

ICS 35.240.15
L 64



中华人民共和国国家标准

GB/T 18392—2001

中华人民共和国组织机构代码证 集成电路(IC)卡技术规范

**Norm of Integrated Circuit (IC) card of certificate of
identity code for organizations institutions and
enterprises of the People's Republic of China**

2001-07-16 发布

2002-03-01 实施

中 华 人 民 共 和 国 发 布
国 家 质 量 监 督 检 验 检 疫 总 局

前 言

本标准是中华人民共和国组织机构代码证集成电路(IC)卡(简称“代码证 IC 卡”)制作、颁发及应用的技术规范。

本标准由中国标准研究中心提出。

本标准由中国标准研究中心归口。

本标准负责起草单位:全国组织机构代码管理中心、中国华大集成电路设计中心、中国长城计算机软件与系统有限公司、华旭金卡(集团)公司、清华大学。

本标准参加起草单位:上海市技术监督信息研究所、深圳市标准与编码研究院、宁波市物品编码所。

本标准主要起草人:顾迎建、张冬青、董浩然、刘渤、何华康、黄晓东、丁荣兴、卢义明、沈同、王家振、龚正孟、周京涛、程晋格、沙江。

中华人民共和国国家标准

中华人民共和国组织机构代码证 集成电路(IC)卡技术规范

GB/T 18392—2001

Norm of Integrated Circuit (IC) card of certificate of
identity code for organizations institutions and
enterprises of the People's Republic of China

1 范围

本标准规定了中华人民共和国组织机构代码证集成电路(IC)卡(以下简称代码证 IC 卡)的技术要求,规定了代码证 IC 卡的卡片规范和代码证 IC 卡的应用。

本标准适用于代码证 IC 卡的设计、制造、管理、发行和应用,以及代码证 IC 卡相关设备接口的设计等。

2 引用标准

下列标准所包含的条文,通过在本标准中引用而构成为本标准的条文。本标准出版时,所示版本均为有效。所有标准都会被修订,使用本标准的各方应探讨使用下列标准最新版本的可能性。

- GB 11714—1997 全国组织机构代码编制规则
- GB/T 12406—1996 表示货币和资金的代码(idt ISO 4217:1990)
- GB/T 2659—2000 世界各国和地区名称代码(eqv ISO 3166-1:1997)
- GB/T 2260—1999 中华人民共和国行政区划代码
- GB/T 7408—1994 数据元和交换格式 信息交换 日期和时间表示法(eqv ISO 8601:1988)
- GB/T 14916—1994 识别卡 物理特性(idt ISO 7810:1985)
- 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
(idt ISO 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
(idt ISO 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
(idt ISO/IEC 7816-3:1989)
- GB/T 17554—1998 识别卡 测试方法(idt ISO/IEC 10373:1993)
- ISO 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 7816-5:1995 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过程

3 定义

3.1 代码证 IC 卡

载体为集成电路(IC)卡的中华人民共和国组织机构代码证。是一种供机器读写的、可作为组织机构代码及其基本信息查询和交换用的识别卡。

全国组织机构代码统一社会信用代码数据服务中心
<https://www.cods.org.cn>

3.2 初始化

由发卡单位对所发的 IC 卡进行的一项操作。主要是将卡内的数据文件,包括应用扩展区内的数据文件进行格式化。

4 卡片规范

4.1 机电特性

4.1.1 卡的物理特性

代码证 IC 卡应符合 GB/T 16649.1 中规定的物理特性要求。

4.1.2 IC 模块的高度

封装于代码证 IC 卡上的 IC 模块表面的最高点不应高于卡表面平面 0.05 mm,最低点不应低于卡表面平面 0.10 mm。

4.1.3 卡的触点尺寸和位置

卡上每个触点的尺寸、数量和位置应符合 GB/T 16649.2 中的规定,且触点位于卡的正面。

4.1.4 卡的电气特性

卡的电气特性在卡触点和接口设备(IFD)触点之间进行测量,并以接地端为参考点。环境温度范围为 0℃~50℃。所有流入卡的电流都认为是正向的。

4.1.4.1 卡的触点分配

卡上触点的定义符合 GB/T 16649.2 的规定。如表 1 所示。

表 1 卡触点的分配

触 点	分 配	触 点	分 配
C1	电源电压(VCC)	C5	地(GND)
C2	复位信号(RST)	C6	不使用
C3	时钟信号(CLK)	C7	输入/输出(I/O)
C4	保留待将来使用	C8	保留待将来使用

4.1.4.2 操作条件

本部分定义了操作条件的两个类别。通过触点 VCC,接口设备应向卡提供下列标称电源:

A 类: 5 V,

B 类: 3 V。

因此,卡和接口设备应或者仅工作在 A 类、或者仅工作在 B 类、或者工作在 A 类及 B 类(以下表示为 AB 类)。A 类卡应与 A 类和 AB 类接口设备一起操作;AB 类卡应与 A 类、B 类和 AB 类接口设备一起操作;B 类卡应与 B 类或 AB 类接口设备一起操作,B 类卡应以这种方法来设计,以使它们在 A 类操作条件下不被损坏。

图 1 表示出了接口设备如何选择适用于卡的操作条件的类别。当操作条件可用于接口设备时,用于卡的第一个操作条件应为 B 类。

操作条件在 A 类时,B 类卡应不提供复位应答。如果卡不提供复位应答,则接口设备应释放卡。在至少 10ms 的延迟后,接口设备应使用下一个可用类别的操作条件。如果卡提供不带类别指示符的复位应答,则接口设备应使用或保持 A 类操作条件(当 A 类操作条件可用时)或释放此卡。如果卡提供带有类别指示符的复位应答,并且接口设备正应用卡所支持的操作条件类别,则正常操作可以继续。如果复位应答不指示当前操作条件类别,但指示接口设备支持另一操作条件类别,则接口设备应激活该卡,在至少延迟 10 ms 后,接口设备应使用那个类别的操作条件。

注:当以 B 类条件操作时,与 GB/T 16649.3 一致的某些卡将被损坏,因此它们仅用于 A 类接口设备。

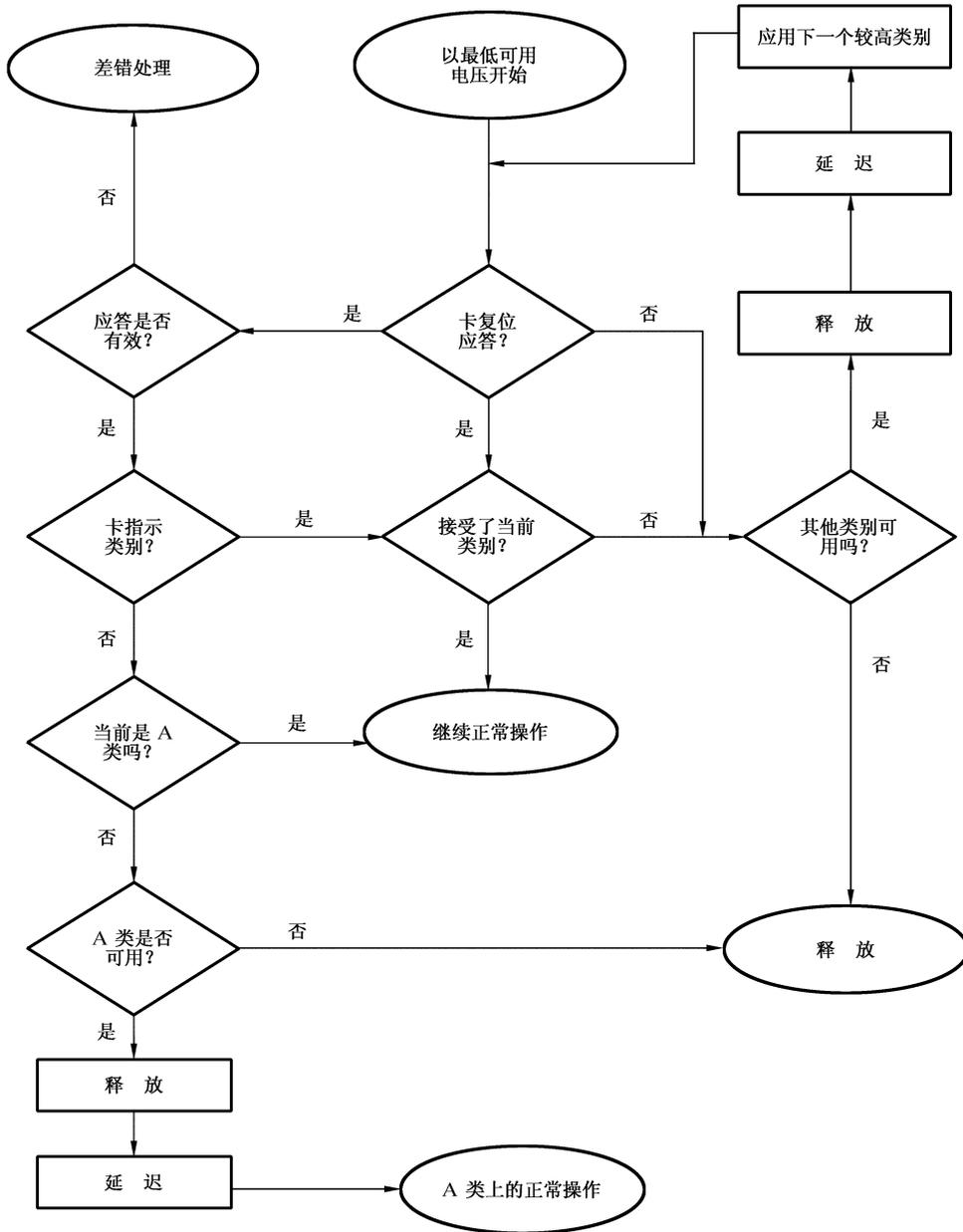


图1 操作条件选择

4.1.4.3 卡的输入/输出触点(I/O)

