

# 中国金融集成电路（IC）卡 借记/贷记规范

## 第五部分：与应用无关的 IC 卡与终端 接口需求

中国金融集成电路（IC）卡标准修订工作组  
二零零四年三月

# 目 录

1. 范围.....	5
2. 参考资料.....	6
3. 定义.....	7
4. 缩写、符号和术语.....	9
第 I 部分 .....	13
机电特性、逻辑接口与传输协议.....	13
1. 机电接口.....	14
1.1 IC 卡的机械特性 .....	14
1.1.1 物理特性.....	14
1.1.2 触点的尺寸和位置 .....	14
1.1.3 触点的分配 .....	15
1.2 IC 卡电气特性 .....	15
1.2.1 测量约定.....	16
1.2.2 输入/输出 (I/O).....	16
1.2.3 编程电压 (VPP).....	17
1.2.4 时钟 (CLK).....	17
1.2.5 复位 (RST).....	17
1.2.6 电源电压(VCC).....	17
1.2.7 触点电阻.....	18
1.3 终端的机械特性 .....	18
1.3.1 接口设备.....	18
1.3.2 触点压力.....	19
1.3.3 触点分配.....	19
1.4 终端的电气特性 .....	19
1.4.1 测量约定.....	19
1.4.2 输入/输出 (I/O).....	19
1.4.3 编程电压(VPP).....	20
1.4.4 时钟(CLK) .....	20
1.4.5 复位(RST).....	21
1.4.6 电源电压(VCC).....	21
1.4.7 触点电阻 .....	22
1.4.8 短路保护.....	22
1.4.9 插入 IC 卡后，终端的加电和断电 .....	22

<b>2. 卡片操作过程</b>	<b>23</b>
2.1 正常卡片操作过程	23
2.1.1 操作步骤	23
2.1.2 IC 卡插入与触点激活时序	23
2.1.3 IC 卡复位	24
2.1.4 交易执行	25
2.1.5 触点释放时序	25
2.2 交易过程的异常结束	26
<b>3. 字符的物理传输</b>	<b>27</b>
3.1 位持续时间	27
3.2 字符帧	27
<b>4. 复位应答</b>	<b>28</b>
4.1 复位应答期间回送字符的物理传输	28
4.2 复位应答期间 IC 卡回送的字符	28
4.3 字符定义	29
4.3.1 TS—初始字符	30
4.3.2 T0—格式字符	30
4.3.3 TA1 到 TC3—接口字符	31
4.3.4 TCK — 校验字符	35
4.4 复位应答过程中终端的行为	35
4.5 复位应答—终端流程	36
<b>5. 传输协议</b>	<b>38</b>
5.1 物理层	38
5.2 数据链路层	38
5.2.1 字符帧	38
5.2.2 字符协议 T=0	38
5.2.3 T=0 的错误检测及纠错	40
5.2.4 块传输协议 T=1	41
5.2.5 T=1 协议的错误检测和纠正	46
5.3 终端传输层(TTL)	48
5.3.1 T=0 协议下 APDU 的传送	48
5.3.2 T=1 协议下 APDU 的传送	53
5.4 应用层	53
5.4.1 C-APDU	53
5.4.2 R-APDU	54
<b>第 II 部分</b>	<b>55</b>
<b>文件、命令和应用选择</b>	<b>55</b>

<b>6. 文件</b>	<b>56</b>
<b>6.1 文件结构</b>	<b>56</b>
6.1.1 应用数据文件(ADF)	56
6.1.2 应用基本文件(AEF)	56
6.1.3 文件到 ISO/IEC 7816-4 的文件结构的映射	56
6.1.4 目录结构	57
<b>6.2 文件引用</b>	<b>57</b>
6.2.1 通过文件名引用	57
6.2.2 通过短文件标识符(SFI)引用	57
<b>7. 命令</b>	<b>58</b>
<b>7.1 报文结构</b>	<b>58</b>
7.1.1 命令 APDU 格式	58
7.1.2 应答 APDU 格式	59
7.1.3 命令-应答 APDU 约定	59
<b>7.2 读记录(READ RECORD)命令-响应 APDU</b>	<b>59</b>
7.2.1 定义和范围	59
7.2.2 命令报文	59
7.2.3 命令报文数据域	60
7.2.4 应答报文数据域	60
7.2.5 应答报文状态码	60
<b>7.3 选择(SELECT)命令-响应 APDU</b>	<b>60</b>
7.3.1 定义和范围	60
7.3.2 命令报文	60
7.3.3 命令报文数据域	61
7.3.4 应答报文数据域	61
7.3.5 应答报文状态码	62
<b>8. 应用选择</b>	<b>64</b>
8.1 应用选择概述	64
8.2 用于应用选择的 IC 卡数据	65
8.2.1 支付系统应用标识符编码	65
8.2.2 支付系统环境结构	65
8.2.3 支付系统目录编码	66
8.2.4 其它目录的编码	67
8.3 建立候选列表	67
8.3.1 终端应用与 IC 卡应用的匹配	67
8.3.2 使用支付系统目录	68
8.3.3 使用 AID 列表	II
8.3.4 最终选择	IV

附录 .....	5
附录 A 使用 T=0 协议交换的示例 .....	6
A1 情况 1 下的命令 .....	6
A2 情况 2 下的命令 .....	6
A3 情况 3 下的命令 .....	6
A4 情况 4 下的命令 .....	7
A5 采用过程字节‘61’和‘6C’的情况 2 命令 .....	7
A6 采用过程字节‘61’的情况 4 命令 .....	7
A7 带警告条件的情况 4 命令 .....	8
附录 B 数据元表 .....	9
附录 C 目录结构示例 .....	12
C1 目录结构示例 .....	12

## 1. 范围

本规范描述了与确保集成电路卡(IC 卡)和终端正确操作和互操作的应用无关的最低功能需求。附加的专用功能亦可能提供,但不在本规范规定之列,其互操作性不能保证。

第一册包括两部分:

