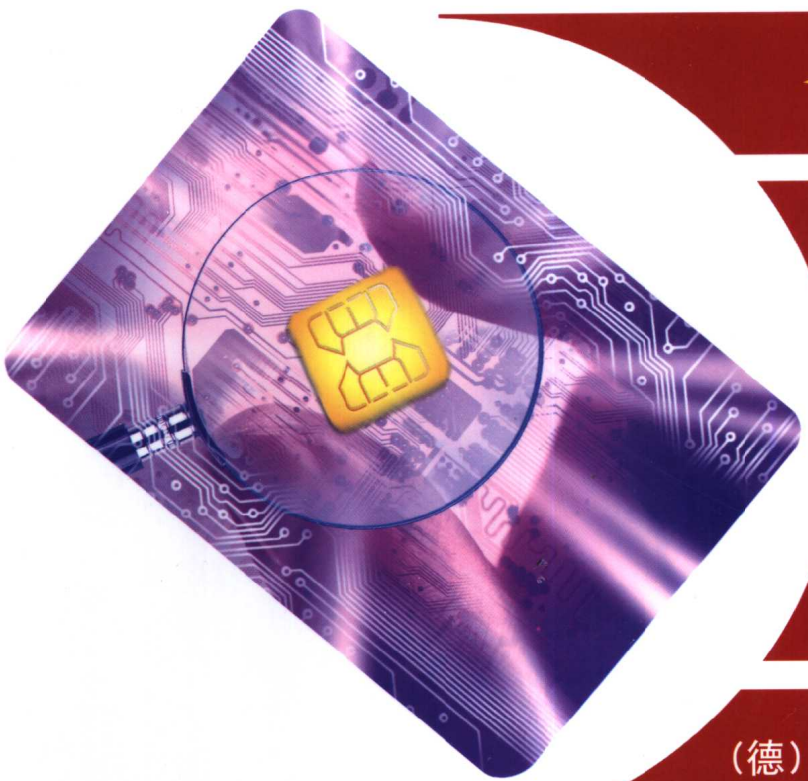
Handbuch der Chipkarten 3.Auflage

智能卡大全

—— 智能卡的结构·功能·应用

（第3版）



王卓人 王 锋 编译

（德）Wolfgang Rankl
Wolfgang Effing 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

智能卡大全

——智能卡的结构·功能·应用

(第3版)

Handbuch der Chipkarten 3. Auflage

(德) Wolfgang Rankl
Wolfgang Effing 编著

王卓人 王 锋 编译

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书以智能卡及其芯片的物理与电气性能，生产工艺流程，智能卡数据信息的传输及加密算法，操作系统的设计及举例，质量保证与安全技术，卡终端及应用范例等内容，详尽地介绍了智能卡结构、功能、设计与应用。书末附有大量有关卡的资料及查询方法，是一部融卡的开发、应用技术及解决方案的大全性书籍。

本书内容实践性强，适合有关大专院校、研究所以及智能卡高级培训班选作教材或供开发设计人员参考。

版权贸易合同登记号：图字 01-2001-3779

图书在版编目(CIP)数据

智能卡大全——智能卡的结构·功能·应用(第 3 版)/(德)兰柯(Rankl, W.),(德)埃芬(Effing, W.)编著；王卓人等编译. —北京：电子工业出版社，2002.12

