

智

能卡开发技术系列

智能卡

研发技术与工程实践

求是科技

李翔 编著



人民邮电出版社
POSTS & TELECOM PRESS



智能卡开发技术系列

智能卡

研发技术与工程实践

求是科技

李翔 编著

人民邮电出版社

图书在版编目 (CIP) 数据

智能卡研发技术与工程实践 / 求是科技编. —北京: 人民邮电出版社, 2003.11
ISBN 7-115-11723-3

I. 智… II. 求… III. 智能卡 IV. F830.46

中国版本图书馆 CIP 数据核字 (2003) 第 090400 号

内容提要

本书详细介绍了在常见的 IC 卡芯片平台上开发卡内操作系统 (COS) 的方法和技巧, 力图通过生动的讲解和典型的应用实例让读者进一步学习掌握并提高这一技术。本书共分 13 章, 主要包括了 COS 开发的基本概念、COS 系统的模块划分、卡片的通信协议、COS 文件系统、COS 的安全体系、COS 的多应用涉及和主要的工作流程等。

同时, 本书还详细介绍了 COS 在金融、社会保障、石化加油和公钥体系等多个领域应用的设计实例, 包括这些应用的主要特点和基本要求、应用对外的命令接口格式以及命令的主要实现流程等。

本书中 COS 主要工作流程设计以及大量的命令接口格式、安全算法实现等可供广大系统设计和开发人员阅读参考。本书专业性和实用性较强, 对于在传统平台上进行 COS 开发具有较高的参考价值。本书适合中高级程序员、软件开发人员和系统分析人员阅读和参考。

智能卡开发技术系列

智能卡研发技术与工程实践

-
- ◆ 编 著 求是科技 李 翔
责任编辑 张立科
 - ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
读者热线 010-67132692
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销
 - ◆ 开本: 787×1092 1/16
印张: 28.5
字数: 688 千字 2003 年 11 月第 1 版
印数: 1-5 000 册 2003 年 11 月北京第 1 次印刷
ISBN7-115-11723-3/TP·3644
-

定价: 39.00 元

本书如有印装质量问题, 请与本社联系 电话: (010) 67129223

前言

随着芯片技术的发展和应用安全性要求的提高, IC 卡作为一种新兴的应用平台, 在诸多领域中有着十分广泛的应用, 如金融、社保、市政、加油等。在 IC 卡系统中, 卡片内的操作系统 COS 是整个系统的核心, 它的设计与开发既要遵循一定的规范, 又存在很大的灵活性。

编写本书的目的就是将笔者多年来设计和开发 COS 的相关经验加以总结归纳, 本着将理论知识和应用相结合的思路, 系统详尽地介绍 COS 系统设计和开发过程中常见的问题, 并且给出解决方案的实例, 希望本书能够给广大的 IC 卡设计开发人员以参考。

本书共分 13 章, 下面简单概述各章的内容。

第 1 章: 初始 IC 卡

本章首先介绍了 IC 卡发展的历史及其在国内外的应用现状, 然后重点介绍了 IC 卡的主要应用领域及其应用特点, 最后引入了 IC 卡系统中最重要的一部分——卡内操作系统 (COS), 详细介绍了 COS 的主要功能和发展现状。熟悉和掌握这些内容有助于从整体上了解和把握 IC 卡的特点和应用要求。

第 2 章: COS 开发的预备知识

本章重点分析了 COS 系统的需求, 并且对 COS 系统的结构进行了初步设计。首先介绍了如何进行 COS 的需求分析, 包括了应用、环境、存储、安全等多个方面; 然后介绍了进行 COS 系统开发前需要掌握的相关知识; 接着简单给出了 COS 开发的通用流程; 最后按照功能将 COS 系统划分为 4 个层次和 4 个主要功能模块。通过本章的学习, 读者将能够对 COS 功能及其开发有一个总体的了解。