第 I 部分 — 机电特性、逻辑接口和传输协议

第 II 部分 — 文件、命令和应用选择

第 I 部分定义了用于 IC 卡和终端之间信息交换的机电特性、逻辑接口和传输协议。具体包括:

- IC 卡和终端的机械性能、电压和信号参数。
- 卡片操作过程的概述。
- 通过复位应答过程建立 IC 卡和终端的通讯。
- 面向字节和面向块的异步传输协议。

第 II 部分定义了用于 IC 卡和终端之间信息交换的数据元、文件和命令。具体包括:

- 数据元和它们在数据对象中的映射。
- 文件的结构和引用方式。
- 应用选择时, IC 卡和终端之间的交换报文的结构及编码。

同时,它还从 IC 卡和终端的角度分别定义了应用选择的过程。此过程所需的卡片数据和文件的逻辑结构以及使用卡片结构的终端逻辑亦在此部分描述。

本规范建立在 ISO/IEC 7816 系列标准之上,使用时应该参照这些规范。但是,如果本规范内的规定和定义与上述标准不同,则以本规范为准。

本规范的适用于 IC 卡和终端生产商、支付系统的系统设计者和开发 IC 卡金融应用的人员。

## 2. 参考资料

本规范引用了以下标准所包含的规定

EMV2000 版本 4.0: 2000 年 12 月	支付系统的集成电路卡应用规范第三册—应用规范
ISO/FDIS 639-1:2001	名称及语言表示代码
ISO/IEC 7811-1:1995	识别卡—记录技术—第 1 部分: 凸印
ISO/IEC 7811-3:1995	识别卡—记录技术—第 3 部分: 凸印字符在 ID-1 卡片上的位置
ISO/IEC 7816-1:1998	识别卡 带触点的集成电路卡 第 1 部分: 物理性能
ISO/IEC 7816-2:1999	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 7816-3:1997	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 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 8859: 1987	信息处理—8 位单字节编码的图形字符集
ISO/IEC 10373:1993	识别卡—测试方法

### 3. 定义

本规范使用以下术语：

应用 Application	卡片和终端之间的应用协议和相关的数据集
块 Block	包含两个或三个域(头域、信息域、尾域)的字符组
字节 Byte	8 个二进制位(bit)
卡片 Card	支付系统定义的支付卡片
冷复位 Cold Reset	当 IC 卡的电源电压 (VCC) 和其它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
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
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
密文 Cryptogram	加密运算的结果
下电序列	2.1.5 节定义的下电序列
Deactivation Sequence	
凸印 Embossing	在卡片正面凸起的字符
尾域 Epilogue Field	块的最后一部分，包括错误校验代码(EDC)字节
金融交易 Financial Transaction	持卡人、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
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
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下降沿之间的最小时间
静止状态 Inactive	当 IC 卡上的电源电压(VCC)和其它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
集成电路 Integrated Circuit(IC)	完成处理和/或存储功能的电子器件
集成电路卡(IC 卡) Integrated Circuit(s) Card	内部封装一个或多个集成电路用于执行处理和存储功能的卡片
集成电路模块 Integrated Circuit Module	嵌入在 IC 卡中包括 IC、IC 载体、连线和触点的子装置
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
磁条 Magstripe	包括磁编码信息的条状物
半字节 Nibble	一个字节的四位或低四位
填充 Padding	在数据串任意端补充二进制位
路径 Path	没有分隔的文件标识符的连接

支付系统 Payment System	本规范中指 Europay, Mastercard 或 Visa 信用卡组织
支付系统环境 Payment System Environment	当符合本规范的支付系统应用被选择, 或者用于支付系统应用目的的目录定义文件 (DDF) 被选择后, IC 卡中所确立的逻辑条件
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)
响应 Response	IC 卡处理完收到的命令报文后, 返回给终端的报文
信号幅度 Signal Applitude	信号高、低电压的差值
信号波动 Signal Perturbation	在正常工作中信号的异常, 如下冲/上冲、电子噪声、纹波、尖刺、串扰等。外部源引起的随机波动不在本规范之列
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
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
T=0	面向字符的异步半双工传输协议
T=1	面向块的异步半双工传输协议
模板 Template	结构数据对象的值域, 定义为数据对象的逻辑分组
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, 也可包括其它部件和接口, 例如与主机通讯的接口
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

#### 4. 缩写、符号和术语

本规范使用以下缩写、符号和术语：

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	应用文件定位器(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)
ASI	应用选择标识(Application Selection Indicator)
ATR	复位应答(Answer to Reset)
b	二进制(Binary)
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	摄氏或摄氏度
C-APDU	命令 APDU(Command APDU)
CIN	输入电容(Input Capacitance)
CLA	命令报文的类别字节(Class Byte of the Command Message)
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)
DC	直流
DDF	目录定义文件(Directory Definition File)
DF	专用文件(Dedicated File)
DIR	目录(Directory)
DIS	国际标准草案
EDC	错误检测代码(Error Detection Code)
EF	基本文件(Elementary File)
etu	基本时间单元(Elementary Time Unit)
FCI	文件控制信息(File Control Information)
f	频率(Frequency)
GND	地(Ground)
hex.	十六进制(Hexadecimal)
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)
IFSI	信息域大小整数(Information Field Size Integer)
IIH	高电平输入电流(High Level Input Current)
IIL	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)
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)
k $\Omega$	千欧
Lc	终端应用层 (TAL) 在情况 3 或情况 4 命令中发出数据的实际长度(Exact Length of Data Sent by the TAL in a Case 3 or 4 Command)
Le	在情况 2 或情况 4 命令中返回给终端应用层 (TAL) 的数据最大期望长度(Maximum Length of Data Expected by the TAL in Response to a Case 2 or 4 Command)
Licc	IC 卡在响应接收到的情况 2 或情况 4 命令时卡内有效或剩余的数据 (由 IC 卡决定) 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)
Lr	响应数据域的长度(Length of Response Data Field)
LRC	冗余校验(Longitudinal Redundancy Check)
l.s.	最低位
M	必备(Mandatory)
$\mu$ m	微米
mA	毫安
MAC	报文鉴别代码(Message Authentication Code)
max.	最大值
MF	主文件(Mater File)
MHz	兆赫
min	最小值
mm	毫米
m.s.	最高位

