

社会保障（个人）卡规范

第 2 部分：机电特性、逻辑接口与传输协议

引言

本部分作为《社会保障（个人）卡规范》的第 2 部分，包括以下主要内容：

——基本物理特性。定义了社会保障卡的物理特性、触点尺寸和位置等。

——电气特性。定义了各触点的电气特性，包括工作电压、工作电流、驱动能力等。

——传输协议。定义了接口设备启动的命令的结构和处理，这些命令用于传输控制及半双工异步传输协议的特定控制。

1 适用范围

本规范适用于人力资源和社会保障领域面向各类参保人员发行的社会保障卡。其使用对象主要是与社会保障卡应用相关的卡片设计、制造、管理、发行和受理以及应用系统的研制、开发、集成和维护等组织机构。

2 参考标准

GB/T 16649. 1—2006	识别卡 带触点的集成电路卡 第 1 部分：物理特性 (ISO/IEC 7816-1: 1998)
GB/T 16649. 2—2006	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: 1999)
GB/T 16649. 3—2006	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: 1997)
GB/T 5095. 2—1997	电子设备机电元件 基本试验规程及测量方法 第 2 部分：一般检查、电连续性和接触电阻测试、绝缘试验和电压应力试验（IEC 60512-2: 1994）
GB/T 17554. 1—2006	识别卡 测试方法 第 1 部分：一般特性测试 (ISO/IEC 10373-1: 1998)
GB/T 17554. 3—2006	识别卡 测试方法 第 3 部分：带触点的集成电路卡及其相关接口设备（ISO/IEC 10373-3: 2001）
ISO/IEC 7816-3: 1997	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 10373-3: 2001	识别卡 测试方法 第 3 部分：带触点的集成电路卡及其相关接口设备
GB/T 14916—2006	识别卡 物理特性 (ISO/IEC 7810: 2003)
JR/T 0025.7	中国金融集成电路（IC）卡规范 第 11 部分：非接触式 IC 卡通讯规范
JR/T 0025.3	中国金融集成电路（IC）卡规范 第 3 部分：与应用无

3 定义

以下定义适用于本规范。

3.1 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。

3.2 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。

3.3 接口设备(Interface Device)

终端上插入 IC 卡的部分, 包括其中的机械、电气和逻辑控制部分。

3.4 终端(Terminal)

为处理社会保障卡业务而在服务网点安装的设备, 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, 例如与主机通信的接口。

3.5 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。

3.6 连接(Concatenation)

两个元素的连接是指将第二个元素附加到第一个元素的末尾。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, 即第一个与第二个相连, 再与第三个相连, ..., 依次类推。

3.7 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。

3.8 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。

3.9 交易(Transaction)

持卡者和业务、管理部门之间根据社会保障卡所支持的应用接受、提供服务的行为。

3.10 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。

3.11 保护时间(Guardtime)

同一方向发送的前一个字符奇偶位后沿和后一个字符起始位前沿之间的最小时间。

3.12 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 0.4V 时, 则称电源电压和这些信号处于静止状态。

3.13 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。

3.14 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/IEC 7810、ISO/IEC 7811 第 1 至第 5 部分、ISO/IEC 7812 和 ISO/IEC 7813 中描述的）。

3.15 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。

3.16 半字节(Nibble)

一个字节的高四位或低四位。

3.17 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’。

3.18 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’。

3.19 T=0

面向字符的异步半双工传输协议。

3.20 T=1

面向块的异步半双工传输协议。

3.21 T=15

不是传输协议，而是特指其后所传输字符的属性为全局接口字符。

3.22 类型 ABC (Class ABC)

卡片和终端支持的供电电压值类型。有三种可以支持的供电电压类型：类型 A=5.0 伏，类型 B=3.0 伏，类型 C=1.8 伏。卡片和终端可以支持其中的一种，也可以支持连续的两种或两种以上的供电电压，如 AB、ABC。

3.23 翘曲 warpage

相对平面的偏离。

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。

APDU	应用协议数据单元(Application Protocol Data Unit)
ATR	复位应答(Answer to Reset)
b	二进制(Binary)
C-APDU	命令 APDU(Command APDU)
CIN	输入电容(Input Capacitance)
COUT	输出电容(Output Capacitance)
CLA	命令报文的类别字节(Class Byte of the Command Message)
CLK	时钟(Clock)
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)
etu	基本时间单元(Elementary Time Unit)
f	频率(Frequency)

GND	地(Ground)
hex	十六进制数(Hexadecimal)
IC	集成电路(Integrated Circuit)
ICC	集成电路卡(Integrated Circuit Card)
ICC	VCC 上的电流(Current at VCC)
IEC	国际电工委员会(International Electrotechnical Commission)
IFD	接口设备(Interface Device)
IIH	高电平输入电流(High Level Input Current)
IIL	低电平输入电流(Low Level Input Current)
INS	命令报文的指令字节(Instruction Byte of Command Message)
I/O	输入/输出(Input/Output)
IOH	高电平输出电流(High Level Output Current)
IOL	低电平输出电流(Low Level Output Current)
ISO	国际标准化组织(International Organization for Standardization)
Lc	终端发出的命令数据的实际长度 (Exact Length of Data Sent by the TAL in aCase 3 or 4 Command)
Le	响应数据的最大期望长度 (Maximum Length of Data Expected by the TAL in Response to a Case 2 or 4 Command)
Licc	IC 卡回送的可用数据的实际长度(Exact Length of Data Available in the ICC to be Returned in Response to the Case 2 or 4 Command Received by the ICC)
LEN	长度(Length)
P1	参数 1(Parameter 1)
P2	参数 2(Parameter 2)
P3	参数 3(Parameter 3)
PIN	个人密码(Personal Identification Number)
PTS	协议类型选择(Protocol Type Selection)
R-APDU	响应 APDU(Response APDU)
RFU	保留为将来使用(Reserved for Future Use)
RST	复位(Reset)
R-TPDU	响应 TPDU(Response TPDU)
SW1	状态码 1(Status Word One)
SW2	状态码 2(Status Word Two)
TAL	终端应用层 (Terminal Application Layer)
tR	信号幅度从 10% 上升到 90% 的时间 (Rise Time from 10% to 90% of Signal Amplitude)
tF	信号幅度从 90% 下降到 10% 的时间(Fall Time from 90% to 10% of Signal Amplitude)

TPDU	传输协议数据单元(Transport Protocol Data Unit)
tR	信号幅度从 10% 上升到 90% 的时间(Rise Time Between 10% and 90% of Signal Amplitude)
VCC	VCC 触点上测量到的电压 (Voltage Measured on VCC Contact)
VCC	电源电压(Supply Voltage)
VIH	高电平输入电压(High Level Input Voltage)
VIL	低电平输入电压(Low Level Input Voltage)
VOH	高电平输出电压(High Level Output Voltage)
VOL	低电平输出电压(Low Level Output Voltage)
VPP	VPP 触点上测量到的编程电压(Programming Voltage Measured on VPP Contact)
VPP	编程电压(Programming Voltage)
WI	等待时间整数(Waiting Time Integer)
‘0’-‘9’ ‘A’-‘F’	十六进制数字
xx	任意值

5 机电接口

本节包括 IC 卡的电气、机械特性。IC 卡和终端的标准指标有所不同，其目的是为防止对 IC 卡的损坏而预留安全余地。

本节定义的 IC 卡特性遵从 ISO/IEC 7816 系列标准，并依据实际需要与技术发展，作了一些细小变动。

5.1 机械特性

本节描述了 IC 卡的物理特性、触点的尺寸和位置、触点的分配。

5.1.1 物理特性

除本节的特殊规定外，IC 卡应满足 GB/T 16649.1 中有关物理特性，如紫外线、X 射线、机械强度、电磁场的要求。

GB/T16649.1 中与凸印有关的要求不适用于本规范。

5.1.1.1 翘曲值

翘曲值 $\leq 1.50\text{mm}$ 。

5.1.1.2 温湿度条件下的尺寸稳定性和翘曲值

将卡依次置于下列环境下各 60 分钟：

- (1) $-35^{\circ}\text{C} \pm 3^{\circ}\text{C}$ ；
- (2) $50^{\circ}\text{C} \pm 3^{\circ}\text{C}$ ，相对湿度 $95\% \pm 5\%$ ；

将卡取出，放在实验室环境条件下保持 24 小时，再测卡片尺寸及卡片翘曲，要求卡片能正常使用，且尺寸值和最大翘曲值的测量的结果应与原测量值一致。

5.1.1.3 卡片表层剥离强度

测量角度为 90 度，取样为 10.00mm 宽，取最低值，卡片的层间剥离强度值应：

——照片区域 $\geq 3.5\text{ N/cm}$ ；

——其余区域 $\geq 5\text{N/cm}$ 。

5.1.1.4 卡片粘接性能:

将卡 5 个一组叠在一起, 放入 $40^{\circ}\text{C} \pm 3^{\circ}\text{C}$ 相对湿度设定为 40%-60% 的箱内, 使卡背面朝下, 其上加以 2.5Kpa 的均匀压力。48 小时之后取出, 应可以用手很容易地将单张卡分开。将卡拿到实验室环境温度下立刻观察, 不能出现脱层、变色或色转移、表面磨光变化、卡上有物质转移现象以及外观形变等变化。

5.1.1.5 卡片切边质量:

每张卡的毛刺长度值 $<0.08\text{mm}$;

5.1.1.6 卡片弯曲刚度

弹性变形量应在 13.00mm 与 35.00mm 之间;

5.1.1.7 动态弯扭曲

进行 GB/T17554.1 中描述的 1000 次弯曲循环测试后, 卡应保持其功能并不应出现开裂;

进行 GB/T17554.1 中描述的 1000 次扭曲循环测试后, 卡应保持其功能并不应出现开裂;

5.1.1.8 外观质量

卡体表面不得有油污、异物等杂物;

