中国金融集成电路(IC)卡规范

全国金融标准化技术委员会　编

中国金融出版社

责任编辑:赵燕红
责任校对:吕　莉
责任印制:裴　刚

图书在版编目(CIP)数据

中国金融集成电路(IC)卡规范(V1.0)/全国金融标准化技术委员会编.
—北京:中国金融出版社,1998.4
ISBN 7-5049-1937-3
Ⅰ.中…
Ⅱ.全…
Ⅲ.集成电路-信用卡-规范-中国
Ⅳ.F 832.2-65
中国版本图书馆 CIP 数据核字(98)第 07448 号

出版:
发行:中国金融出版社
社址:北京广安门外小红庙南里 3 号
邮编:100055
经销:新华书店
印刷:北京印刷一厂
开本:850 毫米×1168 毫米　1/16
印张:9.5
插页:1
字数:262 千
版次:1998 年 6 月第 1 版
印次:1998 年 6 月第 1 次印刷
印数:1—3800
定价:35.00 元

内容提要

该书以国际标准和国内标准为基础，结合国内金融IC卡应用的实际需要和各商业银行试点的经验，对我国金融IC卡的基本应用作出了具体规定，以确定一个满足国内金融IC卡应用需求的技术平台。

前　言

随着电子技术的发展，集成电路(IC)卡的应用得到了社会各界的广泛重视。从1995年中国银行在海南发行国内第一张金融IC卡开始，各商业银行陆续开展了金融IC卡试点工作，业务范围覆盖消费、取现、医疗保险、社会保障和公共事业收费等许多领域，取得了丰富的经验和较好的社会经济效益。

作为一种新兴技术，金融IC卡的相关标准大都处于研制阶段。国际标准化组织(ISO)目前已制定出了部分相关标准，但基本上局限在对卡片技术的原则性规定方面，可操作性较差。为了更好地规范和指导国内金融IC卡业务和技术的发展，尽可能避免投资的浪费，并为今后金融IC卡的跨行、跨地区使用和设备共享做好技术上的准备工作，有必要制定统一的《中国金融集成电路(IC)卡规范》(以下简称本规范)。

《本规范》制定工作坚持积极采用国际标准和国外先进标准的原则，以ISO标准(ISO/IEC7811、ISO/IEC7816等)和Europay、Mastercard、Visa三大国际组织开发研制的用于付款业务的IC卡通用规范平台—EMV'96为基础，结合国内金融IC卡应用的实际需要和各商业银行试点的经验，对我国金融IC卡的基本应用作出了具体规定。其目的是确定一个满足国内金融IC卡应用需求的技术平台。

《本规范》具有以下几方面的特点：

1. 兼容性。本规范是在参照采用ISO相关国际标准和原则的前提下，以EMV规范为基础制定完成的，从而保证了与国外同类产品的兼容性。

2. 灵活性和开放性。本规范设计了一个支持多功能应用的技术平台，详细规定了电子存折、电子钱包和磁条卡功能(Easy Entry)三种基本应用，并允许使用单位依据自身业务的需要进行裁剪和添加。这不仅保证了其功能选择的灵活性，同时也保证了对其他应用的开放性。

3. 通用性和独立性。本规范为金融IC卡应用设计了统一的指令接口界面，但并未规定其具体实现的手段。这样不仅保证了不同厂商开发的卡片的通用性和实现技术的独立性，又有利于促进新技术的采用。

4. 先进性。本规范在采纳现有先进技术的同时，充分考虑到相关技术的发展前景，如JAVA卡技术、RSA技术等，从而保证了技术的先进性。

《本规范》制定工作经历了需求设计和详细设计两个阶段，其内容包括三个部分：

第1部分：卡片规范。本部分主要规定了金融IC卡应用的通用功能、命令和安全机制。包括电气物理特性、逻辑接口和传输协议；数据元和命令集；应用选择和安全机制等内容。

第2部分：应用规范。本部分主要规定了金融IC卡的基本应用，包括应用特有的功能、命令、数据元和安全要求；数据元到文件的映象；交易流程；异常处理；特有的数据对象编码等内容。

第3部分：终端规范。本部分主要规定了金融IC卡应用中对终端的基本功能要求。

《本规范》的第1部分和第2部分已制定完成，第3部分的制定工作将在1998年结束。

IC卡的内部处理、安全控管的详细过程以及主机的信息格式不在本规范范围内。卡片个人化、安全存取模块(SAM)在本规范中暂不做规定。

《本规范》的使用对象主要是与金融IC卡应用相关的卡片设计、制造、管理、发行、受理以及应用系统的研制、开发、集成和维护等部门(单位),也可以供其他单位参考。

本规范由全国金融标准化技术委员会提出。

本规范由VISA国际组织协助制定。

本规范的主要制定单位有:中国人民银行、中国工商银行、中国农业银行、中国银行、中国建设银行、交通银行、上海浦东发展银行、海南国际金融网络股份有限公司和中钞信用卡厂。