mΩ	兆欧
m/s	米/秒
μ A	微安
μ s	微秒
N	牛顿
n	数字型(Numeric)
NAD	节点地址(Node Address)
NAK	否定的确认(Negative Acknowledgment)
nAs	纳安秒
ns	纳秒
O	可选(Optional)
P1	参数 1(Parameter 1)
P2	参数 2(Parameter 2)
P3	参数 3(Parameter 3)
PCB	协议控制字节(Protocol Control Byte)
PDOL	处理选项数据对象列表(Processing Options Data Object List)
pF	皮法
PSE	支付系统环境(Payment System Environment)
PTS	协议类型选择(Protocol Type Selection)
R-APDU	响应 APDU(Response APDU)
R-block	接收就绪块(Receive Ready Block)
RFU	保留(Reserved for Future Use)
RID	注册应用提供商标识(Registered Application Provider Identifier)
RST	复位(Reset)
R-TPDU	响应 TPDU(Response TPDU)
SAD	源节点地址(Source Node Address)
S-block	管理块(Supervisory Block)
SFI	短文件标识符(Short File Identifier)
SW1	状态字 1(Status Word One)
SW2	状态字 2(Status Word Two)
TAL	终端应用层(Terminal Application Layer)
TCK	校验字符(Check Character)
t <sub>F</sub>	信号幅度从 90%下降到 10%的时间(Fall Time Between 90% and 10% of Signal Amplitude)
TLV	标签、长度、值(Tag Length Value)
TPDU	传输协议数据单元(Transport Protocol Data Unit)
t <sub>R</sub>	信号幅度从 10%上升到 90%的时间(Rise Time Between 10% and 90% of Signal Amplitude)
TTL	终端传输层(Terminal Transport Layer)
V	伏特(Volt)
var.	变长(Variable)

---

VCC	VCC 触点上的测得电压(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	编程电压(Programming Voltage)
WI	等待时间整数(Waiting Time Integer)
WTX	等待时间扩展(Waiting Time Extension)
‘0’—‘9’	16 个十六进制数字(16 hexadecimal digits)
‘A’—‘F’	
xx	任意值
专用的	本规范内未定义或/和超出本规范范围的
必须	表示强制的要求
应该	表示推荐的要求

## 第 I 部分

### 机电特性、逻辑接口与传输协议

1. 机电接口

本章包括 IC 卡和终端的电气、机械特性。IC 卡和终端的规范指标有所不同，其目的是为防止对 IC 卡的损坏而预留安全余地。

本章定义的 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。

1.1 IC 卡的机械特性

本节描述了 IC 卡的物理特性、触点分配和机械强度。

1.1.1 物理特性

除本节的特殊规定外，IC 卡应满足 ISO 7816-1 中规定的物理特性。同时 IC 卡应该满足 ISO/IEC 7816-1 定义的其它特性，如紫外线、X-射线、触点的表面断面、机械强度、电磁特性、抗静电特性等的要求，并能在上述条件下正确地运行。

1.1.1.1 模块高度

IC 模块表面的最高点不应高于卡表面平面 0.10mm。

IC 模块表面的最低点不应低于卡表面平面 0.10mm。

1.1.2 触点的尺寸和位置

触点的尺寸和位置必须如图 1 所示：

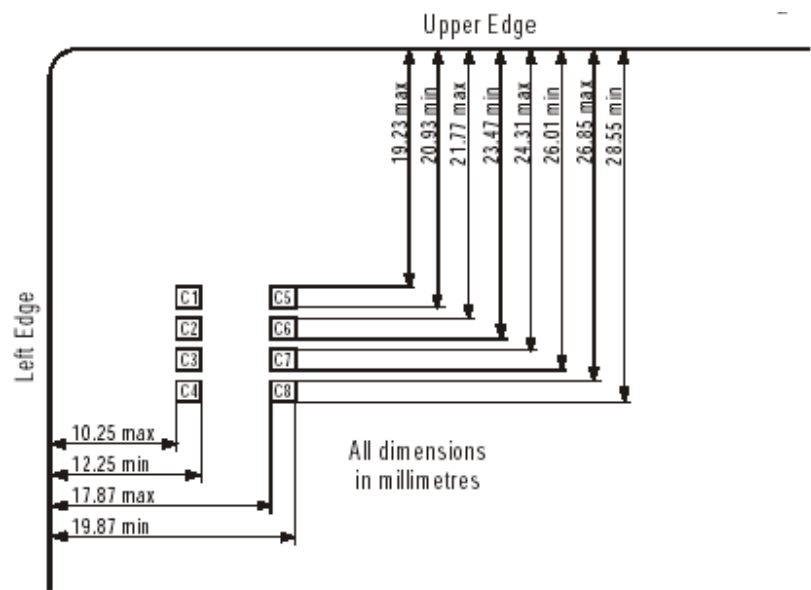


图 1 — IC 卡触点的位置和尺寸

区域 C1、C2、C3、C5 和 C7 表面必须用导电层完全覆盖，构成 IC 卡的基本触点。区域 C4、C6、C8 和 ISO/IEC7816-2 附录 B 所定义的区域 Z1 到 Z8 可以选择导电表面，但强烈建议 Z1 到 Z8 区域无导电表面。如果区域 C6 和 Z1 到 Z8 有导电表面，则它们必须和集成电路(IC)、相互之间以及其它触点区域在电路隔离<sup>1</sup>。同时，任何两个导电区域之间除了通过 IC 都不能导通。基本触点必须如表 1 所示分配。