距离 30CM 目测:

卡片没有 6 个以上 $>0.3\text{mm}$ (长度)的尘点、墨点、气泡、杂质等异常斑点或异物;

印刷没有内容错误、漏印刷、印刷图案错误、印刷位置错误的问题;

印刷表面没有明显色斑、条纹、图案或字符有明显重影、毛刺或缺损。

5.1.1.9 印刷牢度

用胶轮对卡的印刷表面进行磨损实验 500 次, 对卡的图像、颜色、字符进行目测, 无明显掉色、图像及字符模糊不清现象。

5.1.1.10 耐湿性

在 40°C 大气相对湿度达到 95% 放置 48 小时, 卡满足最大翘曲值要求及功能正常。

5.1.1.11 耐化学性

根据 GB/T17554.1 规定的测试溶液中浸泡短时间 (1 分钟), 在模拟人体排汗酸、碱度的溶液中浸泡 24 小时后, 卡应符合尺寸和翘曲要求, 卡的部件应不分离。

5.1.1.12 模块高度

IC 模块表面的最高点不应高于卡表面平面 0.05mm 。

IC 模块表面的最低点不应低于卡表面平面 0.10mm 。

5.1.1.13 抗静电

在带静电人体的正常使用下, 集成电路不应被损坏。

在任意触点和地之间, 有一个 100pF 的电容经过 1500Ω 的电阻放电产生的 2500V 的静电, 卡暴露其中, 其功能不应降低。

5.1.1.14 模块与卡体粘合强度

模块与卡体粘合力 $\geq 90\text{N}$;

5.1.1.15 卡的插拔寿命

卡与读写器间的插拔次数应 ≥ 10 万次; 插拔后的卡功能正常;

5.1.2 触点尺寸和位置

包含各个触点传导区的表面和形状不在本规范中定义。
每个触点都应有一个不小于图 1 中规定尺寸的最小矩形表面区域。
除了要求每个触点和其他触点应电隔离外，本规范不规定触点的最大形状和尺寸。

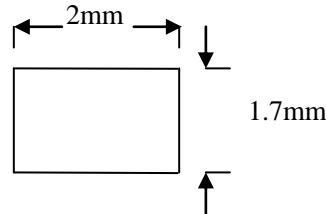


图 1 触点的最小尺寸

芯片触点应符合 ISO/IEC 7816-2 标准，见图 2。

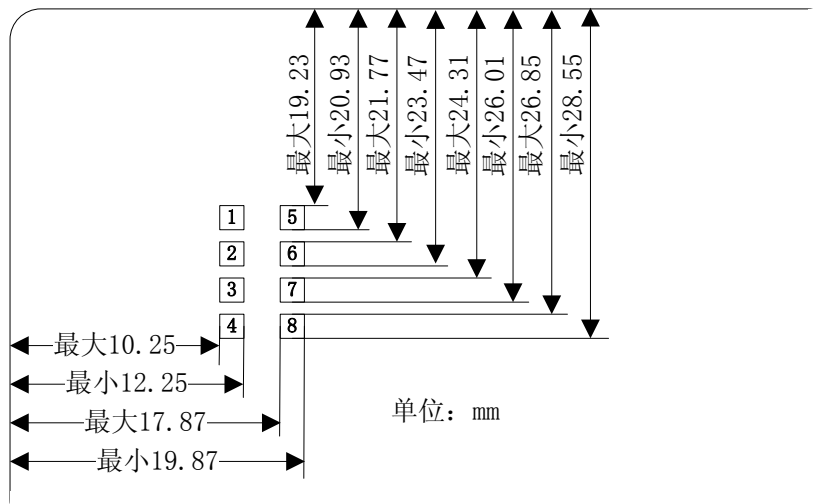


图 2 芯片触点位置示意图

5.1.3 触点分配

IC 卡上触点的分配遵循 ISO/IEC 7816-2 的规定，如表 1 所示：

表 1 IC 卡触点的分配

触电号	分配	触电号	分配
C1	电源电压(VCC)	C5	地(GND)
C2	复位信号(RST)	C6	不使用 ¹
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

C4 和 C8 保留待将来使用，可以不作实际设置。C6 在物理上也可不存在，但如果 C6 存在的话，则应将其同集成电路本身和 IC 卡上的其他触点实行电隔离²。

¹在 ISO/IEC 7816 中定义为编程电压(VPP)。
²电隔离是指当加载 5V 直流电压时，C6 与其他触点间的电阻≥10MΩ。

5.2 卡的电特性

本节描述了在 IC 卡触点上测量出的信号的电特性。

5.2.1 操作条件

5.2.1.1 操作条件的类别

本规范定义了两类操作条件。接口设备应通过触点 VCC 向卡提供下列正常的电源电压：

- 在 A 类条件下为 5V。
- 在 B 类条件下为 3V。

卡片应至少同时支持 A 类和 B 类。

5.2.2 电压和电流值

5.2.2.1 测量约定

所有测量应在 IC 卡和接口设备(IFD)之间的触点上进行，并以 GND 为参照。环境温度范围为 0℃~50℃。

所有流入 IC 卡的电流均为正值。所有时序应参照 5.2.2.2 至 5.2.2.6 中所定义的适当的门限电平来测量。

在流入接口设备的电流小于 1mA，相对于触点 GND 的电压保持在 0V 和 0.4V 之间时，电路为不工作状态。

注：温度范围的限定是由 PVC（大部分卡所用的材料）的特性决定，而不是由集成电路的特性决定。

5.2.2.2 电源电压(VCC)

该触点用来向卡提供电源。在表 2 中，在 1ms 的时间上，对电流值进行求平均值运算，为卡定义了最大电流。接口设备应能够在规定的电压范围内提供此电流并可以提供更大的电流。

表 2 正常操作条件下 VCC 的电特性

符号	条件	最小值	最大值	单位
VCC	A 类	4.5	5.5	V
	B 类	2.7	3.3	
ICC	A 类，在允许的最大频率下	-	60	mA
	B 类，在允许的最大频率下		50	
	当时钟停止时（见 6.1.3.3）		30	

即使在表 3 所规定的瞬间功耗条件下，电源电压仍应将电压值维持在规定的范围内。

表 3 ICC 的尖峰值

类别	最大电荷量 ⁽¹⁾	最大持续时间	ICC 的最大变动量 ⁽²⁾
A	20 nA.s	400ns	100mA
B	10 nA.s	400ns	50mA

(1)最大电荷量是最大持续时间和最大变动量的乘积的一半。

(2)最大变动量在电源电流方面与平均值是不同的。

5.2.2.3 输入/输出(I/O)

该触点作为输入端（接收模式）从终端接收数据或者作为输出端（传输模式）向终端传

送数据。通过该触点交换的信息使用下列两种逻辑状态：

- 1.状态 H，如果卡和接口设备都处于接收模式，或者由发送方强制此状态；
- 2.状态 L，由发送方强制此状态。

当线路的两端都处于接收模式时，该线路应处于状态 H（高电平状态）。当两端处于不匹配的传输模式时，该线路的逻辑状态可以是不确定的，但不应损坏 IC 卡。操作过程中，接口设备和卡不应同时处于传输模式。

表 4 正常操作条件下 I/O 的电特性

符号	条件	最小值	最大值	单位
VIH	VIH	$0.7 \times V_{CC}$	V_{CC}	V
I _{IH}		-300	+20	μA
VIL	VIL	0	$0.15 \times V_{CC}$	V
I _{IL}		-1000	+20	μA
VOH	V_{CC} 接外部上拉电阻 20KΩ	$0.7 \times V_{CC}$	V_{CC}	V
IOH	VOH		+20	μA
VOL	$I_{OL}=1mA^{(1)}$	0	$0.15 \times V_{CC}$	V
t _R 和 t _F	C _{IN} =30pF, C _{OUT} =30pF	-	1.0	μs
I/O 上的电压应维持在-0.3V 至 $V_{CC}+0.3V$ 之间				
(1)接口设备的实现不应要求卡的电流下降大于 500μA。				

当输入电压在允许范围内时，接口设备应能支持所定义范围内的输入电流。接口设备应向卡提供一个阻抗，以便卡能够保持所定义范围内的输出电压。

5.2.2.4 编程电压(VPP)

IC 卡不需要编程电压 VPP。

5.2.2.5 时钟(CLK)

该触点用来向卡提供时钟信号。时钟信号频率的实际值表示为 f。

表 5 正常操作条件下 CLK 的电特性

符号	条件	最小值	最大值	单位
VIH	VIH	$0.7 \times V_{CC}$	V_{CC}	V
I _{IH}		-20	+150	μA
VIL	VIL	0	0.5	V
I _{IL}		-200	+20	μA
t _R 和 t _F	C _{IN} =30pF	-	9%的时钟周期	
CLK 上的电压应维持在-0.3V 至 $V_{CC}+0.3V$ 之间				

时钟信号的占空因数应处于其稳定运行周期的 40%~60%之间。本规范不使用频率切换。

当时钟频率处于 1MHz 到 5MHz（A 类）或 1MHz 到 4MHz（B 类）之间时，IC 卡应能正常工作。

注：在卡片操作过程中，频率值将由终端维持在复位应答期间所用频率的±1%之内。

5.2.2.6 复位(RST)

该触点用来向卡提供符合 6.1.3.1（冷复位）或 6.1.3.2（热复位）的复位信号。

表 6 正常操作条件下 RST 的电特性

符号	条件	最小值	最大值	单位
V _{IH}	V _{IH}	0.8×V _{CC}	V _{CC}	V
I _{IH}		-20	+150	μA
V _{IL}	V _{IL}	0	0.12×V _{CC}	V
I _{IL}		-200	+20	μA
t _R 和 t _F	C _{IN} =30pF	-	1	μs
RST 上的电压应维持在-0.3V 到 V _{CC} +0.3V 之间				