该触点用作输入端(接收模式)从终端接收数据,或者用作输出端(发送模式)向终端传输数据。

a) 接收模式

当电源电压(V_{CC})在本标准允许范围内时,卡接收到的终端信号的电气特性如表2所示:

表2 IC卡接收模式下I/O触点的电气特性

符 号	说 明	最 小 值	最 大 值	单 位
V_{IH}	输入高电平	$0.7 \times V_{CC}$	V_{CC}	V
V_{IL}	输入低电平	0	$0.15 \times V_{CC}$	V
t_R 和 t_F	输入波形的上升和下降时间	—	1.0	μs

b) 发送模式

在发送模式下, IC 卡将把数据传送到终端, 其电气特性如表 3 所示。IC 卡的 I/O 不具备电流源性能。

表 3 IC 卡发送模式下 I/O 触点的电气特性

符 号	说 明	条 件	最 小 值	最 大 值	单 位
V_{OH}	输出高电平	$-20\ \mu\text{A} < I_{OH} < 0, V_{CC}$ 为 min	$0.7 \times V_{CC}$	V_{CC}	V
V_{OL}	输出低电平	$0 < I_{OL} < 1\ \text{mA}, V_{CC}$ 为 min	0	$0.15 \times V_{CC}$	V
t_R 和 t_F	输出波形的上升和下降时间	$C_N = 30\ \text{pF}$	—	1.0	μs

在执行过程中, IC 卡和终端不能同时处于发送模式。

4.1.4.4 卡的时钟触点(CLK)

当 V_{CC} 在本标准允许范围内时, IC 卡在正常操作条件下时钟电气特性见表 4。

表 4 IC 卡 CLK 触点的电气特性

符 号	说 明	条 件	最 小 值	最 大 值	单 位
V_{IH}	输入高电平	—	$0.7 \times V_{CC}$	V_{CC}	V
V_{IL}	输入低电平	—	0	0.5	V
t_R 和 t_F	输入波形的上升和下降时间	$C_N = 30\ \text{pF}$	—	9% 的时钟周期	μs

当时钟占空比是 44%~56% 之间的某个稳定值时, IC 卡应能正常工作。

当时钟频率是 1 MHz~5 MHz(A 类) 或者 1 MHz~4 MHz(B 类) 之间的某个稳定值时, IC 卡可正常工作。

在复位应答到卡—终端会话的整个过程中, 终端应把时钟频率的变化稳定在 $\pm 1\%$ 之间。

4.1.4.5 卡的复位触点(RST)

当 V_{CC} 在本标准允许范围内时, IC 卡在正常操作条件下的复位端电气特性如表 5 所示。

表 5 IC 卡 RST 触点的电气特性

符 号	说 明	条 件	最 小 值	最 大 值	单 位
V_{IH}	输入高电平	—	$0.7 \times V_{CC}$	V_{CC}	V
V_{IL}	输入低电平	—	0	$0.12 \times V_{CC}$	V
t_R 和 t_F	输入波形的上升和下降时间	$C_N = 30\ \text{pF}$	—	1.0	μs

IC 卡用激活低复位方式对异步复位作出应答。

4.1.4.6 卡的电源触点(VCC)

当电源电压为表 6 时, IC 卡可正常工作。

表 6 IC 卡 VCC 触点的电气特性

条 件	最 小 值	最 大 值	单 位
A 类	4.5	5.5	V
B 类	2.7	3.3	V

4.1.4.7 卡的触点电阻

IC 卡触点的电阻应小于 500 m Ω , 测量方法见 GB/T 17554—1998。

4.2 卡片操作过程

4.2.1 卡的正常操作步骤

卡的操作步骤如下：

- a) 将卡插入到接口设备中,激活触点。
- b) 卡复位,建立卡和终端间的通讯。
- c) 执行操作。
- d) 置触点于空闲状态,取出卡。

4.2.1.1 卡的插入和触点激活

将卡插入接口设备时,终端应确保所有的触点处于低电平状态。在触点作物理接触之前, V_{CC} 应不大于 0.4 V 。如果 IC 卡在接口设备中位于插/拔方向正确位置的偏差在 $\pm 0.5\text{ mm}$ 范围内,接口设备应能检测到卡的存在;当接口设备探测到卡已处在此范围内,且所有的触点已作物理接触时,触点将被激活,时序如图 2 所示。

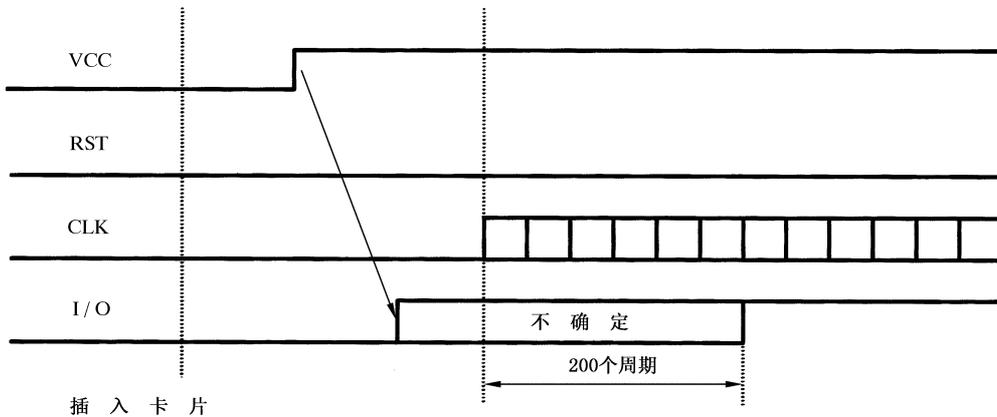


图 2 触点激活时序

- 在激活工作状态下,接口设备应将 IC 卡的 RST 端置于低电平状态。
- 在触点被激活之后而 I/O 和 CLK 激活之前,给 VCC 加电。
- 当接口设备验证了 V_{CC} 在 4.1.4.6 限制的范围内,且稳定时,终端将置 I/O 总线驱动器于接收模式。

——应为 CLK 提供 4.1.4.4 中所定义的一个合适而稳定的时钟。在时钟启动前,将终端的 I/O 线驱动器设置到接收模式,若迟后则不得迟于时钟启动后的 200 个时钟周期。

注:终端可以通过测量来确定 VCC 的状态。根据终端的设计,等待足够的时间使 VCC 达到稳定状态,在终端将 I/O 线驱动器设置到接收模式后,I/O 线的状态取决于 IC 卡的 I/O 线驱动器的状态。

4.2.1.2 卡复位

应使用低电平复位来完成异步复位应答。复位应答传输的协议在 4.3 中描述,其内容在 4.4 中描述。

随着触点的激活,终端将进行一个冷复位,并从 IC 卡获得复位应答,如图 3 所示。

- 终端在 T_0 时刻启动 CLK。
- 在 T_0 后的 200 个时钟周期内,IC 卡将 I/O 线驱动器置于接收模式,在这个时间内,因为终端也要将其 I/O 线驱动器置于接收模式,所以 I/O 线将保证在 T_0 后的 200 个时钟周期内上升到高电平。
- 卡的复位应答在 T_1 以后的 400~40 000 个时钟周期内开始。
- 如果卡的复位应答不是在这个时间段内开始,终端将进入 4.2.1.4 描述的空闲状态时序。