第 3 章: IC 卡芯片

本章首先详细介绍了 IC 卡芯片的种类和逻辑结构, 主要包括了 8 个逻辑模块; 然后根据这些逻辑模块逐一介绍了在不同的应用需求下模块的功能要求及芯片的选型原则; 最后以 ST 公司的系列芯片为例介绍了 3 类面向不同应用需求的芯片性能。

第 4 章: IC 卡的传输协议

COS 的 I/O 模块是最基础的模块之一, 该模块的功能要求遵循传输协议的定义。本章首先介绍了 IC 卡的操作过程, 包括正常流程和异常中断的处理; 然后介绍了一个字符的物理传送过程, 这是 IC 卡数据通信的基础; 接下来介绍了 IC 卡的上电复位应答; 最后给出了通用的 IC 卡传输协议, 包括 T=0 和 T=1 两种类型, 可以划分为物理层、数据链路层、终端传输层和应用层等。

第 5 章: IC 卡的文件系统

本章首先介绍了 IC 卡内文件系统的组织形式, 包括文件系统的逻辑结构和对文件系统的操作; 然后介绍了卡内存在的 3 种文件类型, 并且给出了在实际应用中可能碰到的文件系统

逻辑结构示例；接下来设计了一个简单的文件系统在卡内的存储机构，包括文件头和文件体两个部分；最后根据文件操作的需要，设计了 7 条文件操作命令。

第 6 章：IC 卡的安全体系

IC 卡的安全体系是 COS 系统的核心模块。本章首先介绍了 IC 卡的安全结构，包括安全属性、安全机制和安全状态 3 个部分；然后分别介绍了在卡内安全模块中可能涉及的几个安全算法，包括算法原理和部分算法实现代码；接下来给出了一个卡片安全结构设计的示例，建立了一个简单的卡片安全环境；最后根据安全操作，设计了 8 条相关命令。

第 7 章：多应用 IC 卡的实现

本章首先介绍了 IC 卡的生命周期，包括 IC 卡的使用流程和卡片的生命周期状态；然后介绍了 IC 卡的应用模式，在不同的应用模式情况下，IC 卡系统中不同的角色定义和角色之间的关系转换；接下来介绍了在多应用环境下卡片状态的维护，并且给出了一个多应用 IC 卡设计的示例，包括卡片生命周期的维护、应用之间的保护机制和安全状态的维护机制等；最后根据应用维护操作的不同，设计了 5 条相关命令。

第 8 章：COS 的工作流程

本章以实例的形式重点介绍了 COS 在实际运行过程中涉及到的 4 个主要流程的工作原理，这 4 个流程分别是主守护流程、数据 IO 流程、命令处理流程和数据安全写流程。通过对这几个流程分析，读者能够基本掌握 COS 的整体结构和运行情况。

第 9 章：中国金融集成电路卡应用

本章重点介绍了 IC 卡应用领域的一个最重要的应用，也就是金融卡应用。首先介绍了金融卡应用的基本情况，给出了应用的文件系统设计；然后介绍了金融卡应用规范定义的 13 条命令接口、卡片在使用过程中应用状态的维护情况和卡片的安全结构设计要求；接下来给出了卡片在实际使用过程中的 10 个主要交易流程；最后根据交易流程简单介绍了卡片命令在这些交易流程中的组合使用情况。

第 10 章：社会保障卡应用

本章重点介绍了 IC 卡应用领域的另一个最重要的应用，也就是社会保障卡应用。首先介绍了社会保障卡应用的基本情况，给出了应用的文件系统设计；然后介绍了社会保障卡中医疗保险应用规范定义的 8 条命令接口、和卡片的安全结构设计要求；接下来给出了卡片在实际使用过程中的 10 个主要交易流程；最后根据交易流程简单介绍了卡片命令在这些交易流程中的组合使用情况。

第 11 章：中国石化加油集成电路卡应用

本章重点介绍了中国石化加油集成电路卡应用。首先介绍了加油卡应用的基本情况，给出了应用的文件系统设计；然后介绍了加油卡应用规范定义的 18 条命令接口、卡片在使用过程中应用状态的维护情况和卡片的安全结构设计要求；接下来给出了卡片在实际使用过程中的 13 个主要交易流程；最后根据交易流程简单介绍了卡片命令在这些交易流程中的组合使用情况。