5.2.3 触点电阻

在整个生命周期内，IC 卡触点的电阻（在清洁的 IC 卡和清洁的标准接口设备触点间测量时）应小于 500mΩ（见 ISO/IEC 10373 的测试方法）。

注：一个标准接口设备触点可以看作是在 5.00μm 镍表面上的 1.25μm 的镀金触点。

6 卡片操作过程

本节描述了卡片插入接口设备，完成交易处理直至卡片拔出的操作过程中所有步骤。

6.1 正常操作

本节描述了执行一个正常交易的操作过程。

6.1.1 操作步骤

卡的操作过程包括以下步骤：

- 将 IC 卡插入接口设备，使二者的触点相接并激活；
- 卡和接口设备之间信息交换总是由卡对冷复位（见 6.1.3.1）的应答来启动；
- 进行交易处理操作；
- 释放触点并从接口设备中取出 IC 卡。

6.1.2 IC 卡插入与触点激活

在 IC 卡插入接口设备但触点还没有进行物理接触时，终端应确保其所有触点处于低电平状态（V_{OL} 和 V_{CC} 小于或等于 0.4V）。如果 IC 卡在接口设备中位于插/拨方向正确位置³的偏差在 ±0.5mm 范围内，接口设备应能探测到卡片的存在。当所有触点进行物理接触后，触点才应被激活。终端应按下列顺序（如图 4 所示）来激活触点：

- 终端应在整个激活时序中保持 RST 为低电平状态；
- 触点物理接触之后，应在 I/O 或 CLK 激活之前，根据接口设备选定的操作条件给 V_{CC} 加电（见 5.2.2.2 和表 2）；
- 终端在确认已稳定提供中规定的电压和电流后，将 I/O 置于接收模式并提供《社会保障（个人）卡规范》第 8 部分：终端技术要求中规定的合适、稳定的时钟。终端将其 I/O 置于接收模式可以在时钟启动之前，也可以在此之后，但最迟不得超过时钟启动后的 200

³这里的正确位置是指接口设备触点的中心正对 IC 卡触点（符合 ISO 7816-2 中的有关规定）的中心。

个时钟周期。

注：根据设计，终端可以给 Vcc 一个足够的等待时间使之稳定，待稳定后再通过测量或其他方式检查它的状态。终端将其 I/O 置为接收模式后，其 I/O 状态取决于 IC 卡上 I/O 的状态。

上述的触点激活过程完成后，卡准备好按照 6.1.3.1 和图 5 所规定的时序进行冷复位。

6.1.3 信息交换

如果卡支持操作条件类别，则卡应该根据 7 应答任何的复位。在任何复位应答完成后，接口设备可以启动一次卡的热复位。对热复位的应答可以不同于前一次的应答，或者是冷复位的，或者是热复位的。

IC 卡利用激活的低电平复位信号，采用异步方式进行复位应答。

复位应答的传送方式在 7 中描述，而其内容在 8.2 和 8.3 中描述。

6.1.3.1 冷复位

在 6.1.2 所述的触点激活后，终端将发出一个冷复位信号，并从 IC 卡获得一个复位应答信号（见图 4），过程如下：

——终端在 Ta 时刻启动 CLK；

——在 Ta 后的不超过 200 个时钟周期(ta)内，IC 卡将其 I/O 置为接收模式。由于终端也要在同样时间内将其 I/O 置为接收模式，因此 IC 卡上的 I/O 应确保在 Ta 后最迟不超过 200 个时钟周期内置为高电平；

——终端应从 Ta 开始保持 RST 端为低电平状态至少 400 个时钟周期(tb)，并在时刻 Tb 将 RST 端置为高电平状态；

——IC 卡上 I/O 的复位应答将在 RST 端上信号的上升沿后的 400 到 40000 个时钟周期(tc)内开始；

——如果 IC 卡的复位应答没有在 RST 处于高电平的 40000 个时钟周期内开始，终端将启动 6.1.5 中描述的释放时序。

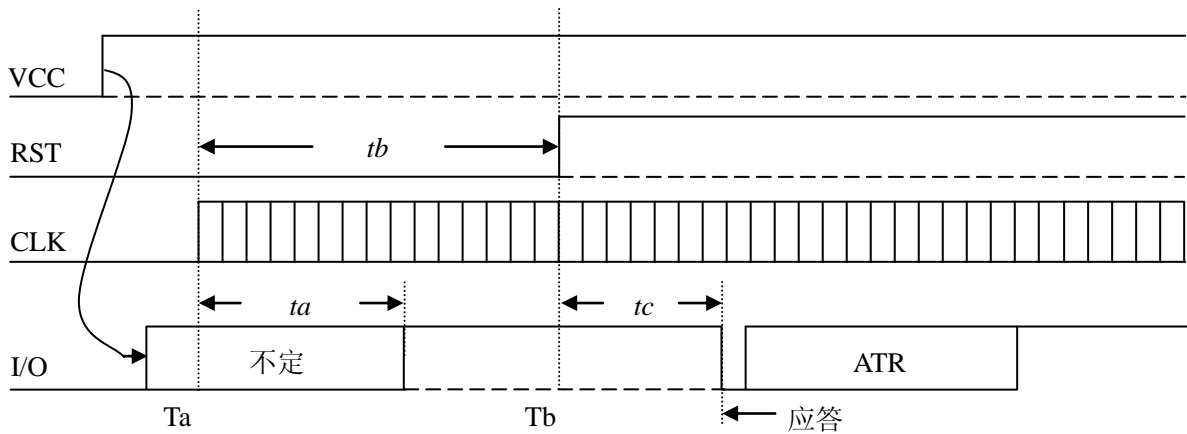


图 4 激活和冷复位

上述过程中的各个时段，需满足下列要求：

$$ta \leq \frac{200}{f}$$

$$\frac{400}{f} \leq tb$$

$$\frac{400}{f} \leq tc \leq \frac{40000}{f}$$

注意：

- 1.假定卡的内部状态在冷复位前是未定义的。因此，卡的设计必须避免不适当的操作。
- 2.接口设备可以在任何时候根据其判断来启动卡的冷复位。

6.1.3.2 热复位

在 6.1.3 中所述的冷复位过程之后，如果收到的复位应答信号不能满足 8 中的规定，终端将启动一个热复位并从 IC 卡获得复位应答（见图 5）。过程如下：

- 热复位将从 T_c 开始，此时终端将 RST 置为低电平状态至少 400 个时钟周期(t_e)；
- 在整个热复位时序中，终端将保持 V_{cc} 和 CLK 的稳定，并且符合《社会保障（个人）卡规范》第 8 部分：终端技术要求的规定；
- 在 T_c 后的不超过 200 个时钟周期(t_d)内，IC 卡和终端将其 I/O 置为接收模式。因此其 I/O 应确保在 T_c 后最迟不超过 200 个时钟周期内置为高电平；
- 终端应从 T_c 开始保持 RST 端为低电平状态，并在时刻 T_d 将 RST 端置为高电平状态；
- IC 卡上 I/O 的复位应答将在 RST 端上信号的上升沿(T_d)后的 400 到 40000 个时钟周期(t_f)内开始；
- 如果 IC 卡的复位应答没有在此时段内开始，终端将启动 6.1.5 中描述的释放时序。

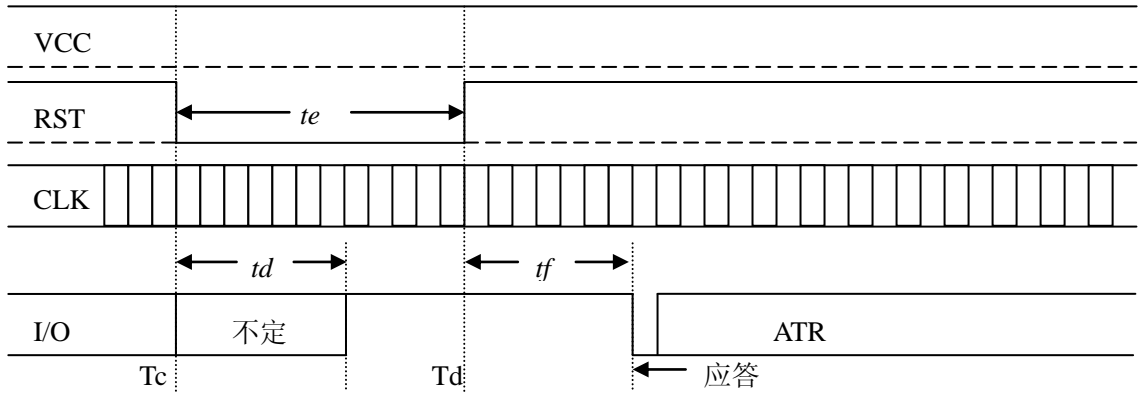


图 5 热复位时序

上述过程中的各个时段，需满足下列要求：

$$t_d \leq \frac{200}{f} \quad \frac{400}{f} \leq t_e \quad \frac{400}{f} \leq t_f \leq \frac{40000}{f}$$

6.1.3.3 时钟停止

对于支持时钟停止的卡来说，当接口设备不再期望从卡获得传输信息，并且 I/O 保持在高电平至少 1860 个时钟周期(t_g)时，按照图 6，接口设备可以（在时刻 T_e ）停止 CLK 上的时钟信号。

在时钟停止时（从时刻 T_e 到时刻 T_f ），CLK 既可以维持在高电平状态，也可以维持在低电平状态。所维持的状态由 8.3.3.10 中所定义参数 X 来确定。