书名原文：Handbuch der Chipkarten 3. Auflage

ISBN 7-5053-8301-9

Ⅰ. 智… Ⅱ. ①兰…②埃…③王… Ⅲ. 智能卡 Ⅳ. F830.46

中国版本图书馆 CIP 数据核字(2002)第 098489 号

责任编辑：王惠民

印　　刷：北京兴华印刷厂

出版发行：电子工业出版社　http://www.phei.com.cn

北京市海淀区万寿路 173 信箱　邮编 100036

经　　销：各地新华书店

开　　本：787 × 1 092　1/16　印张：36.25　字数：860 千字

版　　次：2002 年 12 月第 1 版　2002 年 12 月第 1 次印刷

印　　数：6 000 册　定价：55.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。

联系电话：(010)68279077

序　言

这篇序言在编写上没有采用传统的写法。

本书是对称之为智能卡新技术的进展(达到当前最新技术发展水平)的汇编,特别着重于含有微处理器的智能卡。

这种新型集成电路卡的作用和影响将远远超出任何目前已知的、策划中的、甚至于设想的任务和应用,它将会影响我们日常的生活和行为。

无论如何,智能卡在任何意义上都不应成为一种被迫使用的工具,它应当以其全部潜在的能力来为社会服务。

如果我们保持警觉,智能卡就不会被欺诈团伙所利用。相反,它们能鼓舞我们的奋发精神。比起我们目前把智能卡看作金融交易、授权和认证等媒介的观念(不论这些功能在经济上对未来有多么重要)来说,智能卡最引人入胜之处,更多地是在于它未来的社会角色。

于是,你会问:"智能卡——路在何方?"

目前,在构思完善的对智能卡的潜能宣传广告蛊惑之下,有可能引导人们害怕因用卡而失掉他们的自主权和隐私权——或者至少有所顾忌。

为此,作者在叙述应用的章节里仅限于实例,不触及任何人对智能卡全部潜在应用的最浪漫的联想。

在 1978 年,法国计算机公司 Honeywell Bull SA 的专利部经理告诉我:"有一天,智能卡实业将会像今天的计算机产业一样重要。"现在,我们已经可以看到他是多么正确了。

新科技或它的工艺技术的发展,总是受到来自有着广泛不同利益的、很多感兴趣的人们所采取的步骤来推动。他们包括:基础应用科学研究者、工程师、企业家、"决策者"、以及许多别的人们。

是什么原因激发了这些人呢?

要找出基本动力,"好奇心"当然是动机之一:"智能卡能做到这一切吗?" ——更多地来自实验室,绘图板和计算机——这里有着对名誉的期望以及对金钱和权力的渴求,而且它们又常常交织在一起作用着。

然而,"进步" 作为自然生命的一部分以连续的形式发展,我们也可以把它称之为"进化"——生命中的不断探索。我们总是期待或许可以证明下一个试验不是错误的,如果我们不是被我们的好奇心所驱动,我们该怎样来玩这场游戏呢?

考虑到事物的复杂性和非凡的新颖,"进步"所引起的不断变化的相互依赖,很容易看到对给定技术的估价结果是如何陷入纯粹投机的泥潭,用这样的评估去寻求一个未知的将来,我们可以有理由试问一下这是否是一项十分困难的任务。

我不相信我们会过高地估计了智能卡在未来的重要性,而且相信我们大概仍未能充分预见到它在未来的重要性。这是一项浩大的工程,和 PC 比起来,它甚至是一个更重要的隐秘性技术。

智能卡发展成一门新技术是它本身的潜能所决定的,我们应当问我们自己是否正在打开

了一只潘多拉的盒子?[①]看它可能贮藏些什么——它会不会是一把双刃剑,把个人的隐私暴露在多方面的监督和控制之下?

"文件卡是恐怖行为的最狡诈的工具"。

——E.V.Salomon

智能卡和计算机系统与数据库网络相结合,就能对文件卡[②]的现在和未来做出贡献。如果它成为了某些机构的工具的话,但愿它不会成为用隐私来控制某个人的手段。

目前,我们正处在一个重要的阶段,工程师、企业家和政治家正面临着这种脱颖而出的新技术。于是在此,我用充满智慧的拉丁语格言来提醒年轻的读者们:et respice finem("瞻前顾后,因必有果")。