第 12 章：支持公钥应用的公钥卡

本章介绍了目前最为流行的一个 IC 卡应用，也就是公钥卡应用。首先介绍了公钥（PKI）体系的基本情况，包括 PKI 体系的结构、工作流程及安全分析；然后介绍了 PKI 相关的主要算法原理，包括加密算法和签名算法两大类；接下来根据 IC 卡的实际情况对 PKI 算法在卡内的实现进行了选择，简单设计了一个 PKI 卡的文件结构和 PKI 主要流程在卡内的实现流程；最后设计了 PKI 相关的 9 条命令。

第 13 章：智能卡应用解决方案示例

本章主要介绍了智能卡应用的整体解决方案，包括这些解决方案设计的应用领域的基本情况介绍、相关系统的结构设计、卡片在该系统中的主要功能、以及系统相关软硬件的配置要求等，这些系统包括了校园一卡通应用、社会保障卡应用和网吧监管系统应用，通过这些应用方案，读者能够对 IC 卡的实际应用有一个整体的把握。

附录部分主要提供了在本书中涉及的专用命令及其缩写，以便读者查阅。

由于作者水平有限，书中难免有不足和疏忽之处，恳请读者朋友和各位同仁批评指正。读者通过访问求是科技的网站 <http://www.cs-book.com>，可以下载到本书所涉及的代码。并欢迎对本书的问题和不足提出您最宝贵的建议和意见，同时，在“求是论坛”上还可以进行智能卡的相关技术交流。

编者

2003 年 10 月 于清华园

目 录

第 1 章 初识 IC 卡	1
1.1 IC 卡的发展与现状	1
1.1.1 IC 卡的发展历史	1
1.1.2 IC 卡在国内外的应用情况	2
1.1.3 IC 卡在国内的广泛应用	3
1.2 IC 卡的应用特点	4
1.2.1 IC 卡应用系统	4
1.2.2 IC 卡的应用优势	5
1.2.3 IC 卡支持的典型应用	6
1.3 卡内操作系统 COS	7
1.3.1 COS 的主要功能	7
1.3.2 COS 的发展与现状	8
第 2 章 COS 开发的预备知识	9
2.1 COS 的需求分析	9
2.1.1 卡片所支持的应用	9
2.1.2 卡片的使用环境	10
2.1.3 “应用”在卡内的存在方式	10
2.1.4 数据存储的特殊要求	11
2.1.5 安全要求	12
2.1.6 开发与发行	12
2.2 相关知识的准备	13
2.2.1 与 IC 卡相关的规范	13
2.2.2 与应用相关的规范	14
2.2.3 相关的加密算法	16
2.2.4 COS 开发商提供的相似范例	17
2.3 COS 的开发过程	18
2.3.1 准备环境	18
2.3.2 设计系统	19
2.3.3 编程实现	20
2.3.4 测试	20
2.3.5 检测	20
2.3.6 掩模发行	21
2.4 COS 的基本结构	21
2.4.1 总体结构	21
2.4.2 基本系统服务	21

2.4.3	高级系统服务	22
2.4.4	系统调度	23
2.4.5	应用服务接口	23
2.4.6	模块划分	24
第3章	IC卡芯片	25
3.1	IC卡芯片结构	25
3.1.1	IC卡芯片的种类	25
3.1.2	IC卡芯片的逻辑结构	26
3.2	芯片的性能指标及其选择	29
3.2.1	处理器	29
3.2.2	存储空间	29
3.2.3	加密协处理器	30
3.2.4	硬件安全保护	30
3.2.5	其他机制	30
3.3	典型芯片浏览	31
3.3.1	ST16系列芯片	31
3.3.2	ST19系列芯片	32
3.3.3	ST22系列芯片	33
第4章	IC卡的传输协议	36
4.1	IC卡的操作过程	36
4.1.1	正常操作流程	36
4.1.2	异常中断	39
4.2	字符的物理传送	39
4.2.1	位持续时间	39
4.2.2	字符帧	40
4.3	复位应答	41
4.3.1	回送的物理传输	41
4.3.2	回送字符	41
4.3.3	字符定义	42
4.3.4	应答次序和一致性	46
4.3.5	终端流程	46
4.4	传输协议	47
4.4.1	概述	47
4.4.2	物理层	48
4.4.3	数据链路层	48
4.4.4	终端传输层	56
4.4.5	应用层	59
第5章	IC卡的文件系统	61
5.1	文件系统的组织形式	61