在时刻 T_f ，接口设备重新启动时钟，I/O 上的信息交换在至少 700 个时钟周期(t_h)后可以继续进行。

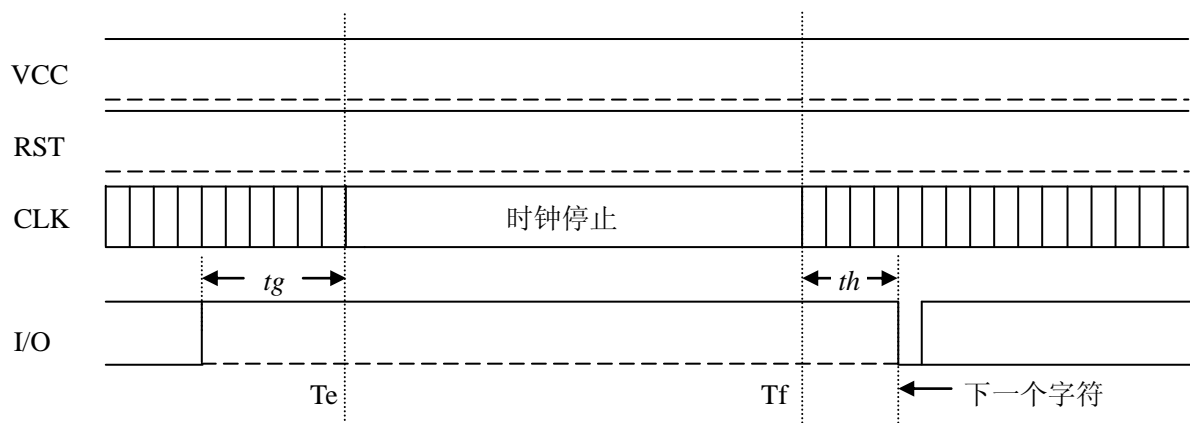


图 6 时钟停止

上述过程中的各个时段，需满足下列要求：

$$\frac{1860}{f} \leq t_g$$

$$\frac{700}{f} \leq t_h$$

6.1.4 交易执行

IC 卡中应用的选择以及执行一次交易操作所需的 IC 卡与终端之间信息交换将在《社会保障（个人）卡规范》第 7 部分：应用流程中描述。

6.1.5 触点释放时序

作为卡片操作的最后一步，根据交易的正常或异常结束（包括在卡片操作过程中将卡从接口设备中拔出），终端将把接口设备触点置为静止状态（见图 7）。过程如下：

——终端将通过把 RST 置为低电平状态来启动释放时序；

——在置 RST 为低电平状态之后且 VCC 断电之前，终端将 CLK（除非 CLK 已停止在低电平状态）和 I/O 设定为低电平状态。

——在置 RST、CLK 和 I/O 为低电平状态之后且卡片触点与接口设备触点物理分离之前，终端将切断 VCC 电源，此时的 Vcc 应小于或等于 0.4V。

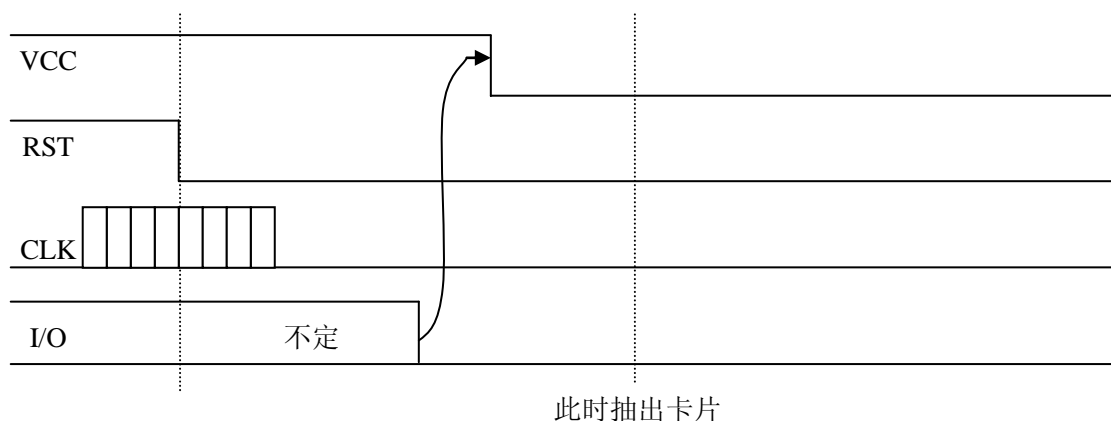


图 7 触点释放时序

6.2 交易过程的异常结束

在交易过程中，如果 IC 卡以 1m/s 的速度过早地从终端中拔出，终端应能感觉到 IC 卡相对于接口设备触点的移动，并在相对位移达到 1mm 之前，根据 6.1.5 中描述的方式将接口设备的所有触点置为静止状态。在这种情况下，IC 卡的电气或机械特性应不受损坏。

注：对于滑触式结构的接口设备，终端有可能感觉到 IC 卡触点与接口设备触点之间的相对位移。此处不对能否感知到相对运动作强制性要求，但在 IC 卡和接口设备触点脱离之前应能够将其置为静止状态。

7 字符的物理传送

在卡片操作过程中，数据通过 I/O 在终端和 IC 卡之间以异步半双工方式进行双向传送。终端向 IC 卡提供一个用作数据交换时序控制的时钟信号。数据位和字符的交换机制在下面描述，这种交换机制适用于复位应答，并在 9 中描述的传输协议中使用。

7.1 位持续时间

在 I/O 上使用的位持续时间被定义为一个基本时间单元(etu)。在复位应答期间，I/O 上 etu 和 CLK 频率(f)之间呈线性关系。

复位应答期间的位持续时间称为初始 etu，由下列方程给出：

$$\text{初始 etu} = \frac{372}{f} \text{ 秒, 式中 } f \text{ 的单位是赫兹}$$

复位应答后（参数 F 和 D 的确定参见 8.3.3.2）的位持续时间称为当前 etu，由下列方程给出：

$$\text{当前 etu} = \frac{F}{Df} \text{ 秒, 式中 } f \text{ 的单位是赫兹}$$

注：本规范描述的基本复位应答，仅支持 F=372 和 D=1。这样初始 etu 和当前 etu 相同且均等于 $\frac{372}{f}$ 。除非另外说明，以后所提到的 etu 均为当前 etu。

在卡的整个交易过程中，f 的值应在 1~5MHz（A 类）或 1~4MHz（B 类）之间。

7.2 字符帧

数据在 I/O 上以下述的字符帧方式传输。采用的约定由 IC 卡在复位应答时发送的初始字符(TS)确定（见 8.3.1）。

字符传送之前，I/O 应被置为高电平状态。

一个字符由 10 个连续位组成（见图 8）：

- 1 个低电平状态的起始位；
- 组成数据字节的 8 个数据位；
- 一个奇偶校验位。

起始位由接收端通过对 I/O 周期采样测得，采样时间小于 0.2etu。

一个字符中的逻辑‘1’位的数目必须是偶数，8 个数据位和奇偶校验自身均做为校验计算位，但起始位不作校验计算。

起始时刻固定地从最后一个检测到的高电平状态到第一个检测到的低电平状态的中间算起，起始位应在 0.7etu 之前被验证是否存在，后续的各位应在 $(n+0.5 \pm 0.2)\text{etu}$ （n 为各位的次序号）间隔内接收到，起始位的次序号为 1。

在一个字符内，从起始位的前沿到第 n 位的后沿之间的时间是 $(n \pm 0.2)\text{etu}$ 。

两个连续字符起始位前沿之间的间隔时间，等于字符持续时间 $(10 \pm 0.2)\text{etu}$ 加上一个保护时间。在保护时间内，IC 卡与终端都应处于接收模式（即 I/O 为高电平状态）。当 T=0 时，

如果 IC 卡或终端作为接收方对刚收到的字符检测出奇偶错误，则 I/O 被设置为低电平状态，以向发送方表明出现错误（见 9.2.3）。

在终端的传输层(TTL)，数据总是采用高位先送方式(m.s.)在 I/O 上传送。一个字节中位的传送顺序（即低位先送还是高位先送）由复位应答回送的 TS 字符确定（见 8.3.1）。

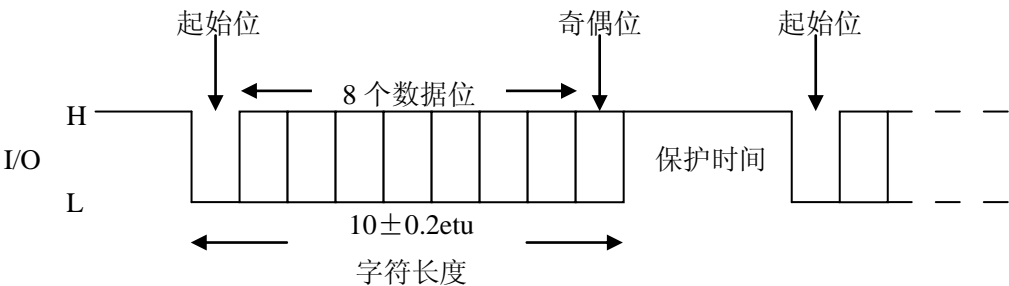


图 8 字符帧

8 复位应答

如同 6.1.3 所述，在终端发出复位信号后，IC 卡以一串字节作为应答（即复位应答）。这些传输到终端的字节规定了卡和终端之间即将建立的通信的特征。传输这些字节的方法及字节的含义在下面描述。

注：在 8 和 9 中，一个字符的最高位指的是 b8 位，最低位是 b1 位。单引号中的值表示以十六进制值标注，例如‘3F’。

8.1 复位应答期间回送字符的物理传输

本节描述了复位应答期间回送字符的结构和时序。
在复位应答过程中，两个连续字符的起始位前沿之间的最小时间间隔为 12 个初始 etu，最大时间间隔为 9600 个初始 etu，这个最大值被称为“初始等待时间”

在复位应答期间，IC 卡应在 19200 个初始 etu⁴内发送完成所有要回送的字符。发送时间应从第一个字符(TS)起始位的前沿开始，到最后一个字符起始位前沿后的 12 个初始 etu 为止。