触点相对于凸印及/或磁条的布局必须如图 2 所示：

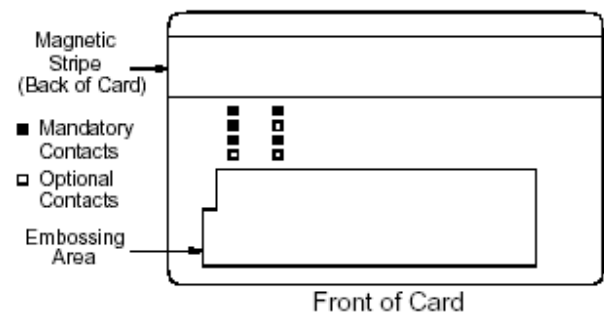


Figure 2 - Layout of Contacts

图 2 — 触点的布局

注：必须注意不能让凸印破坏 IC。同时，在 IC 背面的签名条签字过重亦可能造成 IC 的破坏。

1.1.3 触点的分配

IC 卡上触点的分配遵循 ISO 7816-2 的规定，如表 1 所示：

C1	电源电压(VCC)	C5	接地(GND)
C2	复位信号(RST)	C6	未使用 <sup>2</sup>
C3	时钟信号(CLK)	C7	输入/输出(I/O)

表 1 — IC 卡触点的分配

C4 和 C8 未使用，可以不作实际设置。

1.2 IC 卡电气特性

本节描述了在 IC 卡触点上测量出的信号的电气特性。

<sup>1</sup> 电路上隔绝意味着：在此触点和任何其它导电表面上施以 5V DC 电压时在二者上测得的电阻必须  $\geq 10\text{M}\Omega$ 。  
<sup>2</sup> ISO/IEC 7816 定义为编程电压（VPP）

1.2.1 测量约定

所有测量均应在 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℃。IC 卡必须能够在 0℃～50℃之间正确操作。所有流入 IC 卡的电流均视为正值。

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

1.2.2 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(发送模式)向终端传送数据。在操作过程中，IC 卡和终端不能同时处于发送模式，若万一发生此情况，I/O 触点的状态(电平)将处于不确定状态，但不能损坏 IC 卡。

1.2.2.1 接收模式

在接收模式下，当电源电压(VCC)在 5.1.2.6 节中规定的范围内时，IC 卡必须能正确地解释特性如表 2 所示的来自终端的信号：

符 号	最小值	最大值	单 位
V <sub>IH</sub>	0.7×V <sub>CC</sub>	V <sub>CC</sub>	V
V <sub>IL</sub>	0	0.8	V
t <sub>R</sub> 和 t <sub>F</sub>	—	1.0	μs

表 2 — IC 卡接收模式下 I/O 的电气特性

注：在-0.3V 到 V<sub>CC</sub>+0.3V 范围内的 I/O 信号干扰不应损坏 IC 卡。

1.2.2.2 发送模式

在发送模式下，IC 卡必须向终端传送特性如表 3 所示的数据：

符号	条 件	最小值	最大值	单位
V <sub>OH</sub>	-20μA<I <sub>OH</sub> <0, V <sub>CC</sub> =min.	0.7×V <sub>CC</sub>	V <sub>CC</sub>	V
V <sub>OL</sub>	0<I <sub>OL</sub> <1mA, V <sub>CC</sub> =min.	0	0.4	V
t <sub>R</sub> 和 t <sub>F</sub>	C <sub>IN(终端)</sub> = 30pF max.	—	1.0	μs

表 3 — IC 卡发送模式下 I/O 的电气特性

除向终端发送数据时，IC 卡应将其 I/O 信号驱动模式设置为接收模式，且不要求 I/O 具备任何电流源性能。

### 1.2.3 编程电压 (VPP)

IC 卡不需要编程电压 VPP(见 1.3.3 的注释)

### 1.2.4 时钟 (CLK)

当 VCC 在 1.2.6 节所规定的范围内时, IC 卡必须能在具有表 4 所示特性的时钟信号作用下正常工作:

符 号	条 件	最小值	最大值	单 位
$V_{IH}$		$V_{CC}-0.7$	$V_{CC}$	V
$V_{IL}$		0	0.5	V
$t_R$ 和 $t_F$	$V_{CC}=\text{min. 到 max.}$	—	9%的时钟周期	$\mu s$

表 4 — 到 IC 卡的 CLK 电气特性

注: 在-0.3V 到  $V_{CC}+0.3V$  范围内的 CLK 端干扰信号不应损坏 IC 卡。

当时钟占空因数处于其稳定运行周期的 44%~56%之间时, IC 卡必须能正常工作。

当时钟频率处于 1MHz 到 5MHz 之间时, IC 卡必须能正常工作。

注: 在卡片操作过程中, 频率值必须由终端维持在复位应答期间所用频率的 $\pm 1\%$ 之内。

### 1.2.5 复位 (RST)

当 VCC 在 1.2.6 节所规定的范围内时, IC 卡必须能正确的解释具有表 5 所示电气特性的复位信号:

符号	条 件	最小值	最大值	单 位
$V_{IH}$		$V_{CC}-0.7$	$V_{CC}$	V
$V_{IL}$		0	0.6	V
$t_R$ 和 $t_F$	$V_{CC}=\text{min. 到 max.}$	—	1.0	$\mu s$

表 5 — RST 的电气特性

注: 在-0.3V 到  $V_{CC}+0.3V$  范围内的 RST 端的干扰信号不应损坏 IC 卡。

IC 卡必须利用激活的低复位信号, 采用异步方式进行复位应答。

### 1.2.6 电源电压 (VCC)

在电源电压  $V_{CC}$  为  $5V \pm 0.5V$  直流电的情况下, IC 卡必须能正常工作。此时, 时钟频率应在 1.2.4 节中所规定的范围内, 最大电流为 50mA。

注: 建议 IC 卡的电流损耗尽可能低。在以后颁布的标准中, IC 卡所允许的最大损耗电流将被降低。当 IC

卡中存在多个应用时，应确保 IC 卡的电流损耗与其可能用到的所有终端均能相匹配。

1.2.7 触点电阻

在整个设计寿命期间，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)必须小于 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。

