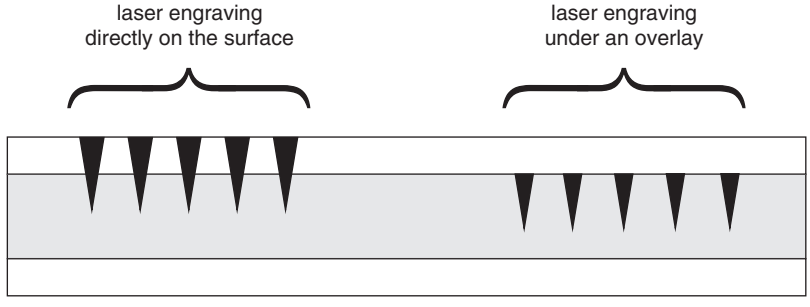

Figure 3.26 Cross section of laser engraving on a card (not to scale). Laser engraving can be performed either on the surface of the card or in an internal layer below a cover foil that is transparent to the laser light

3.5.11 Scratch field

It is sometimes necessary to mark a smart card with a confidential, sealed multidigit number or character string. This card-specific data can be used for purposes such as enabling a particular function or crediting a balance. A scratch field can be laminated onto the card for this purpose. The scratch field consists of a printable substrate covered by a seal layer that can be scratched off as illustrated by several examples in Figure 3.27.

The confidential data is printed on the substrate, which is then covered by the seal layer. The seal layer must have several specific properties. It must be possible for everyone to readily recognize that the layer has been removed, even if this is done with the aid of heat or cold. In addition, the printed data must not be visible from the rear if the entire scratch field is removed from the card body. It must be impossible to read the printed data underneath the

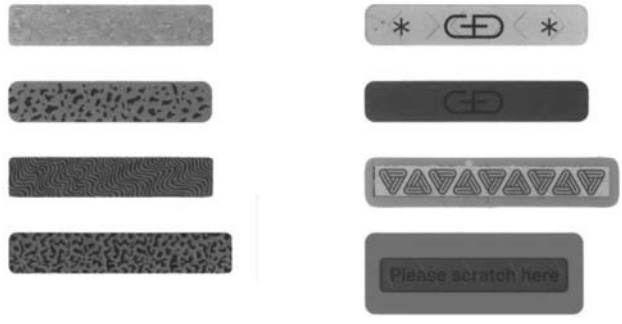

Figure 3.27 Several types of scratch fields (multicolored in the original) (Reproduced with permission from Giesecke & Devrient)

seal layer by using visible, ultraviolet or infrared light. This is essential in order to ensure that the confidential data under the seal layer cannot be spied out before the user scratches off the protective layer.

3.5.12 Thermochrome display

There are applications in which it is desirable to be able to modify the text and imagery on a card from time to time. A good example is a student identification card in the form of a smart card that must be renewed every six months. Ideally it should be possible to read the expiry date without technical aids, which means that it should be possible to print it on the card in addition to storing it in the chip.

Smart cards with microcontroller-driven displays are currently technically possible, but they are still too expensive for large-scale use. Thermochrome (TC) displays are a simple alternative that have some drawbacks compared with real displays, but which are inexpensive and already available. A TC display is a supplementary card component on which characters and imagery can be printed reversibly (printed and subsequently reprinted) using a special card reader.

The operating principle is relatively simple: a print head with a resolution of 200 or 300 dpi, such as is used in thermal-transfer and dye-sublimation printers, is used to heat individual pixels on a thermochrome strip laminated to the card, which has a thickness of 10 to 15 μm. The strip turns dark at the points where it is heated to 120 °C. The darkened areas can be restored to a nearly transparent state by heating the entire TC strip, which amounts to erasing the strip.

The thermochrome method is presently the only economical manner to provide card users with temporary information on the surface of the card that can be read without special equipment. Its major disadvantages are that it is subject to fraud and that it requires special card terminals with built-in thermochrome printer mechanisms.

3.5.13 Moduliertes Merkmal (modulated feature) method

In 1979, the German banking industry decided to incorporate a machine-readable security feature in all German Eurocheque (ec) cards. After several different methods were tested, the Moduliertes Merkmal (MM) method (developed by the firm GAO, now known as Giesecke &

Devrient) was selected as the security method for German ec cards. This security feature is still used in all German Eurocheque cards, even though they are now equipped with microcontroller chips. The objective of this security feature is to prevent unauthorized copying or manipulation of the magnetic-stripe data.

The MM method is a typical example of a secret and very effective security feature. It has been used for more than two decades in millions of cards. Its basic structure is described in summary form in an article by Siegfried Otto [Otto 82].

The name 'MM method' comes from the German term *moduliertes Merkmal* (modulated feature), which can be understood as referring to a machine-readable substance that is incorporated inside the card body [Meyer 96]. A card is verified by reading its MM code using a special sensor and passing the code to a security module called the 'MM box'. The MM box also receives all the data from the magnetic stripe, in particular the MM check value, which is also stored on the magnetic stripe. Inside the MM box, a one-way function based on the DES algorithm is used to calculate a value from the magnetic-stripe data and the MM code. If the result of this calculation is the same as the MM check value, it can be concluded that the magnetic-stripe data matches the card.

If a valid set of magnetic-stripe data is written to a blank card, this will be detected by the fact that the blank card does not have the MM feature. Copying the magnetic-stripe data from one ec card to another ec card can also be detected because the MM check value will not match. The MM feature is invisible, and the details of how it works and where it is located in the card are secret. In addition, it is produced using materials and technology that are not commercially available.