8.2 复位应答期间 IC 卡回送的字符

根据本规范对传输协议的规定（见 9），本节规定了 IC 卡在复位应答期间回送字符的数目和编码，以及传输控制参数值的允许范围。
根据特殊需要，IC 卡也可以选择支持由发卡方确定的其他传输控制参数值，但这已超过本规范的范围。

IC 卡回送的基本复位应答中的字符如表 7 和表 8 所示，字符的次序按照 IC 卡发送的顺序排列，即 TS 为第一个字符。

对于采用 T=0 协议（异步半双工字符传输协议）、不支持时钟停止和操作条件选择的 IC 卡所回送的字符如表 7 所示：

表 7 T=0 时的基本 ATR（不支持时钟停止和操作条件选择）

⁴由于 etu 的大小依赖于时钟频率，因此复位应答所允许的最大时间根据时钟频率的不同而不同（见 7.1）。

字符	值	备注
TS	‘3B’	本规范仅使用正向约定
T0	‘6x’	TB1 和 TC1 存在
	‘2x’	仅 TB1 存在
	‘7x’	TA1,TB1 和 TC1 存在
	‘3x’	TA1 和 TB1 存在, ‘x’表示历史字节的存在个数 K
TA1	XY	‘x’表示 Fi’, ‘y’表示 Di,
TB1	‘00’	不使用 VPP
TC1	‘00’到‘FF’	指明所需额外保护时间的数量, ‘FF’值为特定含义值（见 8.3.3.4）

对于采用 T=0 协议（异步半双工字符传输协议）、支持时钟停止和/或操作条件选择的 IC 卡所回送的字符如表 8 所示：

表 8 T=0 时的基本 ATR（支持时钟停止和/或操作条件选择）

字符	值	备注
TS	‘3B’	本标准仅使用正向约定
T0	‘9x’	TA1 和 TD1 存在
	‘Dx’	TA1,TC1 和 TD1 存在
	‘Cx’	TC1 和 TD1 存在
	‘8x’	TD1 存在 ‘x’表示历史字节的存在个数 K
TA1	‘XY’	‘x’表示 Fi’, ‘y’表示 Di,
TC1	‘00’到‘FF’	指明所需额外保护时间的数量, ‘FF’值为特定含义值（见 8.3.3.4）
TD1	‘80’	TA2 到 TC2 不存在, TD2 存在；使用 T=0 协议
TD2	‘1F’	TA3 存在, TB3 到 TD3 不存在；限定 TA3 是全局接口字节
TA3	b8-b7=‘0’到‘2’, b2-b1=‘1’到‘3’, 其余位=‘0’	XI=0 到 2 UI=1 到 3
TCK	见 8.3.3.11	校验字符

8.3 字符定义

本节对复位应答中可能回送的字符进行了详细描述。在符合基本 ATR 的情况下，一个字符是否存在，以及允许的取值范围（如果存在）由其“基本应答”信息指明。基本应答描述

既不排斥其他字符值的使用，也不排斥发卡方增加或删减字符。例如，如果 IC 卡支持多个传输协议，它可以回送附加字符（见 9）。但是，只有在 IC 卡返回一个基本 ATR，或返回一个《社会保障（个人）卡》第 9 部分：终端技术要求中描述的满足最低功能需求的终端所支持的 ATR，才能保证字符的正确交换。

复位应答中回送字符的最大个数（包括历史字符，但不包括 TS）为 32 个。

8.3.1 TS——初始字符

TS 有两个功能：向终端提供一个便于位同步的已知位模式，并指定解释后续字符的逻辑约定。

对于正向逻辑约定，I/O 的高电平状态等效于逻辑‘1’，并且该数据字节的最低位在起始位之后首先发送，第 1 个半字节 LHHL 用于位同步。

基本响应：IC 卡将回送的 TS 为：(H)LHHLHHLLH——正向约定，值为‘3B’。

8.3.2 T0——格式字符

T0 由两部分组成，高半字节(b5-b8)表示后续字符 TA1 到 TD1 是否存在，b5-b8 位设置成逻辑‘1’表明 TA1 到 TD1 存在；相应地，低半字节(b1-b4)表明可选历史字符的数目（0 到 15）（见表 9）。

基本响应：IC 卡应回送 T0。‘x’的值表示要回送的可选历史字符的数目。

表 9 T0 的基本响应代码

	b8	b7	b6	b5	b4	b3	b2	b1
‘2x’	0	0	1	0	x	x	x	x
‘3x’	0	0	1	1	x	x	x	x
‘6x’	0	1	1	0	x	x	x	x
‘7x’	0	1	1	1	x	x	x	x
‘8x’	1	0	0	0	x	x	x	x
‘9x’	1	0	0	1	x	x	x	x
‘Cx’	1	1	0	0	x	x	x	x
‘Dx’	1	1	0	1	x	x	x	x

8.3.3 TA1 到 TA3——接口字符

在复位应答后的终端和 IC 卡信息交换期间，TA1 到 TA3 表示传输控制参数 F、D、N、P、I、X 及 U 的值。TA1 到 TC1 和 TA3 传送的信息将用于后续数据交换。

8.3.3.1 TA1

TA1 传送 FI 和 DI 的值，其中：

——FI 用于确定 F 的值，F 为时钟速率转换因子。用于修改复位应答之后终端所提供的时钟频率。

——DI 用于确定 D 的值，D 为比特速率调节因子。用于调整复位应答之后所使用的位持续时间。ATR 后位持续时间（当前 etu）的计算方法见 7.1。

8.3.3.2 传输因子 F 和 D

参数 F 和 D 分别是时钟率转换因子和波特率校正调整因子。在电路输入/输出上使用的

etu 依赖于传输因子 F 和 D 的实际值。etu 应等于 F/D 时钟周期。

$$1 \text{ etu} = F/D \times 1/f$$

频率 f 的最小值应当为 1MHz。最大值作为 FI 的功能以 FI 的函数的形式在表 10 中给出。缺省最大值是 5MHz。

为计算 etu，F 和 D 因子对应当采用下面三对值：

Fi 和 Di，按照表 10 和表 11 在 TA1 中由卡指示的值；如果 TA1 不存在，则 Fi 和 Di 设为缺省值；

Fd 和 Dd，缺省值为 372 和 1；

Fn 和 Dn，在 Fd 到 Fi 和 Dd 到 Di 范围里成功的 PPS 交换所协商的值。

在复位应答期间，应用 Fd 和 Dd。复位应答后，F 和 D 的值取决于操作模式

协商模式中，Fd 和 Dd 应继续应用直到 PPS 交换成功完成（见 8.7.2）。PPS 成功交换后，Fn 和 Dn 立即应用。

表 10 Fi，指明的时钟率转换因子的值

FI	0000	0001	0010	0011	0100	0101	0110	0111
Fi	372	372	558	744	1116	1488	1860	RFU
f (max) MHz	4	5	6	8	12	16	20	—

FI	1000	1001	1010	1011	1100	1101	1110	1111
Fi	RFU	512	768	1024	1536	2048	RFU	RFU
f (max) MHz	—	5	7,5	10	15	20	—	—

注：RFU=留作未来使用

表 11 指明的波特率校正参数的值

DI	0000	0001	0010	0011	0100	0101	0110	0111
Di	RFU	1	2	4	8	16	32	RFU

DI	1000	1001	1010	1011	1100	1101	1110	1111
Di	12	20	RFU	RFU	RFU	RFU	RFU	RFU

在复位应答期间使用的缺省值 FI=0（B 类）或 1（A 类）和 DI=1，分别表示 F=372 和 D=1。

基本响应：IC 卡不回送 TA1 值，在整个后续信息交换过程中继续使用缺省值 F=372 和 D=1。

8.3.3.3 TB1

TB1 传送 PI1 和 II 值，其中：

——PI1 在 b1 到 b5 位中定义，用于确定 IC 卡所需的编程电压 P 值。PI1=0 表示 IC 卡不使用 VPP。

——II 在 b6 和 b7 位中定义，用于确定 IC 卡所需的最大编程电流 I 值。II=0 表示不使用此参数。

——b8 位不使用，并设置为逻辑‘0’。

基本响应：如果 T=15 不存在于复位应答中，IC 卡应回送 TB1='00'，表示 IC 卡不使用 VPP；如果 T=15 存在，则 IC 卡不回送 TB1 值。

如回送，字符 TB1 的基本响应代码如表 12 所示：

表 12 TB1 的基本响应代码

b8	b7	b6	b5	b4	b3	b2	b1
0	0	0	0	0	0	0	0

8.3.3.4 TC1

TC1 传送 N 值，N 用于表示增加到最小持续时间的额外保护时间，此处的最小持续时间表示从终端发送到 IC 卡的，作为后续信息交换的两个连续字符的起始位前沿之间的时间。N 在 TC1 的 b1-b8 位为二进制编码，其值作为额外保护时间表示增加的 etu 数目，其值可在 0 到 255 之间任选。N=255 具有特殊含义，表示在使用 T=0 协议时，两个连续字符的起始位前沿之间的最小延迟时间可减少到 12 个 etu，并且在传输的两个方向上是相同的。

注：除 N=255 外，TC1 只适用于终端向 IC 卡发送的两个连续字符间的时段，而不适用于 IC 卡向终端发送字符的情况，也不适用于两个反方向发送字符的情况，见 9.2.2。

如果 TC1 值在'00'到'FE'之间，增加到字符间最小持续时间的额外保护时间为 0 到 254 个 etu。对于后续传输，额外保护时间将在 12 到 266 个 etu 之间。