本规范的主要起草人员有:刘钟、聂舒、陆书春、刘志刚、董利、李阔南、冯文亮、涂小军、阮英、李大明、李建峰、郝民、王汉民、奚力铭、铁锦程、陈敬平等。

目　录

第1部分　卡片规范

第 2 部分　应用规范

第 1 部分　卡片规范

引言

《本规范》第 1 部分卡片规范包括以下主要内容：

——机电接口、逻辑接口和传输协议。用于卡和终端间的信息交换。本篇参照采用了 ISO 7816 第 1 至第 3 部分并与 EMV'96 - 支付系统集成电路卡规范的第 1 部分等同。

——数据元和命令集。定义了金融应用中所使用的一般数据元、命令集和对终端响应的基本要求。金融应用中所需的专用命令在《本规范》第 2 部分应用规范中定义。

——应用选择。定义了卡和终端完成应用选择的处理过程，并规定了与卡中此过程相关的数据文件的逻辑结构。此部分与 EMV'96 - 支付系统集成电路卡规范的第 3 部分等同。

——安全机制。定义了金融应用中有关安全的总体要求、加密算法和安全机制。应用安全特征和设备要求在《本规范》第 2 部分应用规范中定义。

1. 范围

《本规范》第 1 部分卡片规范适用于由银行发行或接受的金融 IC 卡。其使用对象主要是与金融 IC 卡应用相关的卡片设计、制造、管理、发行、受理以及应用系统的研制、开发、集成和维护等部门(单位)，也可以作为其他行业 IC 卡应用的参考。

2. 参考资料

EMV'96:1996	支付系统的集成电路卡规范
EMV'96:1996	支付系统的集成电路卡应用规范
EMV'96:1996	支付系统的集成电路卡终端规范
FIPS Pub 180 - 1:1995	安全哈什标准
IEC 512 - 2:1979	机电设备机电器件规范　第 2 部分：触点电阻测试、绝缘测试和电压测试
ISO 639:1988	名称及语言表示代码
GB 2659:1994	世界各国和地区名称代码(ISO 3166:1993)
GB/T 12406:1996	表示货币和资金的代码(ISO 4217:1995)
GB/T 15120.1	识别卡　记录技术　第 1 部分：凸印(ISO/IEC 7811 - 1:1992)
GB/T 15120.3	识别卡　记录技术　第 3 部分：ID - 1 型卡上凸印字符的位置(ISO/IEC 7811 - 3:1992)
SJ/S 9028	识别卡　金融交易卡　ISO/IEC 7813:1990
GB/T 16649.1:1996	识别卡　带触点的集成电路卡　第 1 部分：物理特性(ISO/IEC 7816 - 1:1987)
GB/T 16649.2:1996	识别卡　带触点的集成电路卡　第 2 部分：触点的尺寸和位置(ISO/IEC 7816 - 2:1988)
GB/T 16649.3:1996	识别卡　带触点的集成电路卡　第 3 部分：电信号和传输协议(ISO/IEC 7816 - 3:1989)
ISO/IEC 7816 - 3:1992	识别卡　带触点的集成电路卡　第 3 部分：电信号和传输

	协议 修订稿 1:T=1,异步半双工块传输协议
ISO/IEC 7816-3:1994	识别卡 带触点的集成电路卡 第 3 部分:电信号和传输协议 修订稿 2:协议类型选择(国际标准草案)
ISO/IEC 7816-4:1995	识别卡 带触点的集成电路卡 第 4 部分:行业间交换用命令
ISO/IEC 7816-5:1994	识别卡 带触点的集成电路卡 第 5 部分:应用标识符的编号系统和注册程序
ISO/IEC 7816-6:1995	识别卡 带触点的集成电路卡 第 6 部分:行业间数据元(国际标准草案)
ISO 8731-1:1987	银行业务 已批准的报文鉴别算法 第 1 部分:DEA
ISO 8372:1987	信息处理 64 位块加密算法的运算方法
GB/T 16263:1996	信息技术开放系统互联 抽象语法表示 1(ASN.1)的基本编码规则(ISO/IEC 8825:1990)
GB/T 15150:1996	产生报文的银行卡 交换报文规范 金融交易内容(ISO 8583:1987)
ISO 8583:1993	产生报文的银行卡 交换报文规范 金融交易内容
GB/T 15273	信息处理八位单字节代码型图型字符集 (ISO 8859:1987)
ISO/IEC 9796-2	信息技术 安全技术 报文恢复的数字签名方法第 2 部分:使用哈什函数的机制
ISO/IEC 9797:1993	信息技术 安全技术 使用块加密算法进行加密检查的数据完整性机制
ISO/IEC 10116:1993	信息技术 n 位块加密算法的运算方法
ISO/IEC 10118-3:1996	信息技术 安全技术 哈什函数 第 3 部分:专用哈什函数
ISO/IEC 10373:1993	识别卡 测试方法