A MM box is built into in every German bank machine (ATM), as well as some POS terminals. These devices can thus check whether the magnetic-stripe data matches the card, as illustrated in Figure 3.28 on the following page. The method itself is not specified by any standard, and it is used only in Germany. Thanks to the MM method, the magnetic stripes of German Eurocheque cards are protected against copying, which nowadays does not otherwise present any technical difficulties.

As the security of the MM method is primarily based on materials and technology instead of secret keys, confidentiality is essential for protecting it against attacks. Generally speaking, confidentiality is a widely used and well-proven way to achieve additional protection with physical security features of this sort.

3.5.14 Security features

An especially large number of visual security features were developed in the period between the large-scale use of cards without chips and the introduction of smart cards. During this period, such features were the only way to verify the authenticity of the cards. The embedded microcontrollers in the new cards and the cryptographic methods that they make possible have diminished the importance of these features. They are nevertheless still very important whenever the authenticity of a card must be verified by a person instead of a machine, since a person cannot access the chip without special equipment.

Here we can only provide a highly condensed description the essential and best-known security features used with cards. There are many other features available, such as invisible markings that can only be seen with IR or UV illumination, magnetic codes, and special printing processes using rainbow-colored inks.

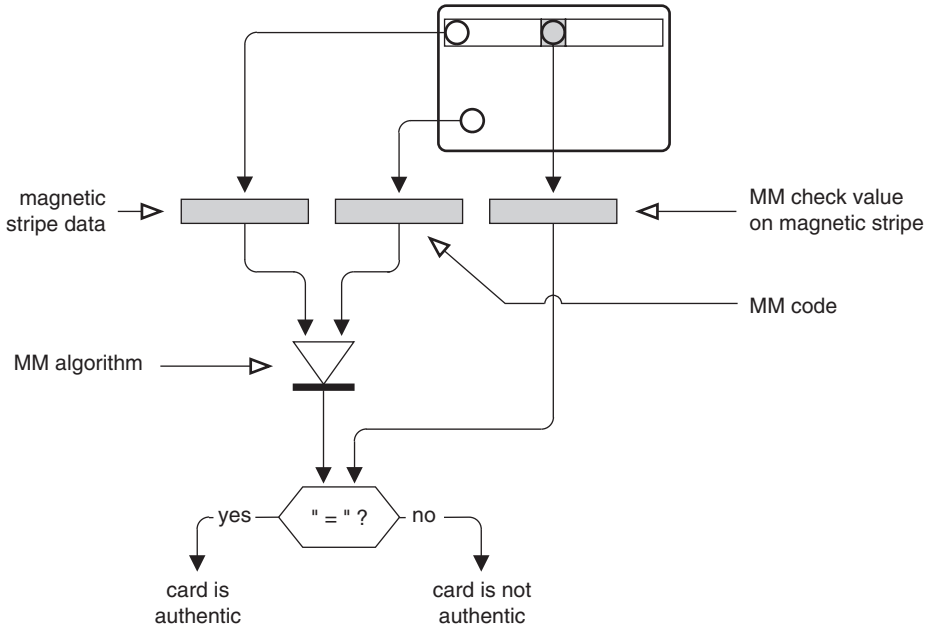

Figure 3.28 Operating principle for verifying the authenticity of a German Eurocheque card using the MM method. The security module (MM box) protects the MM algorithm and the subsequent comparison; only a yes/no result is reported to the higher-level system

In principle, it would be possible at some time to have security features in the chips as well as on the card body. It is conceivable that security chips could be used in the same way as banknote paper is now used. Genuine bank notes cannot be printed without real banknote paper, which has specific features to show that it is genuine. In order to incorporate similar security features into chips, special chips with specifically modified hardware are necessary. A terminal can then detect the modification, which constitutes the feature of the chip, and assess the genuineness of the chips from the result.

As an example of a hardware feature, suppose that computation of a fast cryptographic algorithm is implemented in supplementary hardware in a certain chip. The time required to compute a particular value could be made so short, thanks to the hardware implementation of the algorithm, that it would not be possible to perform the same computation in an equally short time using a software emulation with a different chip. A terminal could thus distinguish this chip from other chips by making a simple timing measurement. There are chips available with hardware features similar or identical to what we just described. Naturally, they are not freely available, just as banknote paper is not freely available. Of course, such hardware features are only suitable for very large-scale applications due to the high cost of developing chip-specific hardware. The fact that such chips are almost inevitably available from only one manufacturer, with no possibility of an alternate source, is also difficult for many card issuers to accept.