如果 TC1='FF'，则后续传输的字符间最小持续时间在使用 T=0 协议时为 12 个 etu。

基本响应：IC 卡应回送'00'到'FF'之间的 TC1 值。

T0 的 b7 位可以为'0'，表示 IC 卡不回送 TC1。在此情况下，在以后的卡片操作过程中，将默认 TC1='00'。

字符 TC1 的基本响应代码如表 13 所示：

表 13 TC1 的基本响应代码

b8	b7	b6	b5	b4	b3	b2	b1
x	x	x	x	x	x	x	x

注：建议将 TC1 设置为 IC 卡可接受的最小值。TC1 取值过大将导致终端与 IC 卡之间的通信缓慢，这样将延长交易时间。

8.3.3.5 TD1

TD1 表示是否还要发送更多的接口字节以及后续传输所使用的协议类型，其中：

——高半字节用于表示字符 TA2 到 TD2 是否存在，这些位(b5-b8)设置为逻辑'1'状态时，分别表示 TA2 到 TD2 字符的存在；

——低半字节用于表示后续信息交换所使用的协议类型。

基本响应：当不支持 B 类操作条件和时钟停止时，IC 卡不回送 TD1，则 T=0 协议作为后续传输类型的缺省值；当支持 B 类操作条件或时钟停止时，IC 卡回送 TD1='80'，表示 TD2 存在，且后续传输协议类型为 T=0 协议。

8.3.3.6 TA2

TA2 的存在与否表示 IC 卡是以特定模式还是以协商模式工作。

基本响应：IC 卡将不回送 TA2，TA2 不存在表示以协商模式工作。

8.3.3.7 TB2

TB2 传送 PI2, PI2 用于确定 IC 卡所需的编程电压 P 的值, 当 PI2 出现时, 它将取代 TB1 中回送的 PI1 的值。

基本响应: IC 卡不应回送 TB2。

8.3.3.8 TC2

TC2 专用于 T=0 协议, 并传送工作等待时间整数(WI), WI 用来确定由 IC 卡发送的任意一个字符起始位前沿与 IC 卡或终端发送的前一个字符起始位前沿之间的最大时间间隔。工作等待时间为 $960 \times D \times WI$ 。

基本响应: IC 卡不回送 TC2, 且后续通信中使用缺省值 WI=10。

8.3.3.9 TD2

TD2 表示还要发送更多的全局接口字节, 其中:

——高半字节用于表示字符 TA3 到 TD3 是否存在, 这些位(b5-b8)设置为逻辑‘1’状态时, 分别表示 TA3 到 TD3 字符的存在;

——低半字节为参数 T=15, 表示 TD1 之后的接口字节是全局的。

基本响应: 如果 IC 卡不回送 TD1, 则 IC 卡也不回送 TD2 值; 否则, IC 卡应回送 TD2=‘1F’, 表示 TA3 存在。

8.3.3.10 TA3

TA3 传送 XI 和 UI 的值, 其中:

——XI 在 b8、b7 位中定义, 用于确定时钟停止指示符 X 的值。X 向接口设备表明是否支持时钟停止, 如果支持, 则在时钟停止时 CLK 端上的电平状态见表 14。

——UI 在 b1 到 b6 位中定义, 用于确定类别指示符 U 的值。U 向接口设备表明卡所接受的操作条件见表 15。

表 14 时钟停止指示符 X

XI	00	01	10	11
X	不支持时钟停止	低电平	高电平	都可以

表 15 类别指示符 U

UI	00 0001	00 0010	00 0011	其他值
U	仅用 A 类操作条件	仅用 B 类操作条件	可用 A 类或 B 类操作条件	RFU

基本响应: IC 卡将根据实际情况回送 TA3 值。

8.3.3.11 TCK——校验字符

TCK 具有一个检验复位应答期间所发送数据完整性的值。TCK 的值应使从 T0 到包括 TCK 在内的所有字节进行异或运算而结果为零(零)。

基本响应: 如果 T=15 不存在于复位应答中, 则 IC 卡不回送 TCK, 否则, IC 卡应回送 TCK。

8.4 历史字节

历史字节指明一般信息, 如果 K 不为零, 则复位应答在 K 个历史字节 T1 T2..... TK 上连续出现。

本规范所规定的基本历史字节如表 16 所示:

表 16 基本历史字节的编码

字符	值
T1-T2	芯片提供机构注册标识号
T3-T5	芯片提供方或卡操作系统提供方自定义
T6-T7	卡片制造机构注册标识号
T8-T9	卡序列号（发卡地区所在地的行政区划代码前 4 位）
TA-TD	卡序列号（发卡地区自行编排并保持每张卡的唯一性）

8.5 复位应答的次序和一致性

在 IC 卡的触点如 6.1.2 中所描述的那样激活之后，终端应启动一个如 6.1.3.1 中所定义的冷复位。

——如果 IC 卡在冷复位应答时回送的字节数不符合 8.2 与 8.3 中的规定，或者来自 IC 卡的复位应答在 8.1 中规定的 19200 个初始 etu 之内没有完成，终端不应马上终止卡片操作过程，而应发送一个在 6.1.3.2 中定义的热复位信号；

——如果冷复位应答符合本规范且在 19200 个初始 etu 之内回送，终端应使用其回送的参数继续进行卡片操作过程；

——如果终端按以上描述启动了一个热复位，而 IC 卡在热复位应答中回送的字节数不符合 8.2 和 8.3 中的规定，或者来自 IC 卡的复位应答在 8.1 中规定的 19200 个初始 etu 之内没有完成，终端应按照 6.1.5 中规定的次序释放触点并终止卡片操作过程；

——如果热复位应答符合本规范且在 19200 个初始 etu 之内回送，终端应使用其回送的参数继续进行卡片操作过程；

——如果在冷复位或热复位应答期间，IC 卡回送的两个连续字符起始位前沿之间的时间超过了 9600 个初始 etu，终端应按照 6.1.5 中规定的次序释放触点并终止卡片操作过程。

8.6 复位应答—终端上的流程图

图 9 给出了一个 IC 卡向终端回送复位应答的过程，以及由终端执行检查以确保该复位应答符合 8 中规定的实例。

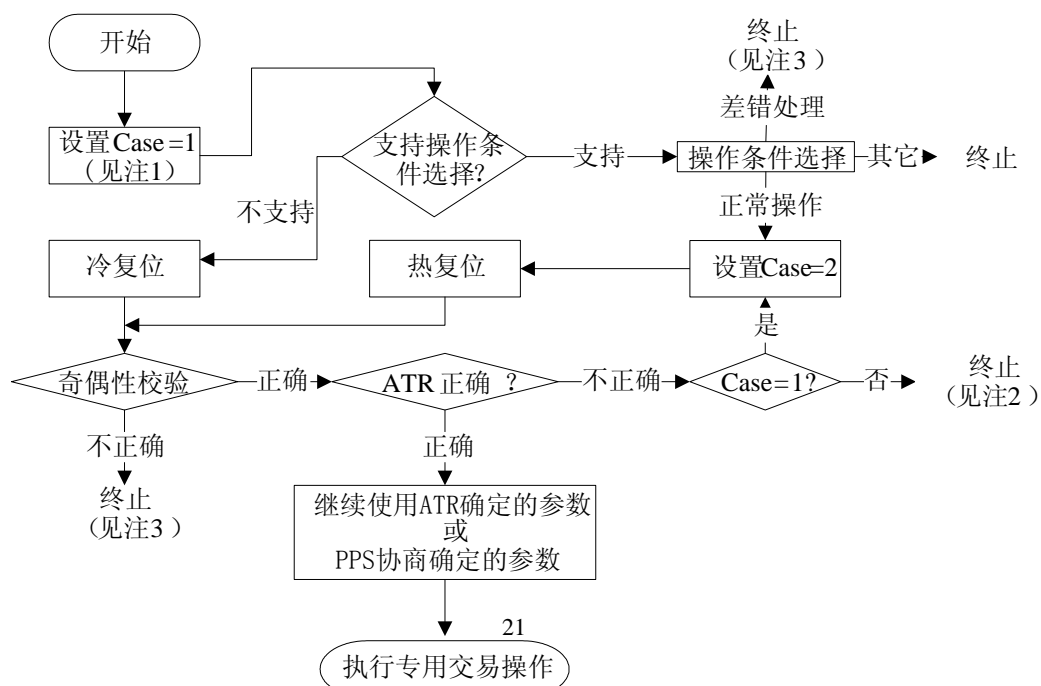


图 9 ATR—终端上的流程图

注 1: “Case”是一个过程变量, 用来表示是执行一次冷复位还是执行一次热复位。Case=1 时为冷复位, Case=2 时为热复位。

注 2: 如果过程在此处结束, 则 IC 卡可能是一个商业协议终端可接受的非社会保障卡。终端应在卡插入前, 通过特殊处理过程而事先做好准备, 以便接受这种卡。这可以在终端上设置专用按钮来做到, 相应地, 处理过程也是专用的。

注 3: 如果过程在此处结束, 则可以将 IC 卡从终端中拔出, 并按照要求正确操作而使 IC 卡重新复位。终端上应显示一条相应的信息。

8.7 操作模式

8.7.1 协商模式

复位应答后, 卡进入协商模式。

在协商模式中, 只要接口设备发送给 IC 卡的第一字节允许在 PPS 请求与协议命令之间有明显差别, 则“缺省选择”是可能的。

在复位应答后无 PPS 请求, 则“首选协议”将使用 Fd 和 Dd (见 8.3.3.2)。

当 IC 卡提供参数 F、D 的其它值 (F 范围为 Fd 到 Fi, D 的范围为 Dd 到 Di) 时, 接口设备应发送一个带 Fn 和 Dn 的 PPS 请求, 成功完成 PPS 交换后 (见 8.7.2.2), 协商协议应使用 Fn 和 Dn。

注: 如果 ATR 带有值 Fi 和 Di, 且 Fi、Di 不等于 Fd、Dd, 则接口设备可以:

选择带有 Fd、Dd 的缺省协议,

发送带 Fn 和 Dn 的 PPS 请求, 以协调 Fn、Dn。

8.7.2 协议和参数选择

8.7.2.1 概述

本条规范了明确的协议和参数选择。应用在指示协商模式的复位应答之后。

PPS 请求和应答以与复位应答相同的方式发送。例如, 相同的波特率 (使用 Fd 和 Dd), 符合 TS (8.3.1) 规定的协议, 连续两个字符的上沿具有最小延迟 12etu。然而如果接口设备字节 TC1 出现在复位应答中, 且值不为“FF”, 则应保证有足够的保护时间 (见 8.3.3.4)。PPS 响应的两个连续字符的上沿之间的延迟不应超过“初始等待时间” (见 8.1)。

8.7.2.2 PPS 协议

只有接口设备被允许开始 PPS 交互

接口设备应发送一个 PPS 请求给 IC 卡。

如果 IC 卡收到一个错误 PPS 请求, 则它不作任何响应。

如果 IC 卡收到一个正确 PPS 请求, 则应返回一个 PPS 响应, 否则将超过初始等待时间。

如果超过初始等待时间, 则接口设备或者复位, 或者拒绝 IC 卡。

如果接口设备收到错误 PPS 响应, 则接口设备或者复位, 或者拒绝 IC 卡。

如果 PPS 交换失败, 则接口设备或者复位, 或者拒绝 IC 卡。

8.7.2.3 PPS 请求与相应的结构和内容

每个 PPS 请求和 PPS 响应都是由初始字符 PPSS、格式字符 PPS0, 三个可选参数字符 PPS1、PPS2 和 PPS3, 以及最后一个字节校验字符 PCK 组成。

PPSS 编码为“FF”，标识 PPS 请求或 PPS 响应。

PPS0 的 B5, B6 和 B7 位设置为逻辑“1”，分别对应表示 PPS1, PPS2 和 PPS3 的存在。低四位 B1-B4 编码表示选择的协议类型(本规范规定社会保障卡只使用字符传输协议 T=0)，与 TD 的编码方式相同。B8 位保留。

PPS1 与 TA1 的编码方式相同，表示 FI 和 D。如果不传输 PPS1，缺省值为 FI=1, D=1。

PPS2 字节中如果 B1 位置“1”，则表示支持 N=255；B2 置“1”表示向接口设备传输数据时，额外有 12 个 etu 的保护时间；B2 置“0”表示不需要额外保护时间。B3-B8 位保留。

PPS3 的编码及使用没有定义。

PCK 的值应使自 PPSS 至 PCK 的所有字节的异或值为零。

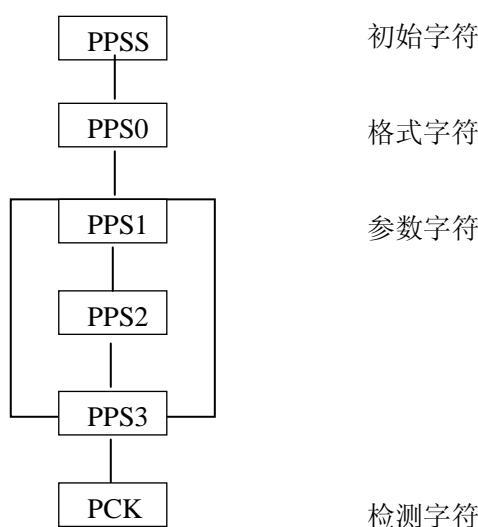


图 10 PPS 请求和相应的结构

9 传输协议

本节规定了在异步半双工传输协议中，终端为实现传输控制和特殊控制而发出的命令的结构及其处理过程。

本规范规定社会保障卡只使用字符传输协议(T=0)。在 ATR 中提供的其他参数和与特定协议相关的参数将在本节相应的部分定义。

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，包含以下定义：

a) 字符帧，定义了字符交换。

b) T=0，定义了 T=0 时的字符交换。

c) 对 T=0 的检错与纠错。

——传输层，定义了面向应用的报文传输。

——应用层，根据相同的应用协议，定义报文交换的内容。

9.1 物理层

T=0 协议使用了物理层和 7.2 中定义的字符帧。

9.2 数据链路层

描述了传输协议 T=0 的时段分配、特殊选择与错误处理。

9.2.1 字符帧

在 7.2 中定义的字符帧适用于 IC 卡与终端之间的所有报文交换。

9.2.2 字符协议 T=0

9.2.2.1 特定选项——用于 T=0 的时段分配

在复位应答中，TC1 的值决定了终端发送到 IC 卡的两个连续字符起始位前沿之间的最小时间间隔在 12 到 266 个 etu 之间（见 8.2 和 8.3）。

IC 卡发送到终端的两个连续字符起始位前沿之间的最小时间间隔为 12 个 etu。

在 IC 卡发送的任意字符的起始位前沿与 IC 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（工作等待时间）将不超过 $960 \times D \times WI = 9600$ 个 etu（位速率转换因子 D 的缺省值是 1，当 ATR 中不回送时，WI 的缺省值为 10）。

相反方向发送的两个连续字符起始位前沿之间的最小时间间隔不小于 16 个 etu。

注：由终端向 IC 卡发送的两个连续字符起始位前沿之间的最小时间间隔由 TC1 值控制，可以小于相对发送的两个连续字符之间所允许的最小时间间隔（16 个 etu）。

9.2.2.2 命令头

命令均由终端应用层(TAL)发出，它包括一个由 5 个字节组成的命令头。每个命令头由 5 个连续字节 CLA、INS、P1、P2 和 P3 组成：

——CLA：命令类别；

——INS：指令代码；

——P1 和 P2：附加参数；

——根据不同的 INS，P3 指明发送给 IC 卡的命令的字节长度或期待 IC 卡响应的最大数据长度。

对于 T=0，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)，命令应用协议数据单元(C-APDU)到 C-TPDU 的映射将在 9.3 中描述。

TTL 传送 5 个字节的命令头给 IC 卡并等待一个过程字节。

9.2.2.3 过程字节

IC 卡接收到命令头后，向 TTL 回送一个过程字节。过程字节向 TTL 指明了下一步该做什么，其编码与 TTL 行为的对应关系如表-17 所示：

表 17 终端对过程字节的响应

	过程字节值	步骤
i	与 INS 字节值相同	所有余下的数据将要由 TTL 传送或者 TTL 准备接收所有的来自 IC 卡的数据
ii	与 INS 字节值的补码相同 (INS)	下一个数据字节将由 TTL 传送或者 TTL 准备接收来自 IC 卡的下一个数据字节
iii	'60'	TTL 提供根据本条所定义的额外工作等待时间
iv	'6x'或'9x'，除'60'之外（过程字节或	TTL 将等待下一个过程字节或状态码 SW2

状态码 SW1)	
----------	--

在情况(i)、(ii)和(iii)中, 操作完成后 TTL 将等待另一个过程字节。

在情况(iv)中, 第二个过程字节或状态码(SW2)已被收到后, TTL 将要做以下事情:

——如果过程字节为‘61’, TTL 将向 IC 卡发送一个最大长度为‘xx’的“GET RESPONSE”命令头, ‘xx’为 SW2 值。

——如果过程字节为‘6C’, TTL 将立即向 IC 卡重发前一个命令的命令头, 其长度为‘xx’, ‘xx’是 SW2 值。

——如果过程字节是‘6x’ (除‘60’和‘61’及‘6C’之外) 或者‘9x’ (即状态), TTL 将在响应 APDU (R-APDU)中向 TAL 回送状态码 (与其他必要数据一起, 见 9.3), 并等待下一个 C-APDU。

在 TTL 和 IC 卡之间交换命令和数据时, TTL 和 IC 卡都必须清楚地知晓数据流向和 I/O 的驱动者 (TTL 或 IC 卡)。

9.2.2.4 C-APDU 的传输

对于 T=0 协议, 只要求 IC 卡回送数据或只包含送向 IC 卡的命令数据的 C-APDU, 可直接映射到 T=0 命令 C-TPDU (9.3 中的情况 2 和情况 3)。既不需要 IC 卡接收、也不要求 IC 卡回送数据的 C-APDU, 以及要求 IC 卡接收数据并回送数据(9.3 中情况 1 和 4)的 C-APDU 将通过 9.3 中定义的 T=0 的传输规则进行传输。

9.2.3 T=0 时的错误检测及纠错

在 T=0 协议中, 错误检测及纠错是必须的, 但不适用于复位应答过程。

若字符没有正确地接收到或者接收正确但校验不正确, 接收方应在字符起始位的前沿脉冲之后的 10.5 ± 0.2 个 etu 内, 向 I/O 发送持续 1-2 个 etu 时间的低电平信号, 表示有错误发生。

发送方应在字符起始位前沿脉冲发出后的 11 ± 0.2 个 etu 内, 检测 I/O 的电平状态。此时若 I/O 为高电平状态, 则表明字符已准确收到。

若发送方检测到错误, 就应在检出错误之后至少延迟 2 个 etu, 并重复发送一次有错误嫌疑的字符, 最多只发送三次。

9.3 传输层

本节描述了在终端和 IC 卡之间命令和响应 APDU 的传输机制。APDU 是命令或响应报文。由于命令和响应报文都可以包含数据, TTL 应能处理在 9.4 中定义的命令的四种格式。C-APDU 和 R-APDU 的组成在 9.4.1 和 9.4.2 中描述。

TAL 传送 C-APDU 到 TTL。在发送到 IC 卡之前, 应将其变换成传输协议认可的形式。IC 卡处理完命令后, 以 R-APDU 的格式将数据 (如果存在的话) 和状态码回送给 TTL。

9.3.1 C-APDU 和 R-APDU 的映射方式和数据交换

如何将 C-APDU 映射到 T=0 命令头取决于命令情况。如何将 IC 卡回送的数据 (如果存在) 和状态码映射到 R-APDU 取决于回送数据的长度。

由 IC 卡回送的过程字节 SW1 SW2=‘61xx’和 SW1 SW2=‘6Cxx’用来控制 IC 卡和 TTL 之间的数据交换, 它不会回送给 TAL。过程字节 SW1 SW2=‘61xx’或 SW1 SW2=‘6Cxx’表示命令在 IC 卡中的处理没有完成。