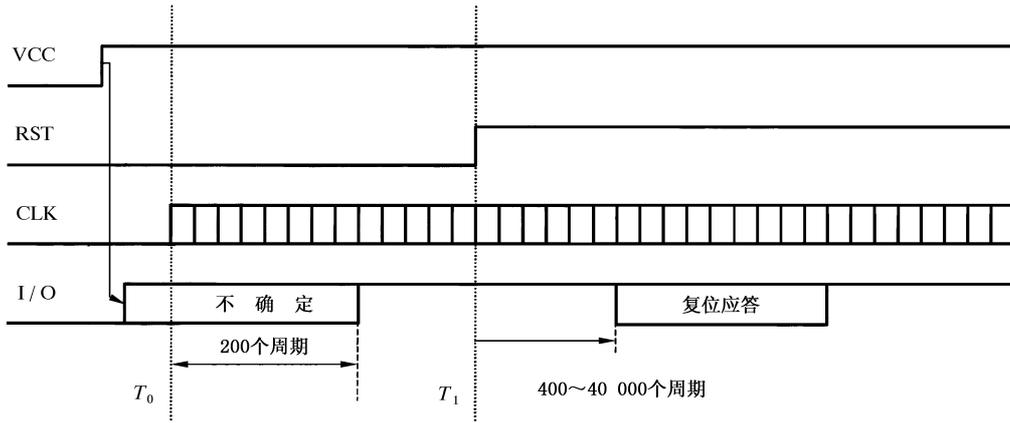


图3 复位时序

4.2.1.3 执行操作

在执行过程中,卡和终端间的信息交换,参见第5章。

4.2.1.4 触点闲置

卡操作的最后阶段,即执行的正常或异常终止阶段(包括在卡的操作过程中,将卡从接口设备中抽出),终端将把接口设备的触点置于空闲状态,如图4所示。



——终端通过把 RST 置于低电平状态来启动空闲时序。

——在将 RST 置于低电平状态之后,在 VCC 下电之前,终端将 CLK 和 I/O 端置于低电平状态。

在 RST、CLK 和 I/O 置于低电平状态之后,在卡片脱离接口设备的物理接触之前,终端下降 VCC, 此时的 V_{CC} 应不大于 0.4 V。

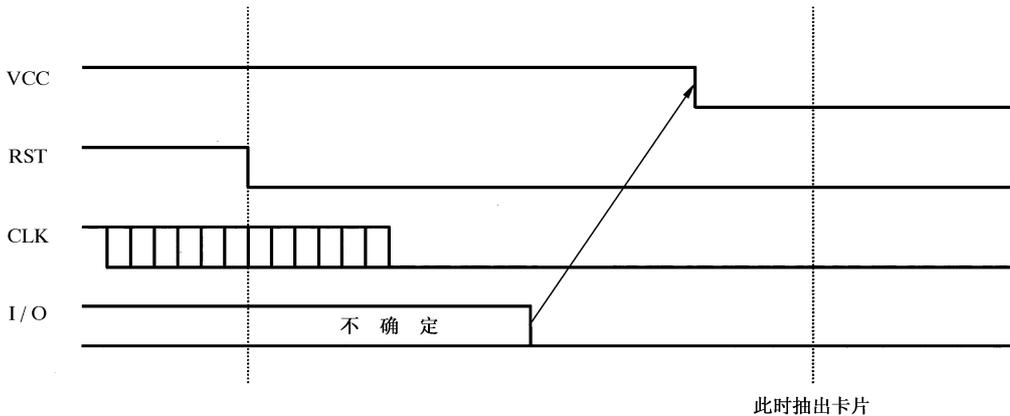


图4 触点闲置时序

4.2.2 卡执行过程中的异常中断

在执行过程中,如果卡以 1 m/s 的速度提前从终端中抽出,终端应能感觉到卡相对于接口设备的移动。当移动的相对位移达到 1 mm 时,根据 4.2.1.4 中的规定,接口设备的所有触点处于闲置状态。

注:对于滑触式结构的接口设备,终端有可能感觉到卡触点与接口设备之间的相对位移。此处不对能否感知到相对运动作强制性要求,但在卡和接口设备的触点脱离前应能将其置为闲置状态。

4.3 物理传输特性

终端和卡之间 I/O 线上的数据传输采用异步半双工协议。终端向卡提供时钟信号。

4.3.1 位定义

I/O 线上使用的位宽定义为一个基本时间单元(etu),I/O 线上的 etu 和 CLK 的频率 f 间存在一线性关系。

复位应答过程中,位宽称之为初始 etu ,并由公式(1)给出:

$$\text{初始 } etu = 372/f(s) \quad \dots\dots\dots(1)$$

这里 f 的单位为 Hz。

紧接复位应答后的位宽称之为当前 etu ,由公式(2)给出:

$$\text{当前 } etu = F/Df(s) \quad \dots\dots\dots(2)$$

这里 f 的单位为 Hz。

参数 F 和 D 的意义参见 GB/T 16649. 3。

4.3.2 字符帧

数据是按下述的字符帧方式在 I/O 线上传输的。在字符传送之前,I/O 线应处于高电平状态。

一个字符由 10 个连续的位组成(见图 5):

- 1 个低电平状态的起始位;
- 8 个数据位(低位在前);
- 1 个偶校验位。

起始位通过在 I/O 线上周期性取样来检测,取样时间应小于 $0.2 etu$ 。

8 位数据和校验位中的逻辑 ‘1’ 的个数应为偶数。

起始位的出现可以在 $0.7 etu$ 之内来验证,后续位可以在 $0.5 n \pm 0.2 etu$ 的时间间隔内检测接收,其中 n 是位的序号,起始位是 1。

在一个字符内,从起始位的前沿到第 n 位的后沿的时间间隔为 $(n \pm 0.2)etu$ 。

两个连续字符起始位前沿之间的时间间隔是字符时间 $(10 \pm 0.2)etu$,加上保护时间(最少 2 个 etu)。无错误传输时,在保护时间内,IC 卡和终端都将被设置在接收状态(I/O 线在高电平状态)。对于 $T=0$,如果 IC 卡或终端作为接收方对刚收到的字符检测到奇偶错误的话,I/O 线将被接收方设置到低电平状态,向发送方表明传输出错。

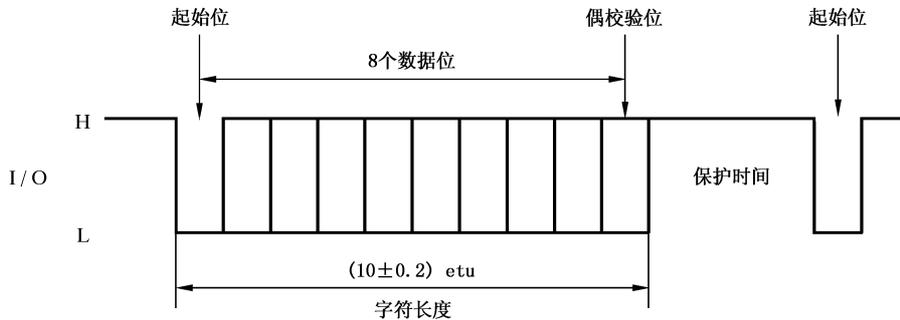


图 5 字符帧

4.4 复位应答

终端对卡复位以后,卡用一串字节来应答,称之为复位应答。这些传输到终端的信息,定义了建立在卡和终端之间的通讯特性。



4.4.1 复位应答返回字符的物理传输

在复位应答过程中,在两个连续字符的起始位前沿的最小时间间隔是 $12 etu$,最大时间间隔是 $9\ 600 etu$ 。

卡将在 $19\ 200 etu$ 内,传输在复位应答中应返回的所有字符。这个时间是第一个字符(TS)起始位的前沿和最后一个字符起始位的前沿加上 $12 etu$ 之后的时间。

4.4.2 卡复位应答返回的字符

代码证 IC 卡的复位应答结构如图 6 所示,各字符的含义依次描述如下:

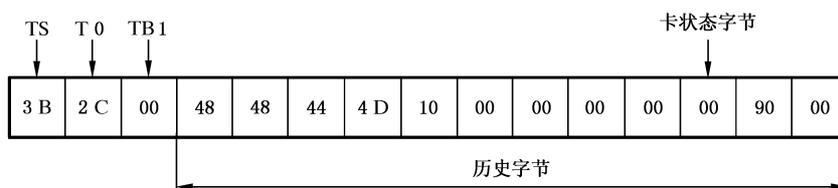


图 6 代码证 IC 卡复位应答结构

初始字符(TS)——“3B”,代码证 IC 卡使用正向的逻辑约定,即 I/O 线上的 H 状态(高电平)等价于逻辑“1”,且起始位之后发送的 8 个数据的低位在前。

格式字符(T0)——“YX”,前半字节“Y”可以为“7”“6”或“2”。

“7”表明后续存在接口字符 TA1、TB1 及 TC1;“6”表明后续存在接口字符 TB1 和 TC1;“2”则表明后续只存在接口字符 TB1。后半字节“X”指明接口字符后面历史字节的个数,代码证 IC 卡不限定其取值及历史字节的含义。