1.3 终端的机械特性

本节描述了终端接口设备的机械特性。

1.3.1 接口设备

用于插入 IC 卡的接口设备必须具备接收 IC 卡的能力，并具有以下特性：

- 物理特性满足 ISO/IEC 7816-1 的规定
- 正面触点位置应满足 ISO/IEC 7816-2 中图 2 的规定。
- 凸印应满足 ISO/IEC 7811-1 和 3 的规定

接口设备的触点分布必须保证如图 3 所示的 IC 卡插入后，所有触点都可以正确导通。除了用于导通 IC 卡的 C1 到 C8 的触点之外，接口设备不应该有其它触点。

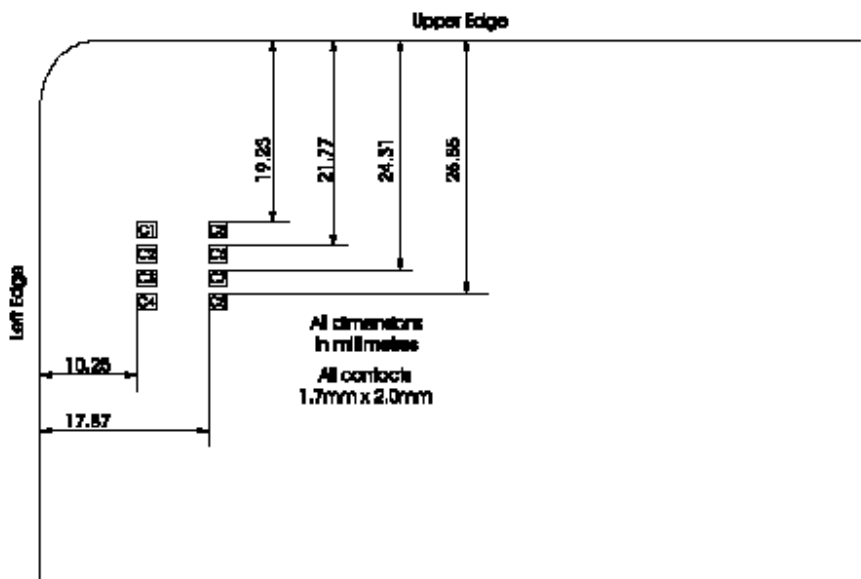


图 3 — 终端触点分布和尺寸

定位的导轨和夹板(如果使用)不应损坏 IC 卡，尤其不能损坏卡上磁条、签名条、凸印和全息标志等区域。

注：作为一个基本原则，持卡人应在任何时候都能将 IC 卡插入或拔出。因而接口设备上插入 IC 卡位置处，应该配有一种机械设备，使持卡人能够在设备发生故障(如掉电)时取回 IC 卡。

1.3.2 触点压力

任何一个接口设备触点对相应的 IC 卡触点所施加的压力应在 0.2N 到 0.6N 之间。

1.3.3 触点分配

接口设备触点的分配如表 6 所示。

C1	电源电压(VCC)	C5	地(GND)
C2	复位信号(RST)	C6	未使用 <sup>3</sup>
C3	时钟信号(CLK)	C7	输入/输出(I/O)

表 6 — 接口设备触点的分配

C4 和 C8 不使用，在物理上可以不存在。

1.4 终端的电气特性

本节描述了在 IFD 触点上测量出的信号的电气特性。

1.4.1 测量约定

除非生产商另有指明，所有测量应是在 IC 卡和接口设备之间的触点上进行，并以 GND 为参考。环境温度范围为 5℃~40℃。必须限制终端的内部温度，以防损坏 IC 卡。  
所有流出终端的电流均为正值。

1.4.2 输入/输出 (I/O)

该触点作为输出端(发送模式)向 IC 卡传送数据，作为输入端(接收模式)从 IC 卡接收数据。在操作过程中，终端和 IC 卡不能同时处于发送模式,若万一发生此情况，I/O 触点的状态(电平)将处于不确定状态，但不应损坏终端。  
当终端和 IC 卡都处于接收模式时,触点必须处于高电平状态。除非 VCC 加电并稳定在 1.4.6 节中允许的范围内，终端不应将 I/O 置于高电平状态。见 2.1.2 节有关触点激活的内容。  
在任何情况下，均应将流入或流出 I/O 触点的电流限定在±15mA 以内。

<sup>3</sup> ISO/IEC 7816 中定义为编程电压（VPP）。

1.4.2.1 发送模式

在发送模式下，终端必须向 IC 卡传送特性如表 7 所示的数据：

符号	条 件	最小值	最大值	单位
$V_{OH}$	$0 < I_{OH} < 20\mu A, V_{CC} = \min.$	$0.8 \times V_{CC}$	$V_{CC}$	V
$V_{OL}$	$-0.5mA < I_{OL} < 0, V_{CC} = \min.$	0	0.4	V
$t_R$ 和 $t_F$	$C_{IN(IC)} = 30pF \text{ max.}$	—	0.8	$\mu s$
信号干扰	低电平	-0.25	0.4	V
	高电平	$0.8 \times V_{CC}$	$V_{CC} + 0.25$	V

表 7 — 发送模式下的终端 I/O 电气特性

除向 IC 卡传送数据时，终端应将其 I/O 信号驱动模式设置为接收模式。

1.4.2.2 接收模式

在接收模式下，终端必须能正确解释从 IC 卡发来的具有表 8 所示特性的信号：

符 号	最小值	最大值	单 位
$V_{IH}$	$0.6 \times V_{CC}$	$V_{CC}$	V
$V_{IL}$	0	0.5	V
$t_R$ 和 $t_F$	—	1.2	$\mu s$

表 8 — 接收模式下的终端 I/O 电气特性

1.4.3 编程电压 (VPP)

C6 必须在电气上隔离。电气隔离意味着在 C6 和其它任何触点上施以 5V DC 的电压时，二者之间的电阻应该  $\geq 10M\Omega$ 。如果在终端中导通，则 C6 必须在整个卡片操作过程中保持在 GND 和  $1.05 \times V_{CC}$  之间。