如果 IC 卡回送给 TTL 的状态码是 SW1 SW2='9000'，表示正常完成了命令的处理。任何其他的状态码都表明 IC 卡中断了命令的处理，处理失败的原因在状态码中指出。TTL 收到来自 IC 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、警告还是错误情况。

以下描述的是将 IC 卡回送的数据和状态字节构造成 R-APDU 格式的方法，仅适用于 IC 卡已成功完成了命令处理，或全部数据（如果存在）在过程字节'61xx'和'6Cxx'的控制下已被 IC 卡返回的情况。INS、INS 和'60'过程字节的详细使用在此不作描述。

9.3.1.1 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'。

交换流程如下：

——TTL 发送 T=0 的命令头到 IC 卡；

——IC 卡回送状态码给 TTL。

完成命令处理后，由 IC 卡向 TTL 回送的状态码不加改变地映射到 R-APDU 必备的尾域。

注：IC 卡应分析 T=0 命令头，判断是命令情况 1 还是命令情况 2 在请求最大长度的响应数据。

9.3.1.2 情况 2

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'Le'被映射到 T=0 命令头的 P3。

交换流程如下：

——TTL 发送 T=0 的命令头到 IC 卡；

——在过程字节的控制下，IC 卡向 TTL 回送数据和状态（在非正常处理时只返回状态）。

注：在 IC 卡回送的过程控制字节'61xx'和'6Cxx'的控制下，TTL 可以要求重发 T=0 命令头，并使用“GET RESPONSE”命令从 IC 卡取回数据。

完成命令处理后，由 IC 卡向 TTL 回送的数据（如果存在）和状态按照下述方法映射到 R-APDU：

(i)如果 $Le \geq Licc$ ，回送数据被映射到 R-APDU 的条件体，返回的状态无变化地被映射到 R-APDU 必备的尾域。

(ii)如果 $Le < Licc$ ，回送数据的前 Le 字节被映射到 R-APDU 的条件体中，返回的状态无变化地被映射到 R-APDU 必备的尾域。

9.3.1.3 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。

交换流程如下：

——TTL 发送 T=0 的命令头到 IC 卡；

——如果 IC 卡回送一个过程字节而不是状态码，则在此过程字节的控制下，TTL 向 IC 卡发送 C-APDU 条件体的部分数据。如果 IC 卡回送状态码 SW1 SW2，TTL 将中断命令处理过程；

——如果处理过程没有在步骤 2 处中断，则 IC 卡返回命令处理结束后的状态。

IC 卡完成命令处理后回送给 TTL 的状态码，或由 IC 卡返回的引起 TTL 中断命令处理的状态码，都不加改变地映射到 R-APDU。

9.3.1.4 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。

交换流程如下：

——TTL 发送 T=0 命令头到 IC 卡；

——如果 IC 卡回送一个过程字节而不是状态码，则在此过程字节控制下，TTL 给 IC 卡发送 C-APDU 条件体的部分数据。如果 IC 卡回送状态码 SW1 SW2，TTL 将中断命令处理过程；

——如果处理过程在步骤 2 中没有中断，IC 卡应回送过程字节‘61xx’给 TTL，请求 TTL 发出“GET RESPONSE”命令从 IC 卡取回数据。在命令处理的这个阶段中，IC 卡不应回送状态码 SW1 SW2=‘9000’。TTL 应发送“GET RESPONSE”命令到 IC 卡取回提及的数据，小于或等于 IC 卡回送的过程字节‘61xx’中的‘xx’字节值的数据指定为“GET RESPONSE”命令的长度字节。这样，“GET RESPONSE”命令可以同情况 2 的命令一样处理。在过程字节控制下，IC 卡向 TTL 回送数据和状态码（或在非正常处理情况下，只有状态码）。

完成命令处理后，IC 卡回送给 TTL 的数据（如果存在）和状态码，或仅是引起 TTL 终止命令处理过程的状态码，按照下述规则映射到 R-APDU：

(i)如果 $Le \geq Licc$ ，回送的数据被映射到 R-APDU 的条件体，返回的状态不加改变地被映射到 R-APDU 必备的尾域。

(ii)如果 $Le < Licc$ ，回送数据的前 Le 个字节被映射到 R-APDU 的条件体，返回的状态不加改变地被映射到 R-APDU 必备的尾域。

9.3.2 过程字节‘61xx’和‘6Cxx’的使用

由 IC 卡回送到 TTL 的过程字节‘61xx’和‘6Cxx’指明了 TTL 取回当前正在处理的命令请求数据的方式。在 T=0 协议下，这些过程字节仅仅用在命令情况 2 和 4 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 $\leq 'xx'$ 。

过程字节‘6Cxx’通知 TTL 立即重发前条命令，同时命令头置为 P3=‘xx’。

命令情况 2 和 4 在容错处理过程中，使用过程字节的规定如下：在发生错误时，IC 卡回送错误或警告状态码而不是‘61xx’或‘6Cxx’。

9.3.2.1 命令情况 2

如果 IC 卡收到一个命令情况 2 的头并且 $Le \neq Licc$ ，应回送过程字节‘6CLicc’（或状态码指出一个警告或错误情况，而非 SW1 SW2=‘9000’）通知 TTL 立即重发 P3=Licc 的命令头。

注：这是对“GET RESPONSE”命令的有效响应。

如果 IC 卡收到命令情况 2 的头并且 $Le = Licc$ ，IC 卡在过程字节控制下，或者回送请求的数据和相关状态码，或者回送过程字节‘61xx’（或表明警告或错误情况的状态码，而非 SW1 SW2=‘9000’）通知 TTL 按最大长度‘xx’发出“GET RESPONSE”命令。

9.3.2.2 命令情况 4

如果 IC 卡收到一个命令情况 4 的命令，处理完随 C-APDU 一同发送来的数据之后，应回送过程字节‘61xx’（或表明警告或错误情况的状态码，而非 SW1 SW2=‘9000’），通知 TTL 按最大长度‘xx’发出“GET RESPONSE”命令。

此时发出的“GET RESPONSE”命令的处理方法参见 9.3.2.1 中的描述。

9.3.3 GET RESPONSE 命令

TTL 发出“GET RESPONSE”命令，是为了从 IC 卡取得对应于命令情况 2 和 4 的 C-APDU 的 Le 字节的数据。

命令报文的结构见表 18：

表 18 GET RESPONSE 命令报文结构

代码	值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Le	预期数据的最大长度

正常处理结束后，IC 卡回送状态码 SW1 SW2=‘9000’和 Licc 字节的数据。

在错误情况发生后，错误状态码(SW1 SW2)的编码见表 19：

表 19 GET RESPONSE 错误响应

SW1	SW2	含义
‘64’	‘00’	“GET RESPONSE”失败
‘67’	‘00’	域长度错误
‘6A’	‘86’	P1 P2 ≠ ‘00’

9.4 应用层

应用协议由 TAL 和 TTL 之间一组有序的数据交换组成，本节的后续部分定义了应用协议。

应用层交换的每一步由命令-响应对组成，其中 TAL 通过 TTL 给 IC 卡发送命令，IC 卡处理该命令后通过 TTL 返回一个响应给 TAL。每一个特定的命令都与一个特定的响应相匹配。一个 APDU 就是一个命令报文或一个响应报文。

命令报文和响应报文都可以包含数据，传输协议通过 TTL 来管理四种命令情况，如表 20 所示：

表 20 APDU 中数据存在的情况

情况	命令数据	响应数据
1	无	无
2	无	有
3	有	无
4	有	有

注：由于安全报文传送总有数据（至少是 MAC）要送往 IC 卡，因此对安全报文传送而言，只存在情况 3 和 4 的命令。当使用安全报文传送时，情况 1 的命令就变为情况 3，情况

2 的命令就变为情况 4。

9.4.1 C-APDU

C-APDU 包含一个必备的、连续四字节的命令头，用 CLA、INS、P1 和 P2 表示，同时包括一个可变长度的条件体。

命令头定义如下：

——CLA：指令类型，除‘FF’外可赋任何值。

——INS：指令码，只有在最低位为‘0’，且高半字节既不是‘6’也不是‘9’时，INS 才有效。

——P1 P2：参数字节。

注：每一个命令头的完整定义将在《社会保障（个人）卡》规范第 5 部分：命令中描述。

条件体定义如下：

——Lc 占一个字节，定义了 C-APDU 中发送数据的字节数。Lc 的取值范围从 1 到 255。

——在 C-APDU 中将要发送的数据，字节数由 Lc 定义。

——Le 占一个字节，指出期望在 R-APDU 中返回的最大字节数。Le 的取值范围从 0 到 255；如果 Le=0，期望返回数据的最大字节数是 256。

注：每一个命令的条件体中各数据域的完整定义将在《社会保障（个人）卡》规范第 5 部分：命令中描述。

可能的 C-APDU 结构的四种情况见表 21：

表 21 C-APDU 的情况

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

9.4.2 R-APDU

R-APDU 是一串字节，这一串字节由一个条件体以及必备的两字节状态码 SW1 SW2 组成。

条件体是一串数据字节，其最大长度在 C-APDU 中的 Le 中定义。

必备的状态码标明 IC 卡在处理完命令后的状态。

SW1 SW2 的编码遵循下述规定：

——SW1 的高半字节是‘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；

——命令正常结束时，SW1 SW2 的取值为‘9000’；

——当 SW1 的高半字节为‘9’，且低半字节不为‘0’时，其含义依赖于相关的应用；

——当 SW1 的高半字节为‘6’，且低半字节不为‘0’时，SW1 的含义与应用无关。

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）所代表的含义将在《社会保障（个人）卡》规范第 5 部分：命令中描述。