接口字符(TA1)指明位定义中的参数 F 和 D,具体说明参见 GB/T 16649.3。若复位应答字符中没有 TA1,则终端应按 F=372,D=1 作处理。

接口字符(TB1)指明 PI1 和 II 的值,具体说明参见 GB/T 16649.3。若复位应答字符中没有 TB1,则终端应按 TB1=00 作处理。

接口字符(TC1)指明字符帧传送间的额外保护时间,其取值及意义参见 GB/T 16649.3。若复位应答字符中没有 TC1,则终端应按 TC1=00 作处理。

4.5 传输协议

代码证 IC 卡支持 $T=0$ 协议。协议根据以下层次模型定义:

- 物理层,定义了位交换。
- 数据链路层,包含如下内容:
 - 字符帧,定义了字符交换;
 - $T=0$ 时的字符交换;
 - $T=0$ 时的检错与纠错。
- 传输层,定义了面向应用的信息传输。
- 应用层,根据应用协议,定义信息交换。

4.5.1 物理层

$T=0$ 协议使用第 4.3 中的物理层定义。

4.5.2 数据链路层

4.5.2.1 字符帧

在 4.3.2 中定义的字符帧适用于所有在 IC 卡与终端之间的信息交换。

4.5.2.2 字符协议($T=0$)

4.5.2.2.1 字符时序

终端到卡发送的两个连续字符起始位前沿之间的最小时间间隔为 12 etu。

卡到终端发送的两个连续字符起始位前沿之间的最小时间间隔为 12 etu。

卡发送字符的起始位前沿与卡或终端发送的前一个字符的起始位前沿之间的最大时间间隔应不超过 9 600 etu。

相反方向发送的两个连续字符的起始位前沿之间的最小时间间隔是 12 etu。

4.5.2.2.2 命令头

命令全部由终端应用层(TAL)初始化,它通过终端传输层(TTL)向卡发送一个由 5 个字节组成的命令头,命令头由 5 个连续字节 CLA、INS、P1、P2 和 P3 组成,如下:

- CLA 是命令类型；
- INS 是指令代码；
- P1 和 P2 包含了附加特殊参数；
- P3 指出了发送给卡的命令的数据长度或卡响应的最大数据长度(根据不同的 INS)。

这些字节和通过命令发送的数据一起构成命令传输协议数据单元(C-TPDU),映射在 C-TPDU 之上的命令应用协议数据单元(C-APDU)将在 4.5.3 中描述。

TTL 传送 5 个字节的命令头给卡,并等待一个过程字节。

4.5.2.2.3 过程字节

卡接收到命令头后,紧接着返回一个过程字节给 TTL。过程字节向 TTL 指明了下一步该做什么,如表 7 所示。

表 7 终端对过程字节的响应

序号	过程字节值	步骤
(1)	与 INS 字节相同	所有余下的数据将要由 TTL 传送或 TTL 将准备接收来自 IC 卡所剩的数据
(2)	“60”	TTL 将提供额外工作等待时间
(3)	“6X”或“9X”,除“60”之外(过程字节或状态码 SW1)	TTL 将等待下一个过程字节或状态码 SW2

注:在(1)、(2)情况中,TTL 完成动作后将等待另一个过程字节。
 在(3)情况中,第二个过程字节或状态码(SW2)被收到后,TTL 将做如下事情:
 ——如果过程字节为“61”,TTL 将发送一个最大长度(P3)为“XX”的得到响应命令(GET RESPONSE)给 IC 卡,“XX”为 SW2 的值。
 ——如果过程字节为“6C”,TTL 将立即重发前一个命令的命令头给卡,它的 P3 值用“XX”代替,“XX”是 SW2 的值。
 ——如果过程字节是“6X”(除“60”、“61”及“6C”之外)或者“9X”,TTL 将通过响应 APDU (R-APDU)返回状态码给 TAL,并等待下一个 C-APDU。

在 TTL 和卡之间交换命令和数据时,TTL 和卡都被假设知道数据的流向,以及知道 TTL 或卡哪一个正在驱动 I/O 线。

4.5.2.3 字符协议的错误检测及纠错

错误的检测和纠错是必须的。

若在字符接收中发现错误,接收器应在字符起始位的前沿之后的 (10.5 ± 0.2) etu 时,向 I/O 线发送持续 1~2 个 etu 时间的低电平信号,以指示有错误发生。

发送方应在字符起始位前沿发出后的 (11 ± 0.2) etu 处,检测 I/O 线上的电平状态,若 I/O 线上此时为高电平状态,则表明字符已准确接收到。

若发送方发现错误,就应在检出错误后至少延迟 2 个 etu,重复发送一次有错误嫌疑的字符。

4.5.3 终端传输层

4.5.3.1 C-APDU 和 R-APDU 的变换和数据交换

C-APDU 到命令头的变换取决于命令的具体情况。通过 R-APDU,由卡返回的数据(如果存在)和状态的变换取决于数据的返回长度。

由卡返回的过程字节 SW1SW2 = “61”和 SW1SW2 = “6C”用来控制卡和 TTL 之间的数据交换,而不能返回给 TAL。如果卡返回过程字节 SW1SW2 = “61”或 SW1SW2 = “6C”,则表示在卡中的处理没有完成。

如果卡返回给 TTL 的状态码是 SW1SW2 = “9000”,表示完成了命令的正常处理。由卡返回的任

何其他的状态码都指明卡没能正确完成处理,并已结束了处理过程,处理失败的原因在状态码中指明。**TTL** 收到来自卡的任何状态码(但不包括过程字节“61XX”和“6CXX”)时,都结束命令的处理,不论是正常、警告还是错误。

对卡返回的数据和状态如何变换到 **R-APDU** 的说明,仅适用于卡已完成命令处理后的情况(无论是成功处理还是其他结果)。

下面分 4 种情况讨论从 **C-APDU** 到 $T=0$ 命令头,以及从 **TTL** 状态码到 **R-APDU** 的变换。

4.5.3.2 情况 1

C-APDU 头映射到 $T=0$ 命令头的前四个字节, $T=0$ 命令头的 **P3** 置为“00”。

交换的过程如下:

- a) **TTL** 发送 $T=0$ 的命令头给卡。
- b) 卡返回状态码给 **TTL**。

完成命令处理后,由 **IC** 卡返回到 **TTL** 的状态码,不加改变地变换到 **R-APDU** 的尾部。

4.5.3.3 情况 2

C-APDU 头被映射到 $T=0$ 命令头的前四个字节,“Le”长度字节从 **C-APDU** 的条件体被映射到 $T=0$ 命令头的 **P3**。

交换过程如下:

- a) **TTL** 发送 $T=0$ 命令头到卡。
- b) 在过程字节控制下,卡给 **TTL** 返回数据和状态(在非正常处理时只返回状态)。

注:卡返回的控制过程字节为“61XX”和“6CXX”时,**TTL** 可以重发 $T=0$ 命令头和使用 **GET RESPONSE** 命令从卡取回数据。

完成命令处理后,由卡返回 **TTL** 的数据(如果存在)和状态,按下述方法变化成 **R-APDU**(其中是卡实际要返回的数据):

——如果 $Le \geq Lic$,返回的数据被映射到 **R-APDU** 的条件体,返回的状态被映射到 **R-APDU** 的尾部。

——如果 $Le < Lic$,返回数据的头 **Le** 个字节被映射到 **R-APDU** 的条件体,返回的状态被映射到 **R-APDU** 的尾部。

4.5.3.4 情况 3

C-APDU 头被映射到 $T=0$ 命令头的前四个字节,**C-APDU** 条件体的长度字节“Lc”被映射到 $T=0$ 命令头的 **P3**。

交换过程如下:

- a) **TTL** 发送 $T=0$ 命令头到 **IC** 卡。

b) 如果 **IC** 卡返回一个过程字节而没有状态码字节,则在此过程字节的控制下,**TTL** 向 **IC** 卡发送 **C-APDU** 条件体中的数据。

或如果 **IC** 卡返回状态字节 **SW1SW2**,**TTL** 将中断命令处理过程。

- c) 如果处理过程没有在步骤 b) 处中断,则 **IC** 卡返回处理命令的完成状态。

卡完成命令处理后返回给 **TTL** 的状态码,或由卡返回并引起 **TTL** 中断命令处理的状态码,都不加改变地映射到 **R-APDU**。

4.5.3.5 情况 4

C-APDU 头被映射到 $T=0$ 命令头的前四个字节,**C-APDU** 条件体的长度字节“Lc”被映射到 $T=0$ 命令头的 **P3**。

交换过程如下:

- a) **TTL** 发送 $T=0$ 命令头到 **IC** 卡。

b) 如果卡返回一个过程字节而没有状态码字节,则在此过程字节的控制下,**TTL** 向卡发送

C-APDU 条件体中的数据。

或如果卡返回状态字节 SW1SW2, TTL 将中断命令处理过程。

c) 如果处理过程没有在步骤 b) 处中断, IC 卡就返回过程字节“61XX”给 TTL, 请求 TTL 发出 GET RESPONSE 命令, 从卡取回数据。在命令处理的这个阶段中, IC 卡不会返回状态码 SW1SW2=“9000”。TTL 发送 GET PESPONSE 命令到卡取回数据, 从卡返回的过程字节“61XX”中的“XX”与 C-APDU 条件体中的“Le”字节的小者被映射到 GET PESPONSE 命令的长度字节。于是, GET RESPONSE 命令可以同上面的情况 2 命令一样处理, 在过程字节的控制下, 卡向 TTL 返回数据和状态 (仅在非正常处理时)。

完成命令处理后, 由卡返回到 TTL 的数据 (如果存在) 和状态码, 或由卡返回并引起 TTL 终止命令处理过程的状态码, 按下述规则被映射到 R-APDU (其中 Lic 是卡实际要返回的数据):

——如果 $Le \geq Lic$, 返回的数据被映射到 R-APDU 的条件体, 返回的状态被映射到 R-APDU 的尾部。

——如果 $Le < Lic$, 返回数据的头 Le 个字节被映射到 R-APDU 的条件体, 返回的状态被映射到 R-APDU 的尾部。

4.5.3.6 过程字节“61XX”和“6CXX”的使用

由卡返回到 TTL 的过程字节“61XX”和“6CXX”指明当前正在处理的命令要求以何种方式返回数据。这些过程字节仅仅用在情况 2 和情况 4 命令中。

过程字节“61XX”通知 TTL 发出 GET RESPONSE 命令到 IC 卡, GET RESPONSE 命令头的 P3 置为“XX”。

过程字节“6CXX”通知 TTL 立即重发前条命令, 命令头中的 P3 置为“XX”。

在情况 2 和情况 4 命令的无错误处理过程中, 使用过程字节的规定如下。在发生错误时, IC 卡返回错误或警告状态码而不是“61XX”或“6CXX”。

4.5.3.6.1 情况 2 命令

如果卡收到一条情况 2 命令头并且 $Le \neq Lic$, 卡应返回过程字节“6CLic”(或一个指出警告或错误情况的状态码, 但不能是 SW1SW2=“9000”), 使用 P3=Lic 立即重发命令头。

注: 这对 GET RESPONSE 命令也是有效的。

如果卡收到情况 2 命令头并且 $Le = Lic$, 在过程字节控制下, 卡返回被请求的数据和相关状态码, 或者返回过程字节“61XX”(或指出警告或错误情况的状态码, 但不能是 SW1SW2=“9000”), 通知 TTL 按最大长度“XX”发出 GET RESPONSE 命令。

4.5.3.6.2 情况 4 命令

如果卡收到一个情况 4 命令, 处理完随 C-APDU 命令一同发送来的数据之后, 应返回状态码“61XX”(或指出警告或错误情况的状态码, 但不能是 SW1SW2=“9000”), 通知 TTL 按最大长度“XX”发出 GET RESPONSE 命令。

4.5.3.7 GET RESPONSE 命令

TTL 发出 GET RESPONSE 命令后, 从卡得到数据, 这些数据与情况 2 和情况 4 下的 C-APDU 的 Le 字节相对应。命令信息结构如表 8 所示。

表 8 GET RESPONSE 命令信息结构

CLA	“00”
INS	“C0”
P1	“00”
P2	“00”
E	预期数据的最大长度

正常处理结束后,卡返回 **Lic** 字节的数据和状态码 **SW1SW2**="9000"。

在错误情况发生时,错误状态码(**SW1SW2**)的编码见表 9。

表 9 GET RESPONSE 命令错误情况

SW1SW2	含 义
"6CXX"	Le 错误,重发

4.5.4 应用层

应用层交换的每一步包含命令响应对,其 **TAL** 通过 **TTL** 给卡发送命令,卡处理该命令后通过返回一个响应给 **TAL**,一个特定的命令都与一个特定的响应相匹配。一个 **APDU** 被定义为一个命令信息或一个响应信息。

命令信息和响应信息都可以包含数据,传输协议通过 **TTL** 来管理表 10 中的四种情况:

表 10 APDU 中数据情况的定义

情 况	命 令 数 据	响 应 数 据
1	无	无
2	无	有
3	有	无
4	有	有

4.5.4.1 C-APDU

C-APDU 包含一个连续 4 字节的命令头,用 **CLA**、**INS**、**P1** 和 **P2** 以及一个可变长度的条件体来表示。

命令头定义如下:

——**CLA**:指令类别,除“**FF**”外可赋任何值。

——**INS**:在指令类别中的指令码,当最低位是“0”,并且高位半字节既不是“6”也不是“9”时,**INS** 才有效。

——**P1**、**P2**:完成 **INS** 的参数字节。

注:每一个命令头的全部编码参见 5.3。

条件体定义如下:

——**Lc** 占一个字节,在 **APDU** 中定义为发送数据的字节数,**Lc** 的取值范围从 1~255。

——将要发送的 **C-APDU** 数据域,字节数由 **Lc** 定义。

——**Le** 占一个字节,指出 **R-APDU** 中预期的数据最大字节数。**Le** 的取值范围从 0~255。

如果 **Le**=0,预期数据字节的最大长度是 256。

可能的 **C-APDU** 结构的四种情况见表 11:

表 11 C-APDU 结构

情 况	结 构
1	CLA INS P1 P2
2	CLA INS P1 P2 Le
3	CLA INS P1 P2 Lc Data
4	CLA INS P1 P2 Lc Data Le

4.5.4.2 R-APDU

R-APDU 是一串字符,这一串字符由一个条件体和两个字节状态码 **SW1 SW2** 组成。

条件体是一个数据块,其最大长度由 **C-APDU** 中的 **Le** 决定。结尾部分标明卡在处理命令后的

状态。

SW1 SW2 的编码遵循下述规定：

- SW1 的高位半字节是“6”或“9”。
- 禁止 SW1 的值为“60”。
- SW1 的值为“61”或“6C”时,应作为一个错误来处理。
- SW1 SW2 的值为“9000”时,表示命令正常结束。
- 当 SW1 的高位半字节为“9”,并且低位半字节不为“0”时,表示应用特有的状态。
- 当 SW1 的高位半字节为“6”,并且低位半字节不为“0”时,表示 SW1 是与应用无关的状态。