5.1.1	文件系统的逻辑结构	61
5.1.2	对文件系统的操作	62
5.2	卡内文件的类型	63
5.2.1	主文件——MF	63
5.2.2	专用文件——DF	63
5.2.3	基本数据文件 EF	65
5.2.4	文件系统逻辑结构示例	69
5.3	文件在卡内的存储结构	70
5.3.1	卡内文件的存储	70
5.3.2	文件描述块的内容定义	72
5.3.3	文件描述块的设计示例	72
5.3.4	不同数据类型 EF 文件体设计示例	77
5.3.5	不同用途类型 EF 文件体设计示例	78
5.4	操作卡片文件的相关命令	82
5.4.1	创建文件 (CREATE FILE) 命令	82
5.4.2	删除文件 (DELETE FILE) 命令	85
5.4.3	选择文件 (SELECT) 命令	88
5.4.4	读二进制 (READ BINARY) 命令	91
5.4.5	写二进制 (UPDATE BINARY) 命令	93
5.4.6	读记录 (READ RECORD) 命令	95
5.4.7	写记录 (UPDATE RECORD) 命令	97
第 6 章	IC 卡的安全体系	100
6.1	卡片安全结构	100
6.1.1	卡片安全状态	100
6.1.2	卡片安全属性	101
6.1.3	卡片安全机制	102
6.2	安全相关的主要算法	104
6.2.1	单向散列算法 (HASH)	104
6.2.2	对称数据加解密算法	125
6.2.3	RSA 算法	139
6.2.4	安全报文计算算法	141
6.3	安全结构设计示例	142
6.3.1	卡片安全环境	142
6.3.2	安全状态的维护	144
6.3.3	安全机制的选择	144
6.3.4	安全属性的实现	145
6.4	安全操作相关的基本命令	146
6.4.1	取随机数 (GET CHALLENGE) 命令	146
6.4.2	内部认证 (INTERNAL AUTHENTICATION) 命令	148

6.4.3	外部认证 (EXTERNAL AUTHENTICATION) 命令	150
6.4.4	添加密码 (APPEND PIN) 命令	152
6.4.5	修改密码 (CHANGE PIN) 命令	154
6.4.6	验证密码 (VERIFY) 命令	156
6.4.7	密码解锁 (PIN UNBLOCK) 命令	158
6.4.8	写密钥 (WRITE KEY) 命令	159
6.4.9	其他相关命令	162
第 7 章	多应用 IC 卡的实现	163
7.1	IC 卡的生命周期	163
7.1.1	IC 卡的使用流程	163
7.1.2	IC 卡的生命周期状态图	166
7.2	应用模式	167
7.2.1	卡应用中的角色定义	167
7.2.2	卡应用中的角色关系	168
7.2.3	卡应用的不同模式	168
7.3	多应用环境下的卡片状态维护	169
7.3.1	多应用状态下的应用状态	169
7.3.2	支持多应用的 COS 设计	171
7.4	卡片和应用生命周期维护相关命令	172
7.4.1	应用锁定 (APPLICATION BLOCK) 命令	172
7.4.2	应用解锁 (APPLICATION UNBLOCK) 命令	175
7.4.3	卡片锁定 (CARD BLOCK) 命令	176
7.4.4	激活文件 (ACTIVE FILE) 命令	178
7.4.5	屏蔽文件 (DEACTIVATE FILE) 命令	181
第 8 章	COS 的工作流程	184
8.1	主守护流程	184
8.1.1	工作原理	184
8.1.2	设计示例	185
8.1.3	示例涉及的数据结构	187
8.2	数据 IO 流程	189
8.2.1	流程的工作原理	189
8.2.2	设计示例	190
8.2.3	示例涉及的数据结构	196
8.3	命令处理流程	197
8.3.1	工作原理	197
8.3.2	设计示例	197
8.3.3	示例涉及的数据结构	198
8.4	数据安全写流程	199
8.4.1	工作原理	199