注：在新终端中隔离 C6 可以把它用于本规范未来版本可能规定的其它用途上。

1.4.4 时钟 (CLK)

终端必须产生具有表 9 所示特性的时钟信号：

符号	条 件	最小值	最大值	单位
$V_{OH}$	$0 < I_{OH} < 50\mu A, V_{CC} = \min.$	$V_{CC} - 0.5$	$V_{CC}$	V
$V_{OL}$	$-50\mu A < I_{OL} < 0, V_{CC} = \min.$	0	0.4	V

$t_R$ 和 $t_F$	$C_{IN(ICC)}=30pF\ max.$	—	8%的时钟周期	$\mu s$
信号干扰	低电平	-0.25	0.4	V
	高电平	$V_{CC}-0.5$	$V_{CC}+0.25$	

表 9 — 终端 CLK 的电气特性

稳定运行时，时钟占空因数应在其周期的 45%~55%之间。

频率范围必须在 1MHz~5MHz 之间，且在整个交易期间，除非通过复位应答采用了专用的协商技术，其变化范围不应超过±1%(见 5.2 节)。

1.4.5 复位 (RST)

终端必须产生具有表 10 所示特性的复位信号：

符号	条件	最小值	最大值	单 位
$V_{OH}$	$0<I_{OH}<50\mu A$ , $V_{CC}=\min.$	$V_{CC}-0.5$	$V_{CC}$	V
$V_{OL}$	$-50\mu A<I_{OL}<0$ , $V_{CC}=\min.$	0	0.4	V
$t_R$ 和 $t_F$	$C_{IN(ICC)}=30pF\ max.$	—	0.8	$\mu s$
信号干扰	低电平	-0.25	0.4	V
	高电平	$V_{CC}-0.5$	$V_{CC}+0.25$	V

表 10 — 终端 RST 的电气特性

1.4.6 电源电压 (VCC)

终端必须提供  $5V\pm0.4V$  的直流电压，并必须能稳定输出 0~55mA 的电流。终端应带有保护电路以防止在误操作如对地或 VCC 短路时所造成的损坏。误操作既可能来源于内部，也可能来自外部接口如电源干扰、通讯链路故障等。以 GND 为基准，VCC 决不可以低于-0.25V。

在正常的 IC 卡操作中，电流脉冲会在 IC 卡触点上引起 VCC 波动。电源应能抵消电量≤30nAs、持续时间≤400ns、幅度≤100mA 及电流变化率≤1mA/ns 的电流负载瞬时波动，以确保 VCC 在规定的范围之内。脉冲的最大包络参见图 4。

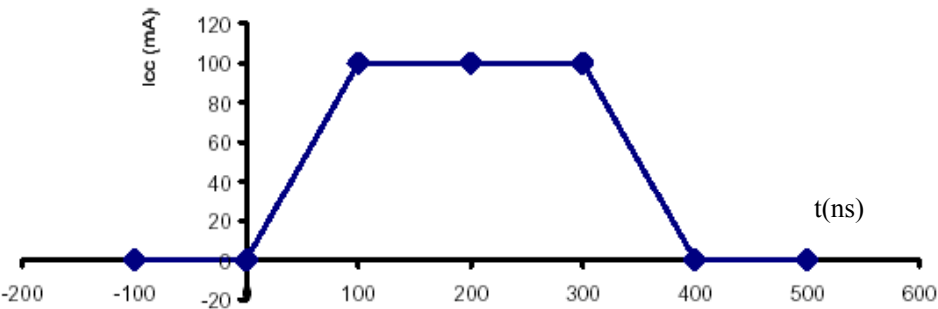


图 4 — 最大电流脉冲包络

注：如果需要，终端应能够具有大于 55mA 的传输能力，但建议终端将稳定电流限制在 200mA 以内。

#### 1.4.7 触点电阻

在终端的整个设计寿命期间，触点电阻(在清洁的接口设备和清洁的标准 IC 卡触点间测量时)应小于 500mΩ。(参见 ISO/IEC 7816-1 的测试方法)

注：标准的 IC 卡触点可以看作是在 5.00μm 的镍表面上的 1.25μm 镀金触点。

#### 1.4.8 短路保护

当任何两个触点之间发生短路时，无论时间长短，终端都不应损坏或功能失常，例如：插入一块金属板片。

#### 1.4.9 插入 IC 卡后，终端的加电和断电

插入 IC 卡后，当对终端进行加电或断电时，所有的信号电压必须保持在 1.4 节规定的范围之内，触点激活和释放的时序应分别符合 2.1.2 节和 2.1.5 节的规定。

## 2. 卡片操作过程

本节描述了从卡片插入接口设备、完成交易处理直至卡片拔出的操作过程的所有步骤。

### 2.1 正常卡片操作过程

本节描述了执行一个正常交易的操作过程。

#### 2.1.1 操作步骤

卡片的操作过程包括以下步骤：

- 将 IC 卡插入接口设备，导通并激活触点；
- 将 IC 卡复位，同时在终端和 IC 卡之间建立通讯联系；
- 进行交易处理；
- 释放触点并从接口设备中取出 IC 卡。

#### 2.1.2 IC 卡插入与触点激活时序

当 IC 卡插入接口设备时，终端应确保其所有触点处于低电平状态( $V_{OL}$  符合 1.4 节的规定， $V_{CC}$  在触点接触时必须小于或等于 0.4V)。当 IC 卡正确插入接口设备以后，触点必须按如下方式激活(参见图 5)：