中国人民银行《银行 IC 卡规范需求说明书》(1997.1)

3.定义

以下定义适用于本规范:

3.1 块 Block

包含两个或三个域(头域、信息域、尾域)的字符组。

3.2 冷复位 Cold Reset

当 IC 卡的电源电压和其他信号从静止状态中复苏且申请复位信号时,IC 卡产生的复位。

3.3 热复位 Warm Reset

在时钟(CLK)和电源电压(VCC)处于激活状态的前提下,IC 卡收到复位信号时产生的复位。

3.4 接口设备 Interface Device

终端上插入 IC 卡的部分,包括其中的机械和电气部分。

3.5 终端 Terminal

为完成金融交易而在交易点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其他部件和接口，例如与主机通讯的接口。

3.6　命令 Command

终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.7　连接 Concatenation

两个元素的连接是指将第 2 个元素附加到第 1 个元素的末尾。每个元素的字节在结果串中的排列顺序与其从 IC 卡发送到终端的顺序相同，即：高位字节先送。每个字节位按照从最高位到最低位的顺序排列。一组元素或对象可以通过最先两个相连的方式连接成一个新元素，即第 1 个与第 2 个相连，再与第 3 个相连，…，依次类推。

3.8　触点 Contact

在集成电路卡和外部接口设备之间保持电流连续性的导电元件。

3.9　响应 Response

IC 卡处理完成收到的命令报文后，返回给终端的报文。

3.10　凸印 Embossing

使字符从卡的正面显著地凸起。

3.11　头域 Prologue Field

块的第一部分，包括节点地址(AD)、协议控制字节(PCB)和长度(LEN)。

3.12　尾域 Epilogue Field

块的最后一部分，包括错误校验代码(EDC)位。

3.13　金融交易 Financial Transaction

持卡者、商户和收单行之间基于收、付款方式的商品或服务交换行为。

3.14　功能 Function

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

3.15　保护时间 Guardtime

同一方向发送的前一个字符奇偶位下降沿和后一个字符起始位上升沿之间的最小时间。

3.16　哈什函数 Hash Function

将位串映射为定长位串的函数，它具有以下两个特性：

——对于一个给定的输出，不可能推导出与之相对应的输入；

——对于一个给定的输入，不可能推导出第 2 个具有同一输出的输入。

另外，如果要求哈什函数具备防冲突功能，则还应具有以下特性：

——不可能找到任意两个不同的输入，得出相同的输出。

3.17　哈什结果 Hash Result

哈什函数的输出位串。

3.18　静止状态 Inactive

当 IC 卡上的电源电压(VCC)和其他信号相对于地的电压值小于或等于 0.4 伏时，则称电源电压和这些信号处于静止状态。

3.19　集成电路 Integrated Circuit(IC)

设计用于完成处理和/或存储功能的电子器件。

3.20　集成电路卡(IC 卡)Integrated Circuit(s) Card

内部封装一个或多个集成电路的 ID－1 型卡(如 ISO 7810、ISO 7811 第 1 至第 5 部分、

ISO 7812 和 ISO 7813 中描述的)。

3.21 报文 Message

由终端向卡或卡向终端发出的,不含传输控制字符的字节串。

3.22 报文鉴别代码 Message Authentication Code

对交易数据及其相关参数进行运算后产生的代码,主要用于验证报文的完整性。

3.23 半字节 Nibble

一个字节的高四位或低四位。

3.24 明文 Plaintext

没有加密的信息。

3.25 密文 Ciphertext

通过密码系统产生的不可理解的文字或信号。

3.26 密钥 Key

控制加密转换操作的符号序列。

3.27 数字签名 Digital Signature

一种非对称加密数据变换,它使得接收方能够验证数据的原始性和完整性,保护发送和接收的数据不被第三方伪造,同时对于发送方来说,还可用以防止接收方的伪造。

3.28 加密算法 Cryptographic Algorithm

为了隐藏或揭露信息内容而变换数据的算法。

3.29 认证机构 Certification Authority

利用公开密钥和其他相关数据为所有者提供可靠校验的第三方机构。

3.30 对称加密技术 Symmetric Cryptographic Technique

发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下,不可能推导出发送方或接收方的数据变换。

3.31 非对称加密技术 Asymmetric Cryptographic Technique

采用两种相关变换进行加密的技术,一种是公开变换(由公共密钥定义),另一种是私有变换(由私有密钥定义)。这两种变换具有以下属性,即私有变换不能通过给定的公开变换导出。