8.4.2	设计示例	200
8.4.3	示例涉及的数据结构	201
第 9 章	中国金融集成电路 (IC) 卡应用	203
9.1	应用描述	203
9.1.1	应用及其实现要求	203
9.1.2	应用过程中包含的交易	203
9.2	应用文件的设计	204
9.2.1	DF 文件	204
9.2.2	数据 EF 文件	204
9.2.3	相关的数据描述	206
9.3	应用相关的命令集	208
9.3.1	修改密码 (CHANGE PIN) 命令	208
9.3.2	圈存 (CREDIT FOR LOAD) 命令	209
9.3.3	消费/取现 (DEBIT FOR PURCHASE/CASH WITHDRAW) 命令	210
9.3.4	圈提 (DEBIT FOR UNLOAD) 命令	211
9.3.5	读余额 (GET BALANCE) 命令	212
9.3.6	取交易认证 (GET TRANSACTION PROOF) 命令	213
9.3.7	取现初始化 (INITIALIZE FOR CASH WITHDRAW) 命令	214
9.3.8	圈存初始化 (INITIALIZE FOR LOAD) 命令	215
9.3.9	消费初始化 (INITIALIZE FOR PURCHASE) 命令	216
9.3.10	圈提初始化 (INITIALIZE FOR UNLOAD) 命令	217
9.3.11	修改初始化 (INITIALIZE FOR UPDATE) 命令	219
9.3.12	重装个人密码 (RELOAD PIN) 命令	220
9.3.13	修改透支限额 (UPDATE OVERDRAW LIMIT) 命令	221
9.4	卡片的状态维护	222
9.4.1	卡片的状态	222
9.4.2	卡片状态的变化	222
9.4.3	状态和命令之间的关系	222
9.5	安全结构设计	223
9.5.1	密钥管理原则	223
9.5.2	应用涉及的密钥	223
9.5.3	子密钥的计算方法	224
9.5.4	过程密钥的计算方法	224
9.6	交易流程	225
9.6.1	交易预处理	225
9.6.2	圈存交易	227
9.6.3	圈提交易	230
9.6.4	消费交易	232
9.6.5	取现交易	235

9.6.6	修改透支限额交易	237
9.6.7	查询余额交易	240
9.6.8	查询明细交易	240
9.6.9	应用维护功能	240
9.6.10	防拔	242
9.7	命令在交易过程中的使用示例	243
9.7.1	圈存交易	243
9.7.2	圈提交易	244
9.7.3	消费交易	245
9.7.4	取现交易	246
9.7.5	修改透支限额交易	247
9.7.6	查询余额交易	248
9.7.7	修改 PIN	249
9.7.8	重装 PIN	250
第 10 章	社会保障 (个人) 卡应用	251
10.1	应用描述	251
10.1.1	应用及其实现要求	251
10.1.2	应用过程中包含的交易	252
10.2	应用文件的设计	252
10.2.1	应用及其文件结构	252
10.2.2	基本应用数据区	254
10.2.3	公共应用数据区	258
10.2.4	就业与失业数据区	262
10.2.5	社会保险数据区	269
10.2.6	医疗保险数据区	273
10.2.7	生命与健康数据区	277
10.2.8	社会救助与优待抚恤数据区	279
10.2.9	应用对文件系统的扩展	283
10.2.10	相关的数据描述	284
10.3	医疗保险应用相关的命令集	285
10.3.1	账户划入 (CREDITFORLOAD) 命令	285
10.3.2	医疗消费 (DEBIT FOR PURCHASE) 命令	286
10.3.3	读取卡内余额 (GET BALANCE) 命令	287
10.3.4	取交易认证码 (GET TRANSACTION PROOF) 命令	288
10.3.5	账户划入初始化 (INITIALIZE FOR LOAD) 命令	289
10.3.6	医疗消费初始化 (INITIALIZE FOR PURCHASE) 命令	290
10.3.7	修改年度起始日期 (UPDATE STARTING DAY) 命令	292
10.3.8	取年度起始日期 (GET STARTING DAY) 命令	293
10.4	安全结构设计	294