3.6 CHIP MODULES

The most important component of a smart card is naturally the chip. This very fragile component cannot simply be laminated to the surface of the card like a magnetic stripe. Instead, it

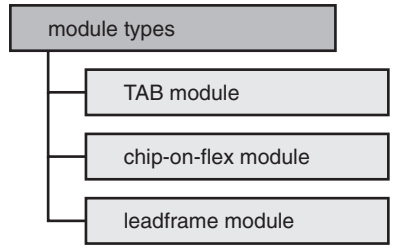

Figure 3.29 Classification of the various types of chip modules

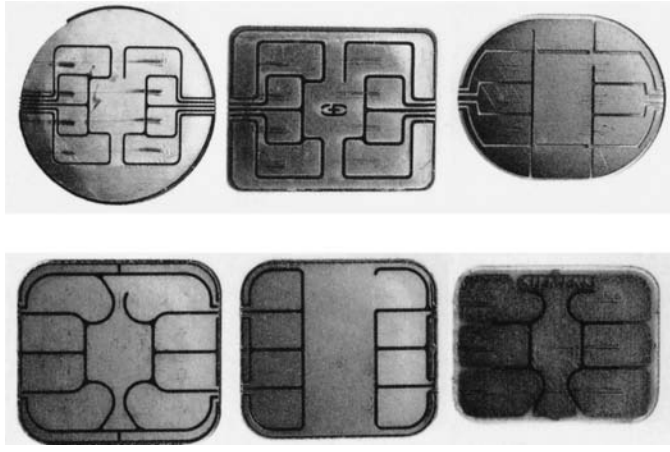

Figure 3.30 The evolution of chip-on-flex technology illustrated by several examples, starting with one of the first eight-contact chip-on-flex modules at the upper left and proceeding to modern modules with six or eight contacts

needs a sort of enclosure to protect it from the rough everyday world of the card. This enclosure is called a chip module, or sometimes a micromodule. In addition to protection from ambient conditions, chips for contact smart cards need six or eight contacts that provide power to the chip and enable data communication with the terminal. A portion of the module's surface is used to provide these electrical contacts to the outside world. Naturally, the chip module should be as inexpensive as possible.

A wide variety of module designs have been devised in the course of smart card development in order to meet these two requirements – protection of the fragile semiconductor chip and provision of contact surfaces. The most important types are listed in Figure 3.29 and illustrated in Figure 3.30.

3.6.1 Electrical connections between the chip and the module

Electrical connections are needed between the chip inside the module and the contacts on the outside of the module. Presently, two methods are generally used for this. With the

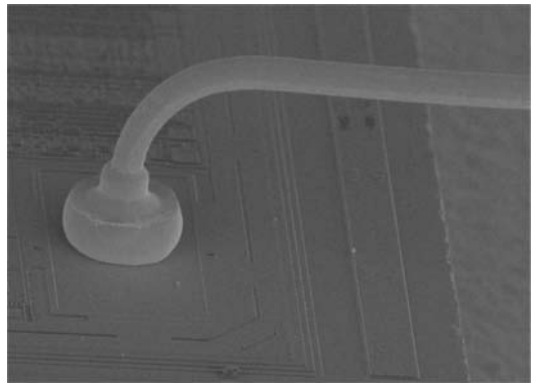

Figure 3.31 Photograph of the joint between a bonding wire and a bonding pad of a smart card microcontroller, magnified 1000 times (Reproduced with permission from Giesecke & Devrient)

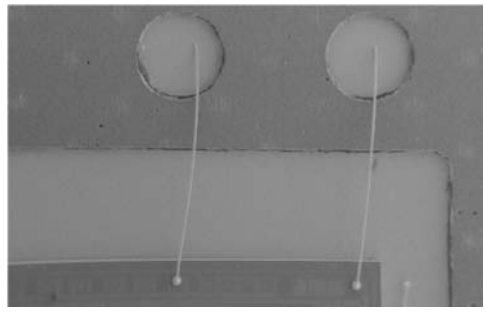

Figure 3.32 View of the electrical connections between a smart card microcontroller (bottom) and the chip module (top), magnified 400 times (Reproduced with permission from Giesecke & Devrient)

wire-bonding method (see Figures 3.31 and 3.32), an automatic bonding machine connects thin gold wires (only a few micrometers in diameter) between the chip and the backs of the contacts. The wires are electrically bonded to the chip and the module using ultrasonic welding. With this method, the contact arrangement on the top surface of the chip is always opposite that of module. This has been a standard method in the semiconductor industry for a long time, and it can be readily used for mass-producing chip modules. Each chip must be electrically connected to the module by five wires.

The die-bonding method was developed to further reduce the cost of fitting chips into modules. With this method, the electrical connections between the chip and module are not made with wires. Instead, the chip is mechanically attached to the back of the module such that each of its contacts is electrically connected to the module.

Another method is flip-chip technology (see Figures 3.33 and 3.34 on page 53), in which the chip is placed with its face against the back of the module with the electrical connections to the module provided by small solder bumps, after which the assembled module is filled with a casting resin. This type of low-cost module is usually designated FCOS (flip-chip on substrate). To ensure backward compatibility with the widely used wire-bonding technology, FCOS chips