智能卡在软件的帮助下能形成可以预想的各种不同的系统。从某种意义上来说,如果它密切地和其独有的处理器相配合,就能创建出无穷的潜力。

让我们选择正确的道路,独立之路!让我们在自主精神的光辉大道上前进(仍有路障要突破……)。

不应当以冷漠的态度来阅读此书,而要以怀疑的乐观主义来使用它,让我们证明自己既不是无能之辈,也不是不具有自主精神的人。

对于一本技术文献来说,这的确是一个不寻常的序言,我满怀喜悦来写它,因为我坚信它是一本重要的书,它包含的信息既准确又重要。

· 准确。因为它的作者们是非常精干的一群人中的成员,是智能卡技术发展的先驱者中的核心,他们熟知这门新技术最深层的奥秘,我们可以通过本书来共享它们。若是在古代,他们可能被认为是大祭司般的人物。

· 重要。因为它有效地向我们提供了创建新组合和新构造的建筑模块。

我希望本书在奠定其作为智能卡这一学科的标准著作方面获得成功。它适合作为:

· 初学者的教科书;

· 好奇的外行人士的百科全书;

· 专业人员的参考书;

· 发明者关于最新技术现状的说明书;

· 探索创建新系统和应用的基础。

这本书获得如此的成功——只要瞥视目录和索引就知道了它所包含的信息量。

感谢已故的 Halmut Grottrup 先生,[③]在我的人生旅程上他伴随我迈出最初的几步,我相信他对此序言也会满意的。

我们仅向作者和出版者,致以深深的感谢之情。

Jurgen Dethloff

1999 年春

---

① Pandora's lox:希腊神话中主神宙斯为报复普罗米修斯把火种盗给人类,于是命火神用粘土造成地球上的第一个女人——潘多拉。宙斯让她保管一只盒子,里面装的苍蝇、蚊子、疾病、疯狂、灾害、罪恶等等。潘多拉私自打开了它,于是人间就充满了这些祸害,而只把希望留在了盒中。潘多拉盒子被用来比喻为灾祸之源——译者注

② 存储有关个人资料的智能卡——译者注

③ 德国人认为序言作者和 Halmut Grottrup 是两位发明家,他们提出了把集成电路结合到识别卡中的概念,他们是倍受尊重的智能卡技术的先驱者——译者注

第三版前言

本书同第二版相比它已经显著地扩充了，在许多方面做了更新以反映技术的现状。

正像前面的版本一样，按照“宁全勿略、细大无遗”的精神，我们在描述和解释这项日新月异的技术时力求全面细致，书中列举了很多的例子、大量说明性的图表和照片，它们是用以帮助读者去理解智能卡越来越复杂的各种技术的最好工具。这一版的一个特点是分层次的列表，便于用来增强对系统状况的掌握和理解。这些增加、扩充和改进导致本书比 1995 年第一版的内容增多了将近三倍。

在 20 世纪 90 年代之初，智能卡工作者有时还需要向新用户和人们详细解释智能卡是什么？现在，这个概念已经扩展到专家的范围以外了，几乎每一个人都知道它是什么。这个小小的、彩色的、带有半导体芯片的塑料卡片已经从它的故乡——法国和德国扩散到了整个世界。在近期，没有任何技术可以和它的胜利进军相匹敌，特别是考虑到这项技术仍处在发展的初级阶段，在我们的视野之内远没有看到停滞和终结的迹象。

当智能卡技术正在飞速前进之际，自然不能以同样的速率来更新《智能卡大全》。本书代表的是 90 年代末的技术和知识状态。如果现在对某些问题出现了不同的见解，我们只能表示因为在编写此书时，没有人能知道未来是怎样的。有鉴于此，我们欢迎读者对每一项评注、建议提出改进，以便使本书尽可能完整地覆盖智能卡这一主题。作为弥补，在 John Wiley & Son [Wiley]的网络服务器上有一个补充文档，以及本书必需的最低限度的附录。

Wolfgang Rankl
[Rankl@gmx.net],[Rankl]
Wolfgang Effing
[Effing-Wolfgang@compuserv.com]
慕尼黑，1999 年 2 月