10.4.1	密钥管理原则	294
10.4.2	应用涉及的密钥	294
10.5	交易与命令的实现流程	296
10.5.1	交易预处理	296
10.5.2	查询应用信息	298
10.5.3	操作员更新应用信息	300
10.5.4	持卡人联网更新应用信息	302
10.5.5	更改个人密码	303
10.5.6	初始化医疗保险支付	305
10.5.7	账户划入交易	306
10.5.8	医疗消费交易	309
10.5.9	应用维护功能	312
10.5.10	防拔	312
10.6	命令在交易过程中的使用示例	313
10.6.1	账户划入交易	313
10.6.2	医疗消费交易	314
10.6.3	其他交易	316
第 11 章	中国石化加油集成电路卡应用	317
11.1	应用描述	317
11.1.1	应用及其实现要求	317
11.1.2	应用过程中包含的交易	318
11.2	应用文件的设计	318
11.2.1	DF 文件	318
11.2.2	数据 EF 文件	319
11.2.3	相关的数据描述	321
11.3	应用相关的命令集	323
11.3.1	修改个人密码 (CHANGE PIN) 命令	323
11.3.2	圈存 (CREDIT FOR LOAD) 命令	324
11.3.3	消费 (DEBIT FOR PURCHASE) 命令	325
11.3.4	圈提 (DEBIT FOR UNLOAD) 命令	326
11.3.5	解扣 (DEBIT FOR UNLOCK) 命令	327
11.3.6	读余额 (GET BALANCE) 命令	328
11.3.7	读取灰锁 (GET LOCK PROOF) 命令	329
11.3.8	取交易认证 (GET TRANSACTION PROOF) 命令	331
11.3.9	灰锁 (GREY LOCK) 命令	332
11.3.10	联机解扣 (GREY UNLOCK) 命令	333
11.3.11	灰锁初始化 (INITIALIZE FOR GREY LOCK) 命令	334
11.3.12	联机解扣初始化 (INITIALIZE FOR GREY UNLOCK) 命令	335
11.3.13	圈存初始化 (INITIALIZE FOR LOAD) 命令	336

11.3.14	消费初始化 (INITIALIZE FOR PURCHASE) 命令	337
11.3.15	圈提初始化 (INITIALIZE FOR UNLOAD) 命令	338
11.3.16	修改初始化 (INITIALIZE FOR UPDATE) 命令	340
11.3.17	重装个人密码 (RELOAD PIN) 命令	341
11.3.18	修改透支限额 (UPDATE OVERDRAW LIMIT) 命令	342
11.4	卡片的状态维护	343
11.4.1	卡片的状态	343
11.4.2	卡片状态的变化	343
11.4.3	状态和命令之间的关系	343
11.5	安全结构设计	344
11.5.1	密钥管理原则	344
11.5.2	应用涉及的密钥	345
11.5.3	子密钥的计算方法	345
11.5.4	过程密钥的计算方法	346
11.6	交易与命令的实现流程	346
11.6.1	交易预处理	346
11.6.2	加油专用消费交易	349
11.6.3	联机解扣交易	353
11.6.4	补扣交易	356
11.6.5	补充交易	359
11.6.6	圈存交易	360
11.6.7	圈提交易	362
11.6.8	加油普通消费交易	365
11.6.9	修改透支限额交易	367
11.6.10	查询余额交易	370
11.6.11	查询明细交易	370
11.6.12	应用维护功能	370
11.6.13	防拔	372
11.7	命令在交易过程中的使用示例	372
11.7.1	加油专用消费交易	372
11.7.2	联机解扣交易	375
11.7.3	补扣交易	376
11.7.4	补充交易	377
11.7.5	圈存交易	378
11.7.6	圈提交易	379
11.7.7	普通消费交易	380
11.7.8	修改透支限额交易	381
11.7.9	查询余额交易	382
11.7.10	修改 PIN	383
11.7.11	重装 PIN	383