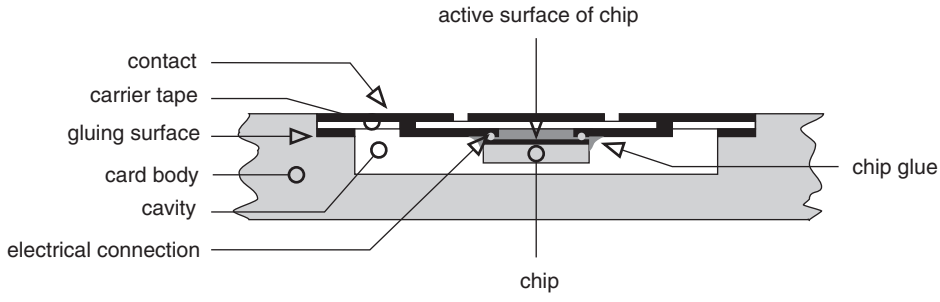

Figure 3.33 Cross section of a chip module made using flip-chip technology

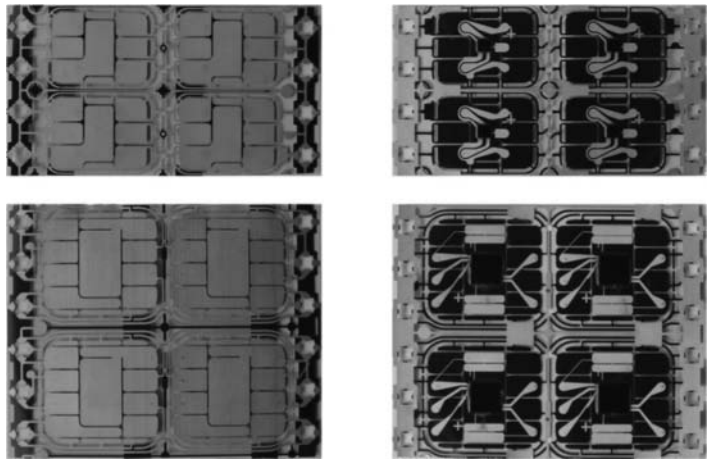

Figure 3.34 Front and back sides of modules for flip-chip technology

often have solder bumps for flip-chip connection as well as the previously standard pads for wire bonding. Such flip-chips can be used equally well in lead-frame and chip-on-flex processes.

3.6.2 TAB modules

Although tape-automated bonding (TAB) was the standard technology for large-volume chip packaging in the early 1990s, it is rarely used now. It has become technically obsolescent and too expensive. It is described here only for the sake of completeness.

Figures 3.35 and 3.36 on the following page illustrate the use of TAB technology for chip modules in smart cards. A specific feature of this technology is that metallic bumps are first electrically attached to the pads of the chip, and the leads of the carrier film are then soldered to these bumps. The solder connections are so sturdy that no additional support is required for the chip, which hangs from its leads. The active surface of the chip is protected against ambient conditions by an encapsulation resin. The advantages of TAB technology are the mechanical strength of the connections to the chip and the low profile of the module. However, these advantages come at the price of higher cost relative to other module technologies.

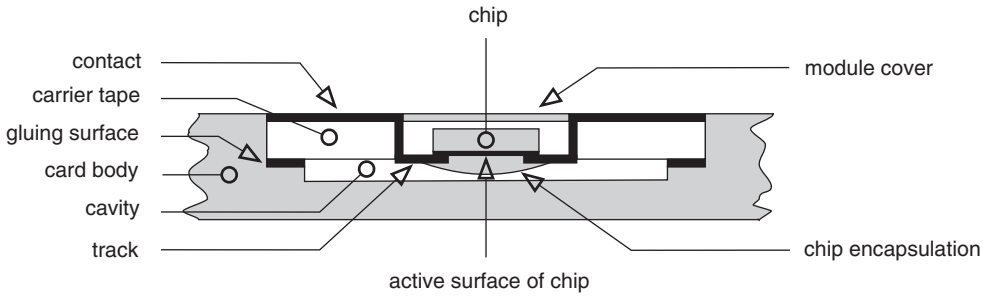

Figure 3.35 Cross section of a chip module in TAB technology

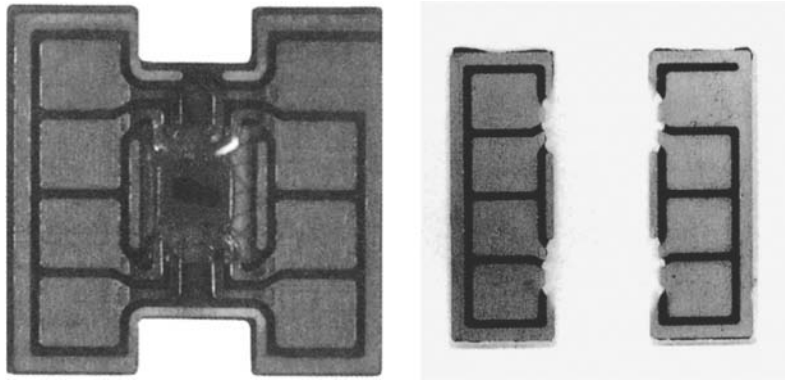

Figure 3.36 A TAB module ready for embedding in a smart card (left), and a TAB module fitted in a smart card (right)

Fitting a TAB module into a smart card is not easy, since the module properties must be taken into account when preparing the lamination foils for the card. Suitable openings are punched in the layers before they are laminated, and then the chip module is inserted. The chip module is welded to the card body during the lamination process. This method produces a very reliable bond between the chip module and the card body. It is nearly impossible to remove the chip from the card without destroying the card.

3.6.3 Chip-on-flex modules

Currently, chip-on-flex modules with wire-bonded chips are the most commonly used type. The structure of such a module is shown in cross section in Figure 3.37 on the next page. With this method, an opening into which the chip module can be glued is milled in the finished card body. The structure of chip-on-flex modules, the production process for these modules, and module embedment in smart cards are illustrated in Figures 3.37 to 3.42 on the following pages.