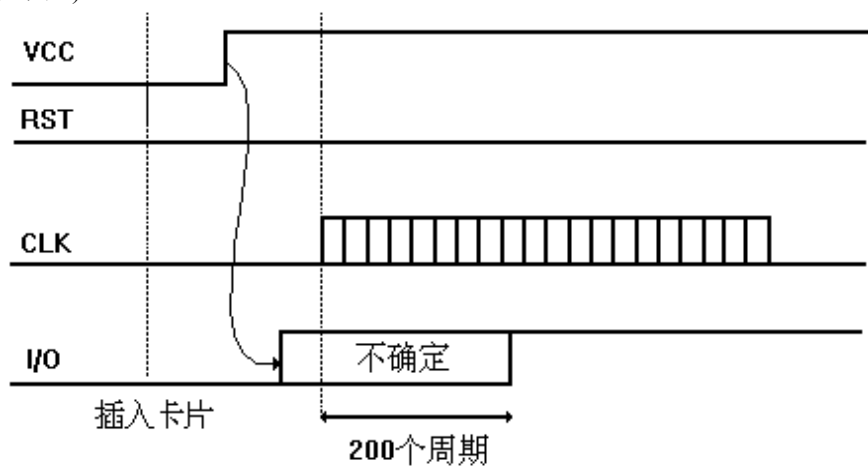


图 5 — 触点激活时序

- 终端必须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 激活之前给 Vcc 加电；
- 终端确认 Vcc 稳定在 1.4.6 节所规定的范围内以后，必须将 I/O 置于接收模式并提供 1.4.4 节规定的合适、稳定的时钟。终端可以在时钟启动之前即将其 I/O 置于接收模式，但最迟也不得超过时钟启动后的 200 个时钟周期。

注：根据设计，终端可以通过测量、等待足够的等待时间使之稳定或通过其它方式来确定 Vcc 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。

2.1.3 IC 卡复位

IC 卡必须利用激活的低复位信号，采用异步方式进行复位应答。  
复位应答(ATR)的传送方式在第 3 节中描述，而其内容在 4.2 和 4.3 节中描述。

2.1.3.1 冷复位

在 2.1.2 节所述的触点激活后，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 6)，过程如下：

- 终端必须在 T0 时启动 CLK。
- 在 T0 后的不超过 200 个时钟周期内，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 T0 后最迟不超过 200 个时钟周期内置为高电平；
- 终端应从 T0 开始保持 RST 为低电平状态 40,000 到 45,000 个时钟周期直到 T1，然后将 RST 置为高电平状态；
- IC 卡上 I/O 的复位应答将在 T1 后的 400 到 40,000 个时钟周期(如图 6 中的 t1 所示)内开始；
- 终端必须在 T1 之后 380 个时钟周期之内打开一个接收窗口且不能在 T1 之后 42,000 个时钟周期内关闭(如图 6 中 T1 所示)。如果没有收到来自 IC 卡的复位应答信息，终端必须在不早于 T1 后 42,001 个时钟周期之后、不晚于 T1 后 42,000 个时钟周期加 50ms 之前启动释放时序。

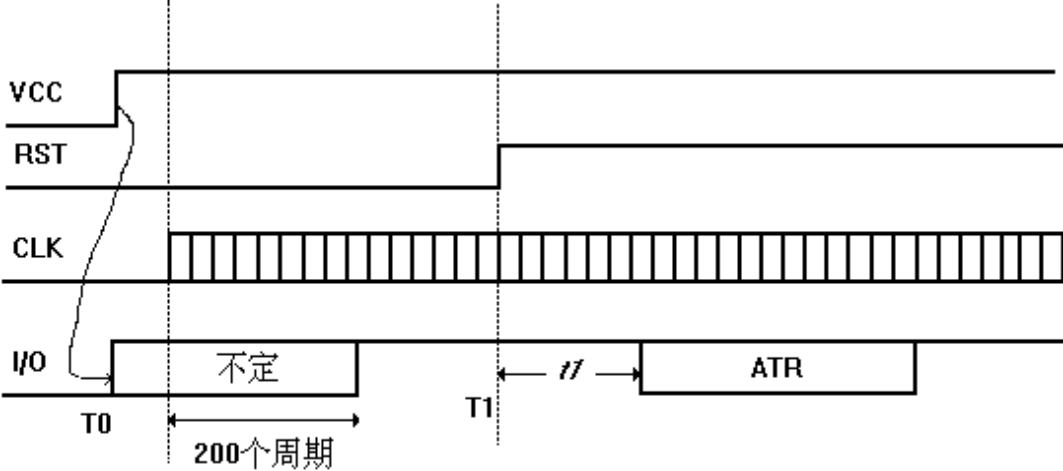


图 6 — 冷复位时序

### 2.1.3.2 热复位

在 2.1.3 节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本规范第 4 节中的规定,终端将启动热复位并从 IC 卡获得复位应答(见图 7)。其过程如下:

- 热复位必须从  $T0'$  开始,此时终端将 RST 置为低电平状态;
- 在整个热复位时序中,终端必须根据 1.4.4 节和 1.4.6 节的规定保持  $V_{CC}$  和 CLK 的稳定;
- 在  $T0'$  后的不超过 200 个时钟周期内,IC 卡和终端将其 I/O 置为接收模式。因此其 I/O 应确保在  $T0'$  后最迟不超过 200 个时钟周期内置为高电平;
- 终端应从  $T0'$  开始保持 RST 为低电平状态 40,000 到 45,000 个时钟周期直到  $T1'$ ,然后将 RST 置为高电平状态;
- IC 卡上 I/O 的复位应答将在  $T1'$  后的 400 到 40,000 个时钟周期(如图 7 中的  $t1'$  所示)内开始;
- 终端必须在  $T1'$  之后 380 个时钟周期之内打开一个接收窗口且不能在  $T1'$  之后 42,000 个时钟周期内关闭(如图 7 中  $T1'$  所示)。如果没有收到来自 IC 卡的复位应答信息,终端必须在不早于  $T1'$  后 42,001 个时钟周期之后、不晚于  $T1'$  后 42,000 个时钟周期加 50ms 之前启动释放时序。