第 12 章 支持公钥应用的公钥 (PKI) 卡	385
12.1 PKI 体系	385
12.1.1 PKI 体系介绍	385
12.1.2 PKI 体系的结构	386
12.1.3 PKI 体系的工作	388
12.1.4 PKI 体系的安全分析	389
12.2 PKI 体系相关算法	390
12.2.1 数字签名	390
12.2.2 加密算法	401
12.3 PKI 卡的实现	406
12.3.1 算法在卡内的选择与实现	406
12.3.2 文件结构	407
12.3.3 处理流程	408
12.4 PK 相关的命令	410
12.4.1 管理安全环境 (MANAGE SECURITY ENVIRONMENT)	410
12.4.2 密钥导入 (WRITE KEY)	413
12.4.3 密钥生成 (GENERATE KEY)	415
12.4.4 密钥导出 (EXPORT KEY)	417
12.4.5 散列计算 (HASH)	418
12.4.6 数据加密 (ENCIPHER)	421
12.4.7 数据解密 (DECIPHER)	422
12.4.8 数字签名 (SIGNATURE)	423
12.4.9 数字签名验证 (VERIFY SIGNATURE)	426
第 13 章 智能卡应用解决方案示例	429
13.1 校园一卡通应用	429
13.1.1 校园一卡通系统介绍	429
13.1.2 一卡通系统的结构	430
13.1.3 一卡通系统的配置	432
13.2 社会保障卡应用	432
13.2.1 社会保障卡系统介绍	432
13.2.2 社会保障卡系统的结构	433
13.2.3 社会保障卡系统的配置	433
13.3 网吧监管系统应用	434
13.3.1 网吧监管系统介绍	434
13.3.2 网吧监管系统的结构	435
13.3.3 网吧监管系统的配置	436
13.4 关于智能卡应用系统的设计开发	436
附录 主要缩略词列表	437

第 1 章 初识 IC 卡

本章主要介绍 IC 卡的一些背景知识,让读者对 IC 卡及其应用情况和卡内操作系统(Chip Operation System, 简称 COS)有一个初步认识,主要包括如下几项内容:

- IC 卡发展的历史。
- IC 卡国内外的应用现状。
- IC 卡的主要应用领域。
- 卡内操作系统的基本概念。
- 卡内操作系统的发展现状。

1.1 IC 卡的发展与现状

1.1.1 IC 卡的发展历史

1970 年,法国人罗兰德·莫瑞诺(Roland Moreno)第一次将可进行编程设置的 IC (Integrated Circuit) 芯片放于卡片中,使卡片具有更多的功能。当时他在专利申请书中,对这项发明作了如下阐述:卡片上具有可进行自我保护的存储器。这样就诞生了世界上第一张 IC 卡。在此后的时间里,随着超大规模集成电路技术、计算机技术以及信息安全技术的发展,IC 卡技术也更趋成熟,它的发展经历了多个重要阶段,其技术也在不断地进步。

智能卡属于半导体卡,半导体卡片采用微电子技术进行信息的存储、处理。按照其组成结构,智能卡可以分为一般存储卡、加密存储卡、CPU 卡和超级智能卡等。

- 一般存储卡 (Memory Card)

一般存储卡也叫非加密存储卡,其内嵌芯片相当于普通串行 EEPROM 存储器,有些芯片还增加了特定区域的写保护功能,这类卡存储信息方便、使用简单、价格便宜、很多场合可替代磁卡,但由于其本身不具备信息保密功能,因此,只能用于保密性要求不高的应用场合。