The substrate is a thin circuit board made from fiberglass-reinforced epoxy resin with a thickness of 120 µm. The contacts are formed from a 35- or 75-µm copper layer laminated onto

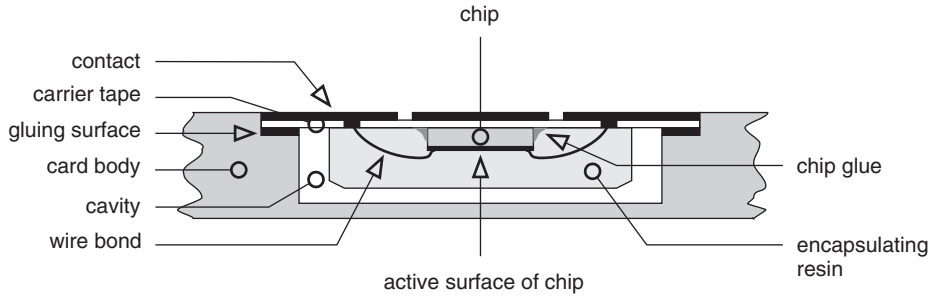

Figure 3.37 Cross-section of a chip-on-flex module

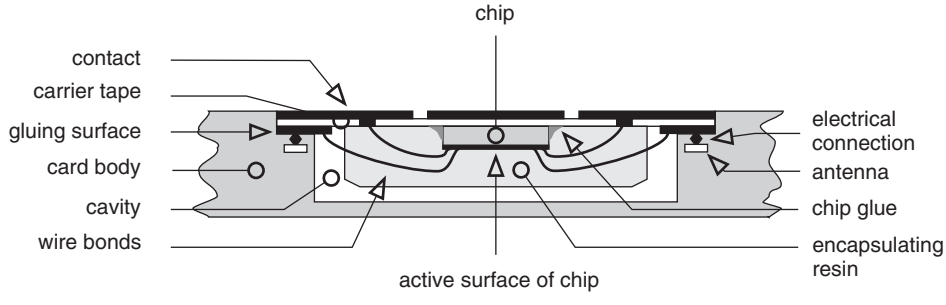

Figure 3.38 Cross-section of a chip module in chip-on-flex technology with supplementary antenna connections for contactless communication

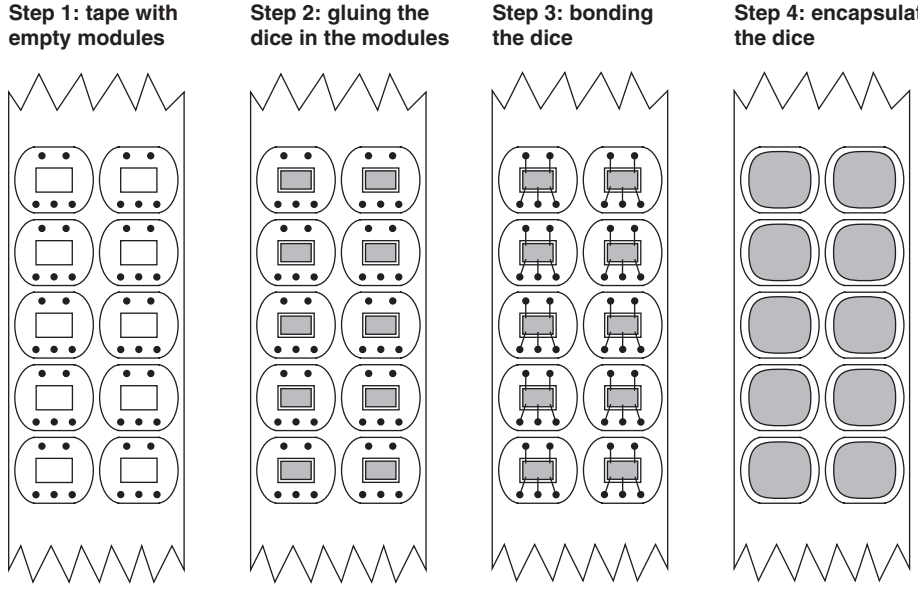

Figure 3.39 The most important process steps in the production of chip-on-flex modules

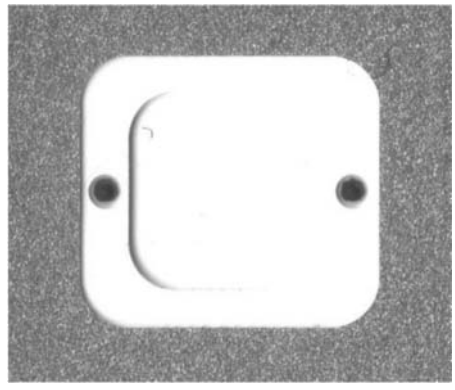

Figure 3.40 Rear view of a chip-on-flex module for a dual-interface card. The two contacts for the electrical connection between the chip module and the antenna embedded in the card body can be seen to the left and right of the first level of the cavity. The cross section of the corresponding module is shown in Figure 3.38 on the previous page