SW1 和 SW2 的其他值(在“6X”和“9X”范围内,除了上面说明的这些数值之外)所代表的含义参见

5.3。

4.6 代码证 IC 卡的外形尺寸和页面式样

单位: mm

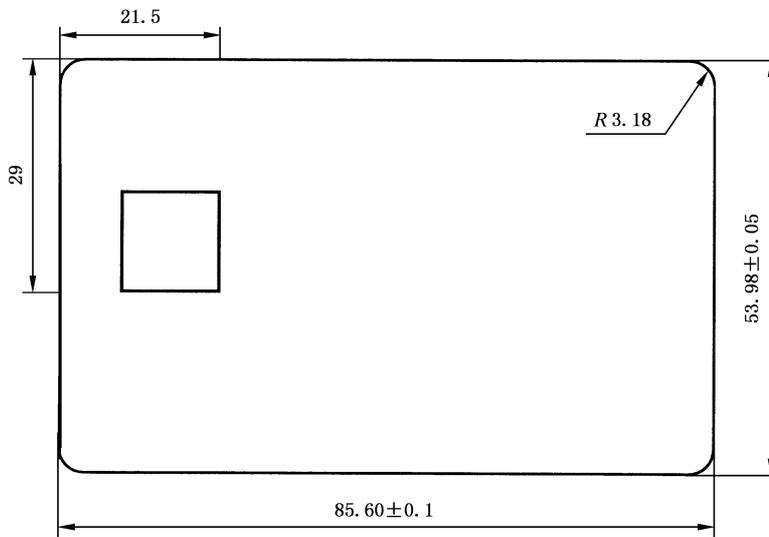


图 7 代码证 IC 卡外形尺寸

单位: mm

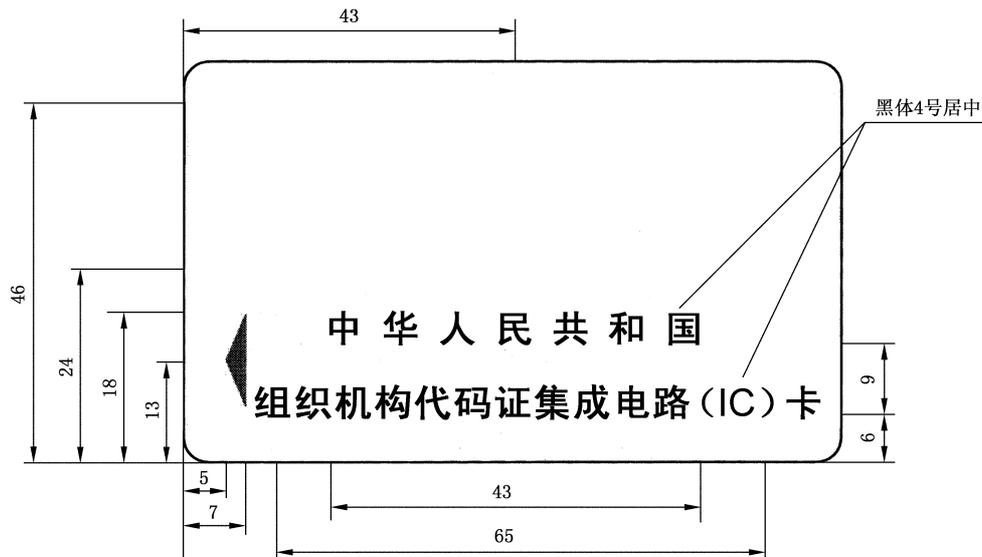


图 8 代码证 IC 卡正面式样

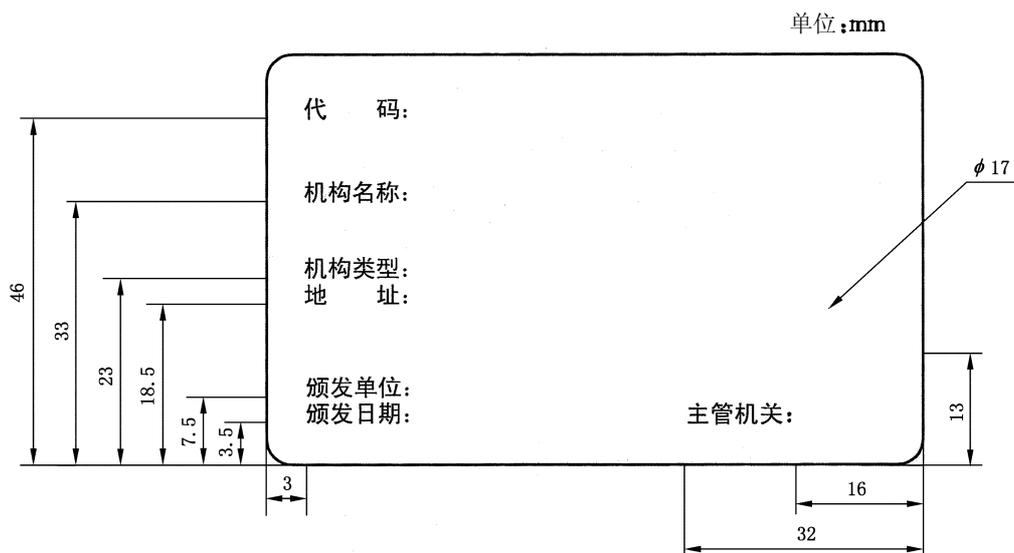


图 9 代码证 IC 卡背面式样

5 代码证 IC 卡应用

5.1 数据项

代码证 IC 卡所定义的数据项如表 12 所示。

表 12 代码证 IC 卡数据项

序号	名称	格式	长度(字节)	备注
1	机构代码	an	9	参照 GB 11714—1997
2	机构名称	an	70	
3	机构地址	an	70	
4	机构类型代码	b	1	
5	机构类型	an	16	
6	法人代表或负责人姓名	an	20	
7	法人代表或负责人身份证号	an	18	
8	经济类型代码	b	2	
9	经济类型	an	40	
10	批准文号或注册号	an	26	
11	注册资金	an	6	
12	货币种类代码	b	3	参照 GB/T 12406—1996
13	货币种类	an	8	
14	外方投资机构国别或地区代码	b	3	参照 GB/T 2659—2000
15	外方投资机构国别或地区	an	24	
16	行政区划代码	an	6	参照 GB/T 2260—1999
17	邮政编码	an	6	
18	电话号码	an	16	

表 12(完)

序号	名称	格式	长度(字节)	备注
19	颁发日期	an	8	参照 GB/T 7408—1994
20	颁发单位名称	an	70	
21	年检日期	an	8	参照 GB/T 7408—1994
22	年检期限	an	8	参照 GB/T 7408—1994

注：an——字母或数字；b——二进制(下同)。

5.2 文件

5.2.1 文件结构

代码证 IC 卡的文件结构符合 ISO 7816-4 的有关规定。采用树状层次结构。

代码证 IC 卡应用起始于一个专用文件(DF)。该专用文件的上一层是主控文件(MF)，下一层是代码证 IC 卡应用定义的基本数据文件(EF)。

代码证 IC 卡所对应的专用文件(DF)和其下属的基本数据文件构成了一个树状结构的分支。该专用文件是其下属的基本数据文件的入口点。

代码证 IC 卡的文件结构如图 10 所示。

全国组织机构代码统一社会信用代码数据服务中心
<https://www.cods.org.cn>

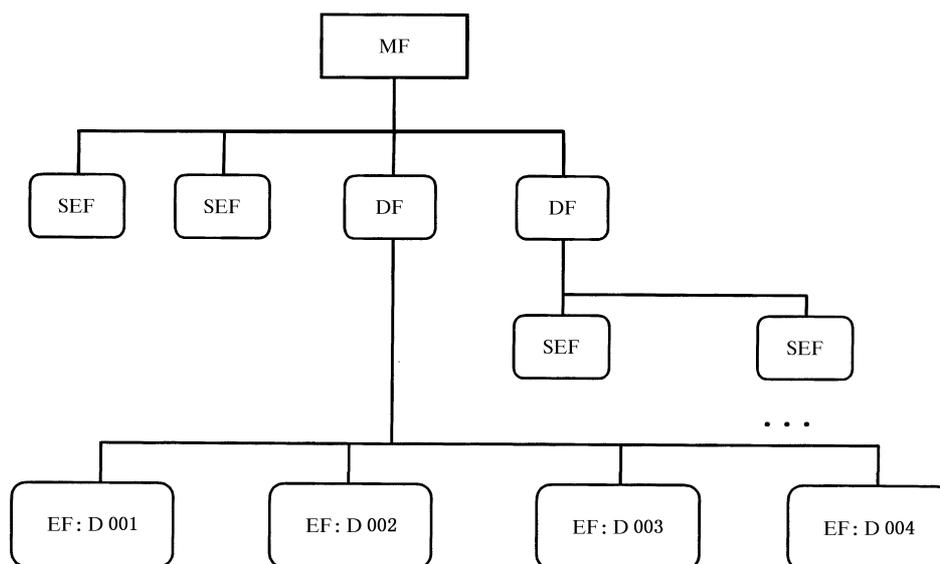


图 10 代码证 IC 卡的文件结构

5.2.2 代码证 IC 卡应用数据文件

代码证 IC 卡应用的基本数据文件使用线性变长记录类型结构。

在代码证 IC 卡应用下定义了四个基本数据文件：

- 发卡机构数据文件见表 13；
- 代码基本信息数据文件见表 14；
- 代码扩展信息数据文件见表 15；
- 代码年检信息数据文件见表 16。

表 13 发卡机构数据文件

文件标识符	D0 01	文件类型	线性变长
文件读控制	自由	文件写控制	AM ___ KEY
记录号	数据项	类型	长度(字节)
1	卡流水号	an	12
2	规范版本	b	1
3	应用版本	b	1
4	初始化日期	an	8
5	初始化机构编码	b	1
6	发卡机构标识号	an	10

表 14 代码基本信息数据文件

文件标识符	D0 02	文件类型	线性变长
文件读控制	自由	文件写控制	AM ___ KEY/AM2 ___ KEY
记录号	数据项	类型	长度(字节)
1	机构代码	an	9
2	机构名称	an	70
3	机构地址	an	70
4	机构类型	an	16
5	机构类型代码	b	1
6	颁发单位名称	an	70
7	颁发日期	an	8

表 15 代码扩展信息数据文件

文件标识符	D0 03	文件类型	线性变长
文件读控制	自由	文件写控制	AM3 ___ KEY/AM2 ___ KEY
记录号	数据项	类型	长度(字节)
1	法人代表或负责人姓名	an	20
2	经济类型代码	b	2
3	经济类型	an	40
4	批准文号或注册号	an	26
5	注册资金(万元)	an	6
6	货币种类代码	b	3
7	货币种类	an	8
8	外方投资机构国别或地区代码	b	3
9	外方投资机构国别或地区	an	24
10	行政区划代码	an	6
11	邮政编码	an	6
12	电话号码	an	16
13	法人或负责人身份证号	an	18