- 加密存储卡 (Security Card)

加密存储器卡内嵌芯片在存储区外增加了控制逻辑,在访问存储区之前需要核对密码,只有密码正确,才能进行存取操作,这类信息保密性较好,使用与普通存储器卡相类似。但是密码一般通过明文进行传递和验证,很容易被破解,一般用于需要进行简单保密要求的应用场合。

- CPU 卡 (Smart Card)

CPU 卡内嵌芯片相当于一个特殊类型的单片机,内部除了带有控制器、存储器、时序控制逻辑等外,还带有算法单元和操作系统,由于 CPU 卡有存储容量大,处理能力强,信息存

储安全等特性，因此，被广泛用于信息安全性要求特别高的场合。

- 超级智能卡（Super Smart Card）

在卡上具有 MPU 和存储器并装有键盘、液晶显示器和电源，有的卡上还具有指纹识别装置等，主要用于高端应用。其核心和 CPU 卡类似，主要增加的是外围的辅助单元。

CPU 卡的出现是 IC 卡发展史上的重要阶段，区别于它的前身——加密存储卡，其芯片具有更强的数据处理能力，能够在卡内完成复杂的数据运算和逻辑控制，从硬件底层提供了对数据和应用强大的安全保护能力，逐步成为了卡应用的主流，本书将要介绍的就是 CPU 卡（根据不同区域场合，也称为智能卡、IC 卡、聪明卡等）。

按照卡片数据的读写方式，智能卡又可分为接触式 IC 卡、非接触式 IC 卡和双界面卡 3 种类型。

- 接触式 IC 卡

由读写设备的触点和卡片上的触点相接触才能够进行数据读写。

- 非接触式 IC 卡

卡片使用过程中与读写设备无直接的电路接触，由无线非接触技术进行读写（例如，光或无线电技术等）。和接触式 IC 卡相比较还增加了射频收发电路，这类卡一般用在使用频繁、使用要求便利的场合。

- 双界面卡

双界面卡综合了以上两种读写技术于一身，既能够提供接触式读写方式，也能够提供非接触式读写接口，方便用户在不同场合使用卡片的不同需求。

智能卡的出现是微电子、计算机和信息安全等多学科技术综合的结果，作为一种成熟的高技术产品，智能卡的广泛使用将能够提高人们生活和工作的现代化程度，这已成为一个国家科技发展水平的标志之一。

1.1.2 IC 卡在国外的应用情况

在 1988 年 10 月至 1989 年 9 月期间，全世界 IC 卡和读写器数量已分别达 4200 万张和 87700 台，其中法国分别占 98% 及 71%，处于世界领先地位。据智能卡月刊（Smart Card Monthly）统计，目前每年的 IC 卡产量突破 4 亿张（其中 CPU 卡所占的比重不低于 50%），IC 卡和 IC 卡处理设备总产值均突破 15 亿美元。这些卡的使用，必然遍布人类生活的各个领域，也必然涉及到数以千计的工程，还有服务、咨询等方面的业务，整个智能数据卡的市场将是巨大的。

新一代智能卡将以储值卡为主，主要应用领域包括 Internet 购物、商店售货亭、移动电话卡、家庭电视付费点播卡等。另外用于存储媒体信息和个人信息的数据卡也将有比较显著的增长。

从具体应用领域来讲，在金融领域世界上最大的信用卡集团 VISA 卡集团，为扩展金融服务范围，满足未来金融服务的需要及提高安全性，开始准备转向智能卡。VISA 还和 MasterCard 以及 Europay 共同制定新的国际银行交易标准，这将极大拓展世界性的智能卡应用范围。

医疗事业领域，法国将在所有医疗事业发行单一的国家智能卡。为从根本上改善法国全国的国有医疗系统的有效性、高效性铺平道路，这种智能卡还将朝着健康医疗信息技术方向