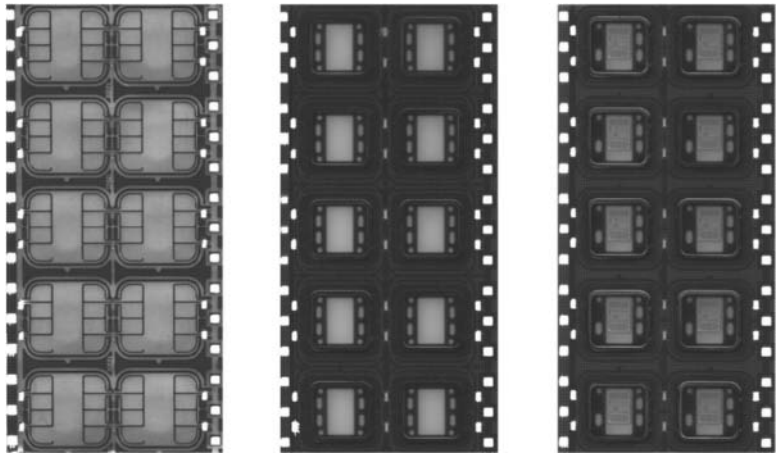

Figure 3.41 Front and rear views of chip-on-flex modules on 35-mm tape. The second figure shows the module without the chip, and the figure on the right shows the module with the bonded chip. The five openings in the substrate board for the bonding wires are clearly visible at the rear

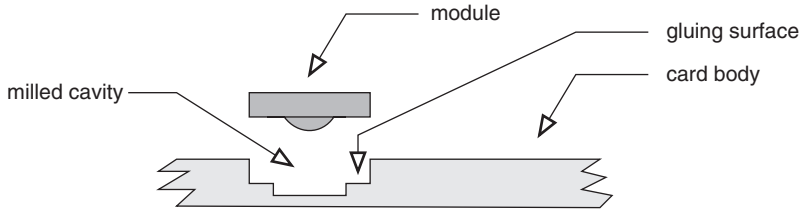

Figure 3.42 Inserting a chip module in a milled card body

the substrate, which is subsequently gold plated using an electrolytic process. This protects the contact surfaces from processes that could degrade their electrical conductivity, such as oxidation. Holes are punched in the substrate to receive the chips and the bonding wires. The chips, which are around 200 µm thick, are taken from the sawn wafer by a pick-and-place robot and attached to the rear of the modules by inserting them in the prepared openings in the circuit board material. Next, the chip contacts are connected to the backs of the contacts using bonding wires a few micrometers in diameter. Finally, the chip and the bonding wires are encapsulated in a blob of opaque resin to protect them against ambient conditions. The total thickness of the finished module is typically around 600 µm.

The advantage of this method is that it is largely based on a standard process used in the semiconductor industry for packaging chips in standard packages, which makes it relatively inexpensive. This method also lends itself well to producing very complex card bodies with many functional elements, since card bodies with manufacturing defects can be rejected before the expensive chip modules are inserted. The disadvantage is that the thickness and area of the chip module are larger than with a TAB module, since not only the chip but also the bonding wires must be protected by the encapsulation. This is especially disadvantageous because the standard smart card thickness of 0.76 mm does not allow much room for overly thick modules.

3.6.4 Lead-frame modules

From a technical perspective, TAB and chip-on-flex technologies are suboptimal because they provide little scope for reducing production cost. With TAB technology, producing the card body is very costly due to the module, and with chip-on-flex technology, the complexity of the module and the wire bonding process create an unfavorable production cost situation. These considerations led to the development of a type of module that has the same mechanical robustness as TAB and chip-on-flex technology but lower production costs: the lead-frame module.

The structure of a lead-frame module is relatively simple. The contact leads, which are stamped from a sheet of gold-plated copper alloy, are held together by a plastic mold body. A chip is placed on the lead-frame module by a pick-and-place robot and wire-bonded to the backs of the leads. The chip is then covered by a protective blob of opaque epoxy resin, usually black. Figure 3.43 shows the structure of a lead-frame module, while Figures 3.44 to 3.46 on the following page show examples of these modules.

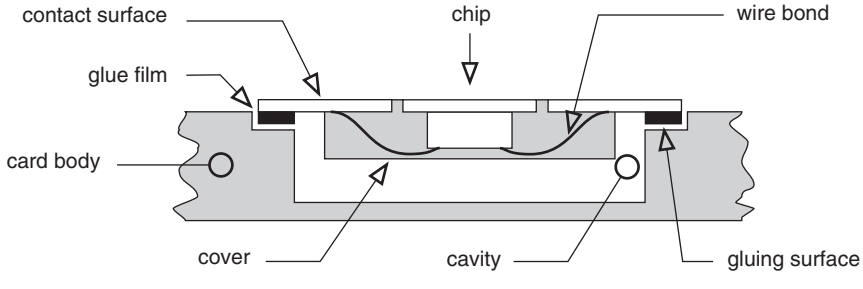

Figure 3.43 Cross section of a chip module in lead-frame technology

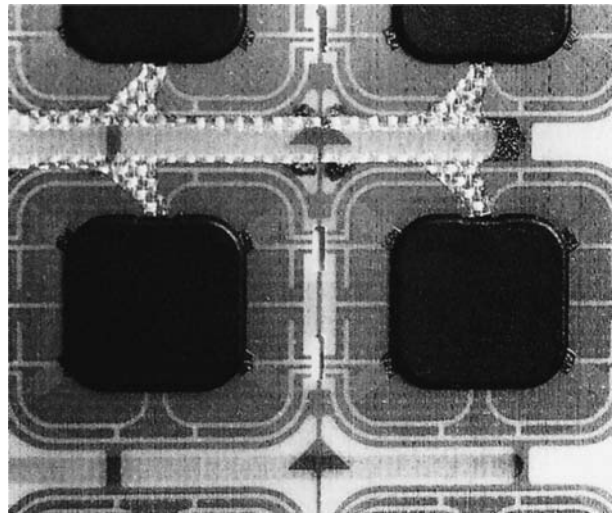

Figure 3.44 Lead-frame modules for contact smart cards, arranged in pairs on 35-mm tape