表 16 代码年检信息数据文件

文件标识符	D0 04	文件类型	线性变长
文件读控制	自由	文件写控制	AM3 ____ KEY/AM2 ____ KEY
记录号	数据项	类型	长度(字节)
1	年检日期	an	8
2	年检期限	an	8

5.2.3 文件选择

代码证 IC 卡应用采用应用标识符(AID)方式进行选择。成功选择了代码证 IC 卡应用对应的专用文件后,该专用文件被置为当前专用文件,并允许使用本标准定义的命令对其进行操作。

基本数据文件采用文件标识符方式进行选择,在对基本数据文件进行存取操作前,必须首先选择它,在成功地选择了某基本数据文件后,该文件被置为当前文件,后续的记录操作命令都将针对此文件进行,直到其他的基本数据文件被选择。

5.3 命令

代码证 IC 卡的卡操作系统规定使用 CNOC-COS。

本标准只列出了命令的定义,命令的详细说明参见“CNOC-COS 用户手册”。

5.3.1 命令 APDU 格式

命令 APDU 的格式如表 17 所示,表 18 解释了 APDU 中参数的内容。

表 17 命令 APDU 格式

CLA	INS	P1	P2	Lc	Data	Le
------------	------------	-----------	-----------	-----------	-------------	-----------

表 18 命令 APDU 的内容

参 数	名 称	长度(字节)	描 述
CLA	类型	1	指令类型
INS	代码	1	指令代码
P1	参数	1	指令参数 1
P2	参数	1	指令参数 2
Lc	长度	1	命令 APDU 中 Data 域的字节长度(1~255)
Data	数据	=Lc	输入卡的数据字节串
Le	长度	1	期望从卡返回的数据字节的长度(1~256)

命令 APDU 中“CLA”的含义见表 19。

表 19 CLA 的含义

b7	b6	b5	b4	b3	b2	b1	b0	含 义
0	0	0	0	0	0	0	0	标准命令
1	0	0	0	0	0	0	0	扩展命令

5.3.2 响应 APDU 格式

响应 APDU 的格式如表 20。

表 20 响应 APDU

DATA	SW1	SW2
-------------	------------	------------

表 21 解释了表 20 中参数的含义。

表 21 响应 APDU 的含义

参 数	名 称	长度(字节)	描 述
DATA	数据	=Le	卡返回的数据字节
SW1	状态字节 1	1	命令执行的状态
SW2	状态字节 2	1	命令执行状态的说明

5.3.3 命令列表

COS 应包含的最小指令集如表 22 所示。

表 22 命令列表

序 号	命 令	CLA	INS	P1	P2
1	SELECT FILE	00	A4	0X	0C
2	INTERNAL AUTHENTICATE	00	88	00	XX
3	GET RANDOM	00	84	00	00
4	EXTERNAL AUTHENTICATE	00	82	00	XX
5	UPDATE RECORD	00	DC	XX	04
6	READ RECORD	00	B2	XX	04
7	GET RESPONSE	00	C0	00	00
8	APPLICATION BLOCK	80	C4	01	00
9	APPLICATION UNBLOCK	80	C6	01	00
10	CARD BLOCK	80	EC	42	4B
11	APPEND RECORD	00	E2	00	00

注：CLA,INS,P1,P2 栏中的数据均为十六进制格式；XX 为可变的十六进制数。

5.3.4 APPLICATION BLOCK 应用锁定

5.3.4.1 功能描述

该命令锁定指定的应用。

该命令执行前,必须通过 MF 下主控密钥的认证。

5.3.4.2 命令格式

命令格式如表 23。

表 23 应用锁定命令 APDU

代 码	值
CLA	80
INS	C4
P1	01
P2	00
Lc	01~10 应用名称长度
Data	应用名称
Le	不存在

5.3.4.3 响应格式

状态字节的含义如表 24。

表 24 应用锁定响应 APDU

SW1	SW2	含 义
90	00	命令执行正常
65	81	写 EEPROM 失败
69	82	安全状态不满足
69	85	使用条件不满足,必须在 MF 下才能锁定应用
6A	82	指定的应用不存在
6A	86	P1~P2 参数错误
6A	87	输入数据的长度与 P1~P2 不匹配

5.3.5 APPLICATION UNBLOCK 应用解锁

全国组织机构代码统一社会信用代码数据服务中心
<https://www.cods.org.cn>

5.3.5.1 功能描述

该命令是 **APPLICATION BLOCK** 命令的逆过程,它恢复被锁定的应用(**DF**)。

该命令执行前,必须通过 **MF** 下主控密钥的认证。

5.3.5.2 命令格式

命令格式如表 25。

表 25 应用解锁命令 APDU

代 码	值
CLA	80
INS	C6
P1	01
P2	00
Lc	01~10 应用名称长度
Data	应用名称
Le	不存在

5.3.5.3 响应格式

响应格式状态字节的含义如表 26。

表 26 应用解锁响应 APDU

SW1	SW2	含 义
90	00	命令执行正常
65	81	写 EEPROM 失败
69	82	安全状态不满足
69	85	使用条件不满足,必须在 MF 下才能恢复应用 DF
6A	82	指定的应用不存在
6A	86	P1~P2 参数错误
6A	87	输入数据的长度与 P1~P2 不匹配

5.3.6 CARD BLOCK 卡片锁定

5.3.6.1 功能描述

该命令永久性地锁定卡片。用于逻辑销毁卡片。

该命令执行前,必须通过卡片锁定密钥的认证。

5.3.6.2 命令格式

命令格式如表 27。

表 27 卡片锁定命令 APDU

代 码	值
CLA	80
INS	EC
P1	42
P2	4B
Lc	不存在
Data	不存在
Le	不存在

5.3.6.3 响应格式

响应格式状态字节的含义如表 28。

表 28 卡片锁定响应 APDU

SW1	SW2	含 义
90	00	命令执行正常
65	81	写 EEPROM 失败
69	82	安全状态不满足
69	86	命令的使用条件不满足(未初始化)
6A	86	P1~P2 参数错误

5.3.7 EXTERNAL AUTHENTICATE 外部认证

5.3.7.1 功能描述

接口设备通过命令 GET RANDOM 申请 64 位(8 个字节)的随机数,然后使用加密算法和相应密钥对随机数做解密处理,该命令将处理结果传送给卡,卡使用同样的密钥对命令传送的结果做加密计算,通过比较还原的随机数与前一条 GET RANDOM 命令所产生的随机数(保留)的一致性来验证外部密钥的正确性。

5.3.7.2 命令格式

命令格式如表 29。

表 29 外部认证命令 APDU

代 码	值
CLA	00
INS	82
P1	00
P2	密钥标识
Lc	08
Data	8 个字节的验证数据
Le	不存在

5.3.7.3 响应格式

响应格式状态字节的含义如表 30。

表 30 外部认证响应 APDU

SW1	SW2	含 义
90	00	命令执行正常
63	CX	密钥验证错误(“X”指示还可重试的次数 0~F)
65	81	写 EEPROM 失败
67	00	长度错误(Lc 不正确)
69	81	命令与文件类型不匹配(非密钥文件)
69	84	密钥失效
6A	86	P1~P2 参数错误
6A	88	指定的安全文件不存在

5.3.8 GET RANDOM 读取随机数

5.3.8.1 功能描述

接口设备向卡申请一个 8 字节的随机数。

5.3.8.2 命令格式

命令格式如表 31。

表 31 读取随机数命令 APDU

代 码	值
CLA	00
INS	84
P1	00
P2	00
Lc	不存在
Data	不存在
Le	08

5.3.8.3 响应格式

命令格式状态字节的含义如表 32。

表 32 读取随机数响应 APDU

SW1	SW2	含 义
90	00	命令执行正常
67	00	长度错误(Le 不正确)
6A	86	P1~P2 参数错误

5.3.9 GET RESPONSE 读取响应

5.3.9.1 功能描述

该命令是一条传输指令,可以从卡返回指定长度的数据。

5.3.9.2 命令格式

命令格式如表 33。

表 33 读取响应命令 APDU

代 码	值
CLA	00
INS	C0
P1	00
P2	00
Lc	不存在
Data	不存在
Le	期望卡返回的响应数据的长度

5.3.9.3 响应格式

响应格式状态字节的含义如表 34。

表 34 读取响应命令 APDU

SW1	SW2	含 义
90	00	命令执行正常
6C	XX	Le 错,“XX”指示正确的长度

5.3.10 INTERNAL AUTHENTICATE 内部认证

5.3.10.1 功能描述

接口设备产生一个 64 位的随机数作为输入数据,卡将由加密算法和指定密钥对其进行解密计算的结果作为响应数据返回给接口设备,由接口设备认证该数据。

5.3.10.2 命令格式

命令格式如表 35。

表 35 内部认证命令 APDU

代 码	值
CLA	00
INS	88
P1	00
P2	00
Lc	08
Data	8 个字节的随机数
Le	08

5.3.10.3 响应格式

响应格式状态字节的含义如表 36。

表 36 内部认证响应 APDU

SW1	SW2	含 义
90	00	命令执行正常
67	00	长度错误(Lc 不正确)
69	81	命令的使用与安全基本文件的类型不匹配
6A	86	P1~P2 参数错误
6A	88	指定的安全文件不存在