译 者 的 话

这本书堪称巨著，它的两位作者是智能卡技术领域的权威。书中的内容以智能卡的发源地——欧洲的广泛应用为背景，详尽而充实，覆盖了卡的生命周期的全过程。

本书德文原版书到1999年已出版了第三版。目前，第四版的编辑出版工作正在进行着。由此可见该书受欢迎的程度，以及它的实用价值。我国有关智能卡的应用正处于起步阶段，不论是在应用的广泛性与普及性和发达国家相比都还有较大的差距，估计国内在短期内还难以写出深度和广度可与此书相当的出版物来。因此，译者不揣冒昧，在电子工业出版社广州公司的大力支持之下，译出此书的第三版贡献给读者，但愿它对学习和工作在此领域内的朋友们有所裨益。

为了符合我国大多数读者的情况，译者参考有关资料把书中程序清单、术语表里的德文诠释为英文，一些缩略语也加注了英文，以求尽量方便读者。

王锋翻译了操作系统一章，该章是本书重点之一；邓晋钧参加了第二，三章的翻译工作；其余各章均由王卓人译出，并承担了全书的统稿和审校工作。由于工作量大，内容新颖而广泛，译者才疏学浅，错漏之处，欢迎读者指正。

译 者

2002.9.于广州

目　录

符号和记号

- 有关智能卡的命令都用大写英文字母表示，必要时附以中文注解，例如 SELECT FILE(选择文件)。
- 按照 ISO 标准，最低有效位均指派为第“1”位，而不是第“0”位。
- 为了和智能卡标准中的经常用法一致，对于数据、对象和所有可计数的量的长度均以十进制数表示。所有其他量都表示为十六进制的数，可按此识别。
- 像在信息技术中的惯例那样，前缀“kilo”和“*mega*”相应之值为：1 024($=2^{10}$)和 1 048 576($=2^{20}$)。

符号和数的表示

“ABC”	ASCII 之值
‘00’	十六进制之值
°0°,°1°	二进制之值
42	十进制之值
Bn	字节数 n(例如：B1)
bn	位(bit)数 n(例如：b2)
Dn	数位(Digit)数 n(例如：D3)

逻辑函数

$\|\|$	链接(数据元或对象)
$\oplus$	逻辑异或(XOR)操作
$\wedge$	逻辑与(AND)操作
$\vee$	逻辑或(OR)操作
$a \in M$	a 是集合 M 的元素
$a \notin M$	a 不是集合 M 的元素
{a,b,c}	元素 a,b,c 的集合

密码函数

$enc_{X_n}(K;D)$	用算法 X 和一个 n 位密钥 K 加密数据 D，例如：$enc_{DES\ 56}$(‘1…0’;42)
$dec_{X_n}(K;D)$	用算法 X 和一个 n 位密钥 K 解密数据 D，例如：$dec_{IDEA\ 128}$(‘1…0’;42)
$S := sign_{X_n}(K;D)$	用算法 X 和一个 n 位密钥对于密钥 K 和数据 D 产生签名 S， 例如：$sign_{RSA\ 512}$(‘1…0’;“Wolf”)
$verify_{X_n}(K;S)$	用算法 X 和一个位密钥对于密钥 K 验证签名 S，例如：$verify_{RSA\ 512}$(‘1…9’;42)

参考资料

See:‘…’	这是对本书另一处的内容的参照
[…]	这是对本书附录中所列万维网(WWW)站的引用
[XY]	这是对本书附录中所列文献或标准的参照，其格式为：X∈{第一作者的姓} 和 Y∈{出版年代的最后两位数字}

程序编码约定

本书中程序编码所用的语法和语义都是基于标准的 BASIC 语言的。为了帮助读者理解，允许在程序清单

中使用自然语言予以说明,虽然这样使程序易于读懂,但也意味着它不可能自动被转换成机器语言。由此所提供的明显改进了的可读性,证明这种折中的正确性。

:=	赋值操作符
=,>,<,<>,≤,≥	比较操作符
+,-,*,/	算术运算操作符
NOT	逻辑非
AND	逻辑与
OR	逻辑或
‖	链接操作符
-	多行命令的行结束符
//…	注解