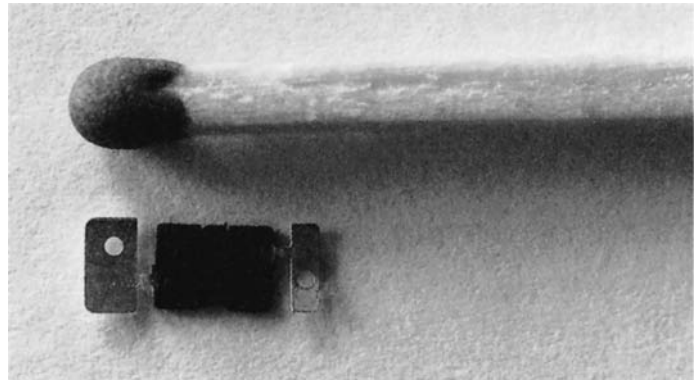

Figure 3.45 A stamped lead-frame module with two coil contacts for a contactless smart card, shown next to a match for comparison

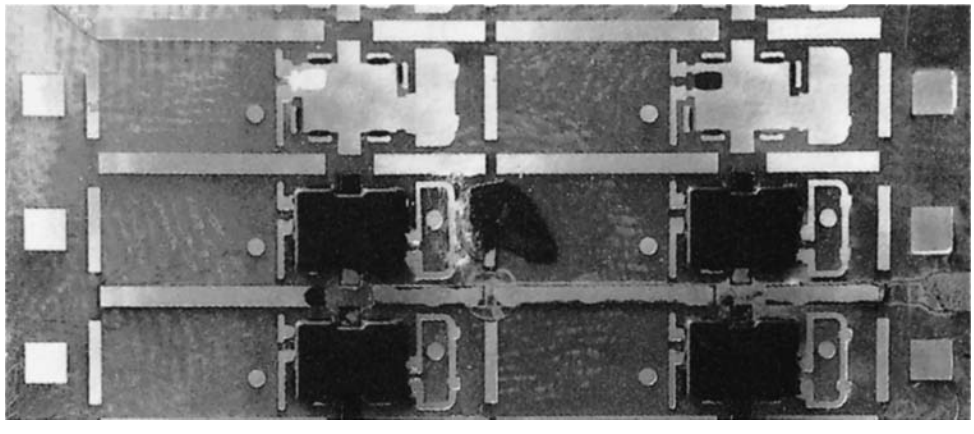

Figure 3.46 Lead-frame modules for contactless smart cards, arranged in pairs on 35-mm tape. Two holes where modules have already been stamped out can be seen at the top

Figure 3.47 A smart card with a special module for direct connection to a PC. Its four contacts have the same form as a USB plug. After the card is broken free from its carrier and placed in an adapter, it can be plugged into the USB port of a computer. This arrangement allows smart card technology to be used directly with computers, without using an intermediate terminal (Reproduced with permission from Giesecke & Devrient)

Lead-frame technology is currently one of the least expensive ways to produce chip modules, with no penalties in terms of the mechanical robustness of the modules.

3.6.5 Special modules

There are also various types of special modules for special applications. Chip modules can be designed to mate with a standard USB connector, including the four electrical connections. In combination with a suitable USB-compatible smart card microcontroller, they can be used to produce smart cards that can be used directly with a PC with no need for a terminal or adapter. Figure 3.47 shows an example of such a product.

4

Electrical Properties

The electrical properties of smart cards depend solely on the embedded microcontroller, since it is the only component of the card with an electrical circuit. This situation will undoubtedly change in the future with the addition of other components to cards, such as displays, keypads and the like, but it will take some time before these new types of smart cards are widely used.

The application that from the very beginning has imposed many stringent requirements on the electrical properties of smart cards is mobile telecommunication in the GSM system. This system, in which an extremely large variety of terminal equipment from a large number of manufacturers must operate with a variety of card types that is probably even larger, has for a long time imposed extremely severe requirements. Due to the large number of smart cards used in the GSM system, the electrical characteristics specified for GSM cards have assumed the status of general requirements for all manufacturers of smart card microcontrollers. It can be assumed that nearly all new smart card microcontrollers comply with the general electrical parameters of the relevant GSM specifications, as otherwise they could not be marketed in the telecommunication sector.

In the early days of smart card technology, in many cases the primary concern was ensuring that the implanted microcontroller was functional, with less attention given to its general electrical properties, such as current consumption. At that time, almost all applications were closed applications using a single type of smart card together with a terminal designed to match the card. The electrical properties of the smart card were relevant only in the sense that they had to be consistent, since the terminal was designed to work with a particular type of microcontroller. However, the present situation is entirely different. With current large-scale applications in which different types of smart cards must work together with many different types of terminals, it is an unavoidable requirement that all of the cards used in the system are either electrically identical or at least have uniform electrical characteristics within clearly defined bounds.

The ISO/IEC 7816-3 standard and Amendment 1 of this standard form the general international basis for the electrical properties of smart cards. The amendment will be incorporated into the main body of the standard in the next major revision and thus disappear as a separate document. This standard specifies all of the fundamental electrical requirements for smart cards, such as voltage ranges, maximum current consumption, and the activation and deactivation sequences.