3.32 私有密钥 Private Key

一个实体的非对称密钥对中仅供实体自身使用的密钥,在数字签名模式中,私有密钥用于签名功能。

3.33 公共密钥 Public Key

一个实体的非对称密钥对中可以公开的密钥,在数字签名模式中,公共密钥用于验证功能。

3.34 公开密钥认证 Public Key Certification

由认证机构签发的一个实体的公共密钥信息,具有不可伪造性。

3.35 保密密钥 Secret Key

对称加密技术中仅供指定实体所用的密钥。

3.36 数据完整性 Data Integrity

数据不受未经许可的方法变更或破坏的属性。

3.37 状态 H State H

高电平状态。根据 IC 卡中的逻辑约定,可以是逻辑 1 或逻辑 0。

3.38　状态 L State L

低电平状态。根据 IC 卡中的逻辑约定，可以是逻辑 1 或逻辑 0。

3.39　T=0

面向字符的异步半双工传输协议。

3.40　T=1

面向块的异步半双工传输协议。

4.缩略语和符号表示

以下缩略语和符号表示适用于本规范：

AAC	应用认证密码(Application Authentication Cryptogram)
AAR	应用授权参考(Application Authorization Referral)
AC	应用密码(Application Cryptogram)
ACK	确认(Acknowledgment)
ADF	应用数据文件(Application Definition File)
AEF	应用基本文件(Application Elementary File)
AFL	应用文件位置(Application File Locator)
AID	应用标识符(Application Identifier)
an	字母数字型(Alphanumeric)
ans	字母数字及特殊字符型(Alphanumeric Special)
APDU	应用协议数据单元(Application Protocol Data Unit)
ARPC	授权响应密码(Authorization Response Cryptogram)
ARQC	授权请求密码(Authorization Request Cryptogram)
ASN.	抽象语法表示(Abstract Syntax Notation)
ATC	应用交易序号(Application Transaction Counter)
ATR	复位应答(Answer to Reset)
b	二进制(Binary)
BER	基本编码规则(Basic Encoding Rules)
BGT	块保护时间(Block Guard Time)
BWI	块等待时间整数(Block Waiting Time Integer)
BWT	块等待时间(Block Waiting Time)
C-APDU	命令 APDU(Command APDU)
CBC	加密数据块链(Cipher Block Chaining)
CIN	输入电容(Input Capacitance)
CLA	命令报文的类别字节(Class Byte of the Command Message)
CLK	时钟(Clock)
cn	压缩数字(Compressed Numeric)
C-TPDU	命令 TPDU(Command TPDU)
CWI	字符等待时间整数(Character Waiting Time Integer)
CWT	字符等待时间(Character Waiting Time)

DAD	目标节点地址(Destination Node Address)
DDF	目录数据文件(Directory Definition File)
DEA	数据加密算法(Data Encryption Algorithm)
DES	数据加密标准(Data Encryption Standard)
DF	专用文件(Dedicated File)
DIR	目录(Directory)
EDC	错误检测代码(Error Detection Code)
EF	基本文件(Elementary File)
EMV	Europay、Mastercard、VISA
etu	基本时间单元(Elementary Time Unit)
FCI	文件控制信息(File Control Information)
f	频率(Frequency)
FIPS	联邦信息处理标准(Federal Information Processing Standard)
GND	地(Ground)
hex.	十六进制数(Hexadecimal)
HHMM	时、分(Hours, Minutes)
HHMMSS	时、分、秒(Hours, Minutes, Seconds)
I-block	信息块(Information Block)
IC	集成电路(Integrated Circuit)
ICC	集成电路卡(Integrated Circuit Card)
IEC	国际电工委员会(International Electrotechnical Commission)
IFD	接口设备(Interface Device)
IFS	信息域大小(Information Field Size)
IFSC	IC卡信息域大小(Information Field Size for the ICC)
IFSD	终端信息域大小(Information Field Size for the Terminal)
I_{IH}	高电平输入电流(High Level Input Current)
I_{IL}	低电平输入电流(Low Level Input Current)
INF	信息域(Information Field)
INS	命令报文的指令字节(Instruction Byte of Command Message)
I/O	输入/输出(Input/Output)
I_{OH}	高电平输出电流(High Level Output Current)
I_{OL}	低电平输出电流(Low Level Output Current)
ISO	国际标准化组织(International Organization for Standardization)
K_M	主控密钥(Master Key)
K_S	过程密钥(Session Key)
Lc	终端发出的命令数据的实际长度(Exact Length of Data Sent by the TAL IN A Case 3 or 4 Command)
lcm	最小公倍数(Least Common Multiple)
Le	响应数据的最大期望长度(Maximum Length of Data Expected