IO-Buffer	变量(用斜体字印出)
Label:	跳转或调用存储单元(用黑体字印出)
GOTO…	跳转
CALL…	函数调用(调用子程序)
RETURN	从一个函数(子程序)中返回

IF…THEN…	1 型判定
IF…THEN…ELSE…	2 型判定

SEARCH(…)	在一个表中搜索:搜索的字符串在括号中
LENGTH(…)	计算长度
EXIST	存在测试(例如:一个对象或数据元)

WITH…	作为引用,开始定义一个变量或对象
END WITH	作为引用,结束对一个变量或对象的定义

缩写(只取首字母)

3DES	三重 DES(见术语表)
A3,A5,A8	GSM 算法 3,5,8
ABA	美国银行家协会
ABS	丙烯腈-丁二烯-苯乙烯(ABS 塑料)
ACK	确认
ACD	访问控制描述符
ADN	缩写的标号数
AFNOR	法国标准化组织协会(见术语表)
AGE	高速公路收费
AGE	自动收费
AID	应用标识符(见术语表)

Amd.	改正
AND	逻辑与操作
ANSI	美国国家标准化组织(见术语表)
APACS	支付清算服务协会
APDU	应用协议数据单元(见术语表)
A – PET	非定形聚苯乙烯对苯二酸酯
API	应用编程接口(见术语表)
ARM	先进 RISC 计算机
ASC	应用专用命令
ASCII	美国信息交换标准码
ASIC	特定用途集成电路(专用集成电路)
ASK	振幅键控
ASN.1	抽象语法记号 1(见术语表)
ATM	异步传输模式
ATM	自动柜员机
ATR	复位应答(见术语表)
BASIC	初学者通用符号指令码
BCD	二进制编码的十进制数字
Bellcore	贝尔通信试验室
BER	基本编码规则
BER – TLV	基本编码规则 – 标记,长度,值
BEZ	Geldkarte 电子钱包清算中心
BGT	字组保护时间
BIN	银行识别号
bit	位,比特
BS	基站
BWT	字组等待时间
CA	认证管理机构
CAD	芯片接受设备
CAFE	有条件的访问 Europe(EU 项目)
CAP	卡的应用
C – APDU	命令 APDU(见术语表)
CAPI	加密 – API(应用编程接口)
CASCADE	智能卡和便携式智能设备的芯片架构
CASE	计算机辅助软件工程
CBC	加密字组链接
CC	通用准则
CCD	卡耦合设备
CCD	电荷耦合器件
CCITT	国际电话与电报顾问委员会(现为 ITU)(见术语表)

CCR	IC卡阅读器
CCS	密码校验和(见术语表)
CD	委员会草案
CDM	卡发行设备
CEN	欧洲标准化委员会(见术语表)
CENELEC	欧洲电子技术标准化委员会
CEPT	欧洲邮政和远程通信会议(见术语表)
CFB	密码反馈
CHV	持卡人认证
CICC	非接触集成电路卡
CISC	复杂指令集计算机
CLA	类
CLK	时钟
CMOS	互补金属氧化物半导体
COS	智能卡操作系统(见术语表)
CRC	循环冗余校验法(见术语表)
CRCF	时钟速率变换因子
CRT	中国冗余定理
Cryptoki	加密权标接口
C - SET	芯片 - SET(安全电子交易)
CT	卡终端
CVM	持卡人认证方法
CWT	字符等待时间
DAD	目标地址
DAM	修正草案
DB	数据库
DBF	数据库文件
DCS	数字蜂窝系统
DEA	数据加密算法
DECT	数字化增强无绳远程通信(先前为:数字化欧洲无绳远程通信)
DES	数据加密标准
DER	特异的编码规则
DF	专用文件(还经常是:目录文件)(见术语表)
DFA	差分故障分析(见术语表)
DFÜ	长距离数据通信
DIL	双列直插
DIN	德国工业标准
DIS	国际标准草案
DO	数据对象
DoD	美国国防部
DOV	数据上的语音