Smart Card Handbook: Fourth Edition Wolfgang Rankl and Wolfgang Effing

As often happens with international standards, ISO/IEC 7816-1 provides a range of options that in many cases is too large for practical use. This has allowed industry standards to become established in addition to the ISO/IEC standard, such as the EMV standard in the payment systems sector and TS 102 221 in the telecommunication sector. These two industry standards do not compete with ISO/IEC 7816-3, but instead complement it with useful restrictions arising from practical experience with smart card applications involving millions of issued cards.

The distinction between smart cards used in payment systems and smart cards used in telecommunication systems came about because certain requirements proved to have fundamentally different natures in these two application areas. For example, in the payment systems sector the current consumption and voltage range are noncritical because the terminals used in these applications are connected to the public power grid. The situation in the telecommunication sector is entirely different, since every milliwatt counts when the objective is to achieve the longest possible operating time with battery-powered mobile equipment. Consequently, the requirements for the least possible current consumption and low supply voltage are highly important in this application area.

Table 4.1 on the facing page provides a summary of the most important electrical requirements of the essential international standards and industry standards. More detailed information is provided in the following sections.

4.1 ELECTRICAL CONNECTIONS

Smart cards have six or eight contacts on the front, which form the electrical interface between the terminal and the microcontroller in the card. All electrical signals pass via these contacts. ISO/IEC 7816-2 specifies that two of the eight contacts (C4 and C8) are reserved for the auxiliary functions AUX1 and AUX2. These contacts can be used for purposes such as a USB interface[1] or for connecting an antenna for contactless data transmission. Some smart card modules have only six contacts because this yields slightly lower production costs than modules with eight contacts. However, they have the same functionality as modules with eight contacts.

The contacts are numbered sequentially from top left to bottom right. Figure 4.2 on page 64 shows the ISO designations and electrical assignments of the eight defined contacts, and Table 4.2 on page 65 describes the functions of the contacts.

Until the late 1980s, an external voltage source was necessary for programming (writing) and erasing the EEPROM because the microcontrollers used at that time did not have onboard charge pumps. Contact C6 was reserved for this purpose. However, since the early 1990s it has been standard practice to generate this voltage directly on the chip using a charge pump, so this contact no longer has a dedicated use. However, it is used now in the telecommunication sector for the Single Wire Protocol (SWP) interface for communication with an NCF component in the mobile telephone.[2]

4.2 SUPPLY VOLTAGE

Smart cards originally operated with a supply voltage of 5 V with a maximum tolerance of $\pm 10\,\%$. This voltage, which is the same as the supply voltage of conventional TTL circuits, was the standard value for all commercially available smart cards and all applications.

[1] See also Section 9.4, ‘USB Transmission Protocol’, on page 272
[2] See also Section 9.6, ‘Single-Wire Protocol’, on page 278

Table 4.1 Overview of three electrical parameters (voltage, current and clock frequency) specified by the most important international standards for smart cards. The tolerances for the maximum current are stated in the relevant standards

Standard and type	Voltage	Clock frequency	Maximum current
ISO/IEC 7816-3			
Class A	5 V (±10 %) ⇒ 4.5 – 5.5 V	1 – 5 MHz	60 mA at 5 MHz
Class B	3 V (±10 %) ⇒ 2.7 – 3.3 V	1 – 5 MHz	50 mA at 4 MHz
Class C	1.8 V (±10 %) ⇒ 1.62 – 1.98 V	1 – 5 MHz	30 mA at 4 MHz
Class A, B, and C with clock stopped			0.5 mA (clock stop)
EMV	5 V (±10 %) ⇒ 4.5 – 5.5 V	1 – 5 MHz	50 mA over the entire clock frequency range
TS 102 221			
Class A, from reset to application selection	5 V (±10 %) ⇒ 4.5 – 5.5 V	1 – 5 MHz	10 mA at 5 MHz (operating state) 200 µA at 1 MHz (idle state)
Class A, during an application-specific session			60 mA at 5 MHz
Class B, from reset to application selection	3 V (±10 %) ⇒ 2.7 – 3.3 V	1 – 5 MHz	7.5 mA at 5 MHz (operating state) 6 mA at 4 MHz (operating state) 200 µA at 1 MHz (idle state)
Class B, during an application-specific session			50 mA at 5 MHz
Class C, from reset to application selection	1.8 V (±10 %) ⇒ 1.62 – 1.98 V	1 – 5 MHz	5 mA at 5 MHz (operating state) 4 mA at 4 MHz (operating state) 200 µA at 1 MHz (idle state)
Class C, during an application-specific session			30 mA at 5 MHz

As with other semiconductor devices, increasingly smaller structure widths and the need for reduced current consumption have made it necessary to markedly reduce operating voltages. This tendency has been further strengthened by the mobile telecommunication sector. The market-driven demand for reducing the weight of mobile telephones required changing from 6-V batteries to 3-V batteries, and as all other components used in mobile telephones were available in 3-V technology, for a while the smart card was the only component in a mobile telephone that still needed 5 V. This meant that an extra voltage converter (with associate extra cost) was necessary to provide electrical power to the smart card.

Consequently, the international standard was revised to allow a voltage range of 3 V ±10 % for smart cards in addition to the 5 V range. This effectively yielded a range of 2.7 to 5.5 V. However, it quickly became apparent that this extension was not sufficient, so the revised