5.3.11 READ RECORD 读取记录**5.3.11.1** 功能描述

读取当前工作基本文件中的指定记录。

该命令执行前,必须成功地通过文件读取权限的认证。

5.3.11.2 命令格式

命令格式如表 37。

表 37 读取记录命令 APDU

代 码	值
CLA	00
INS	B2
P1	被读记录号
P2	04
Lc	不存在
Data	不存在
Le	期望返回的记录长度

5.3.11.3 响应格式

响应格式状态字节的含义如表 38。

表 38 读取记录响应 APDU

SW1	SW2	含 义
90	00	命令执行正常
69	81	命令与文件组织不匹配
69	82	安全状态不满足
69	86	命令不允许(未选择当前工作基本文件)
6A	83	指定的记录不存在
6A	86	P1~P2 参数错误
6C	XX	Le 不对(“ XX ”指示正确的长度)

5.3.12 SELECT FILE 选择文件**5.3.12.1** 功能描述

a) 该命令选择一个文件作为当前文件,此后的所有命令都隐含地针对当前文件操作。

b) 通过选择主控文件或由文件名指定的专用文件设定当前专用文件。

c) 在设定了当前专用文件后,可由文件标识符选择该专用文件所包含的某个工作基本文件作为当前的工作基本文件。

d) 可根据需要返回文件控制参数等文件属性。

e) 复位应答后,主控文件(MF)被缺省设置为当前专用文件。

5.3.12.2 命令格式

命令格式如表 39。

表 39 选择文件命令 APDU

代 码	值
CLA	00
INS	A4
P1	00 选择主控文件(MF) 02 选择当前 DF(MF)下的 EF 04 选择应用(DF)
P2	00 历史上规定的 0C 依然有效
Lc	文件名称/标识符长度
Data	文件名称/标识符
Le	期望返回信息的长度

5.3.12.3 响应格式

响应格式状态字节的含义如表 40。

表 40 选择文件响应 APDU

SW1	SW2	含 义
90	00	命令执行正常
61	XX	命令正常执行,并指出还有“XX”个字节需要返回
67	00	Lc 长度错误
6A	82	选择的文件不存在
6A	86	P1~P2 参数错误
6A	87	Lc 与 P1~P2 不匹配
6C	XX	Le 错,“XX”指示返回数据的正确长度

5.3.13 UPDATE RECORD 修改记录

5.3.13.1 功能描述

对记录结构的工作基本文件中已提交的记录进行修改。

修改记录前,必须已经满足文件写权限的要求。

5.3.13.2 命令格式

命令格式如表 41。

表 41 修改记录命令 APDU

代 码	值
CLA	00
INS	DC
P1	被修改记录号
P2	04
Lc	数据长度
Data	输入的数据字节
Le	不存在

5.3.13.3 响应格式

响应格式状态字节的含义如表 42。

表 42 修改记录响应 APDU

SW1	SW2	含 义
90	00	命令执行正常
63	CX	重试“X”次后,写 EEPROM 成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	命令与文件组织不匹配
69	82	安全状态不满足
69	86	命令不允许(未选择当前文件)
6A	83	指定的记录不存在
6A	85	Lc 与指定修改的记录长度不匹配
6A	86	P1~P2 参数错误

5.3.14 APPEND RECORD 增加记录

5.3.14.1 功能描述

对记录格式的工作基本文件添加新的记录,记录序号自动加一。

5.3.14.2 命令格式

命令格式如表 43。

表 43 增加记录命令 APDU

代 码	值
CLA	00
INS	E2
P1	00
P2	00
Lc	写入记录的长度
Data	欲添加的记录
Le	不存在

5.3.14.3 响应格式

响应格式状态字节的含义如表 44 所示。

表 44 增加记录响应 APDU

SW1	SW2	含 义
90	00	命令执行正常
63	CX	重试“X”次后,写 EEPROM 成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	命令与文件组织不匹配
69	82	安全状态不满足
69	86	命令不允许(未选择当前工作基本文件)
6A	84	文件中没有足够的空间

表 44(完)

SW1	SW2	含 义
6A	85	Lc 与文件组织类型不匹配
6A	86	P1~P2 参数错误

5.4 多应用的支持

代码证 IC 卡支持多应用功能,允许非代码证 IC 卡应用存在,这些应用(如果存在)在文件的树状结构中,与代码证 IC 卡应用处于同一层次。存在于卡中的这些应用,唯一地通过应用标识符加以区分。

5.4.1 应用标识符的编码

应用标识符(AID)的结构符合 ISO 7816-5 的有关规定,它包括两个部分:

一个经过注册的应用提供者标识符,长度为 5 个字节,它唯一地标识应用提供者。

一个可选域,由应用提供者定义,最长为 11 个字节。这个域被称为“专用应用标识符扩展码”,其值由应用提供者确定。

全国组织机构代码统一社会信用代码数据服务中心
<https://www.cods.org.cn>

代码证 IC 卡的应用标识符是:D156000001

5.4.2 代码证 IC 卡应用流程

a) 卡片插入

卡片在插入接口设备后,接口设备应能检测到卡片的插入,然后按照 4.2 的规定给卡加电和信号。

b) 终端接收复位应答

复位结束后,代码证 IC 卡返回复位应答信息,其结构应符合 4.4 关于复位应答的规定。对于不满足此结构的卡片的处理,不在本标准中规定。

c) 选择应用

复位通过后,终端直接进行应用选择。被选择的应用可以是代码证 IC 卡应用,也可以不是。对于非代码证 IC 卡应用的后续处理,不在本标准中规定。

d) 选择并读取发卡机构基本数据文件

代码证 IC 卡应用选择成功后,终端应首先选择并读取发卡机构基本数据文件的内容,以取得卡片的基本信息。

e) 选择并读取代码基本数据文件。

f) 读取代码扩展数据文件,如果不打算读取代码扩展数据文件,则结束操作。

5.5 安全机制

5.5.1 应用共存

为了独立地管理一张卡上不同应用间的安全问题,每一个应用应该放在一个单独的 DF 中。各应用之间应有能力防止跨应用的非法访问。另外,每一个应用也不应该与个人化要求和卡中共存的其他应用规则发生冲突。

5.5.2 密钥管理和使用

代码证 IC 卡应用维护和使用四个密钥,如表 45。

表 45 代码证 IC 卡密钥

密 钥	说 明	产 生
AM_Key	代码证 IC 卡应用主控密钥,用于在代码证 IC 卡应用中建立所有文件	由发卡方通过使用主控密钥,利用分散算法产生
AM2_Key	代码证 IC 卡应用分控密钥,用于修改代码基本数据文件和代码扩展数据文件以及年检数据文件	

表 45(完)

密 钥	说 明	产 生
AM3_Key	代码证 IC 卡应用分控密钥,用于修改代码扩展数据文件和年检数据文件	由发卡方通过使用主控密钥,利用分散算法产生
AY_Key	验证密钥,用于确认 IC 卡的真伪	

代码证 IC 卡应用所使用的卡,由国家代码管理机构统一发行,发卡机构维护和使用两个密钥,如表 46 所示。

表 46 发卡机构密钥

密 钥	说 明
IS_Key	发卡方主控密钥,用于建立代码证 IC 卡应用 DF。并负责建立该应用中的密钥
IS2_Key	非代码证 IC 卡应用 DF 建立密钥

5.5.3 文件操作的安全认证

在代码证 IC 卡应用中,安全认证的方法如下:

- a) 使用 **GET RANDOM** 命令,从卡中取得 8 字节的随机数。
- b) 终端将此随机数作加密处理,将结果通过 **EXTERNAL AUTHENTICATE** 命令传送给卡。
- c) 卡经分析认证后,将认证结果通知接口设备。
- d) 接口设备根据卡的认证结果,决定后续操作。

5.5.4 代码证 IC 卡应用密钥的分散算法

密钥的分散算法将按规定的算法产生。

设卡流水号为 x_1 ,规范版本为 x_2 ,应用版本为 x_3 ,初始化日期为 x_4 ,初始化编码为 x_5 , $y = f(x_1, x_2, x_3, x_4, x_5)$ 。 y 的长度为 8 个字节。

由主控密钥和 y 通过 **DEA** 分散为相应的应用密钥。