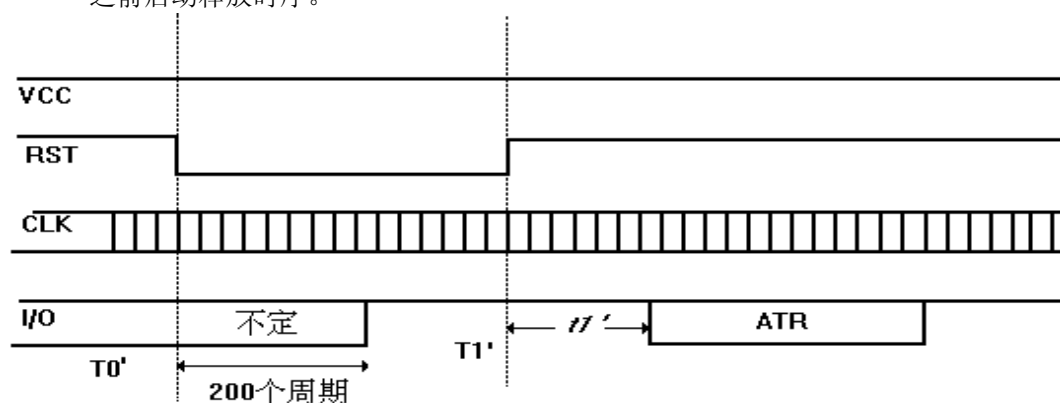


图 7 — 热复位时序

### 2.1.4 交易执行

IC 卡中的应用选择和随后 IC 卡和终端的信息交换在本规范第 8 部分中描述。

### 2.1.5 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片从接口设备中拔出),终端必须如下释放接口设备触点(见图 8):

- 终端必须通过把 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  $V_{CC}$  断电之前,终端必须将 CLK 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，终端必须切断 VCC 电源。此时的 Vcc 应小于或等于 0.4V。
- 释放过程必须在 100ms 内完成。这一时间段从 RST 置于低电平状态开始到 Vcc 达到或低于 0.4V 为止。

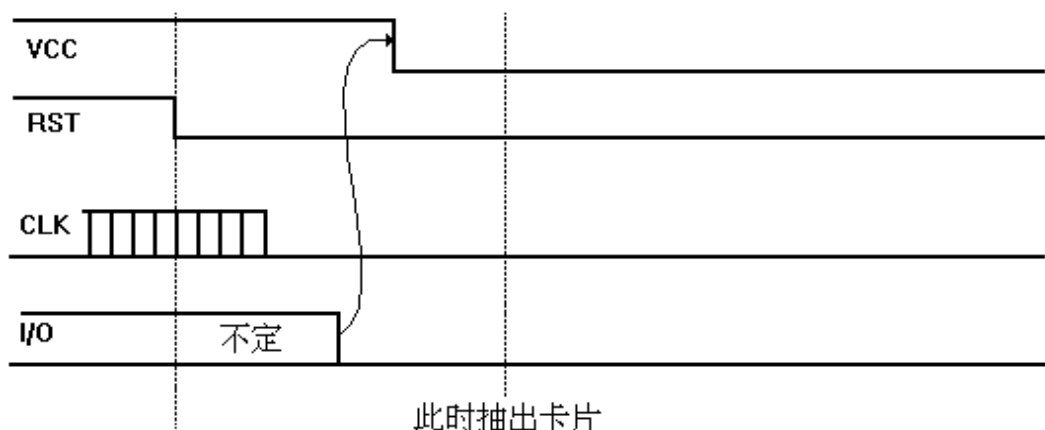


图 8 — 触点释放时序

## 2.2 交易过程的异常结束

在交易过程中，如果 IC 卡以最高 1m/s 的速度过早地从终端中拔出，终端必须能够检测到 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 2.1.5 节描述的方式释放接口设备的所有触点。在这种情况下，IC 卡的电气或机械特性不能受到损坏。

注：对于滑触式结构的接口设备，终端有可能检测到 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 卡和接口设备的触点脱离之前必须释放触点。

### 3. 字符的物理传输

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输。终端向 IC 卡提供一个用作数据交换的时序控制时钟信号。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,并在第 5 节中描述的两种传输协议中使用。

#### 3.1 位持续时间

在 I/O 上使用的位持续时间定义为基本时间单元(etu)。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 (和全局参数 F 和 D 的确定, 参见第 4 节) 后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  $\frac{372}{f}$ 。除非另有说明, 以后所提到的 etu, 均为当前 etu。

#### 3.2 字符帧

数据在 I/O 上以如下所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 4.3.1 节)。

字符传输之前, 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 9):

- 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, 采样时间应小于或等于 0.2etu。

一个字符中的逻辑‘1’的数目必须是偶数, 8 个数据位和校验位自身均参加校验计算, 但起始位不参加校验计算。

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, 起始位的存在性必须在 0.7etu 之内验证, 后续各位必须在(n+0.5±0.2)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, 从起始位的下降沿到第 n 位的后沿之间的时间是(n±0.2)etu。

两个连续字符起始位下降沿之间的间隔时间, 等于字符持续时间(10±0.2)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 将被设置为低电平状态, 以向发送方表明出现错误(见 5.2.3 节)。

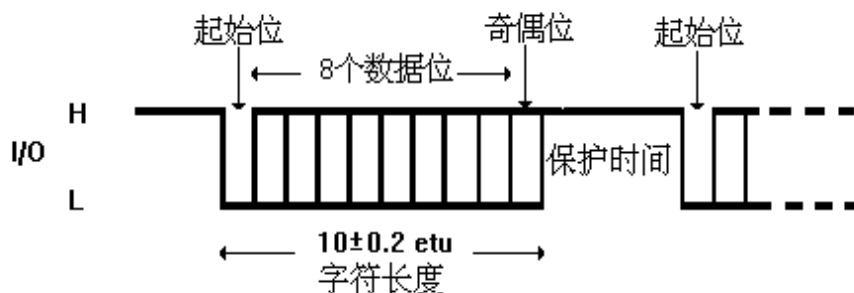


图 9 — 字符帧

在终端传输层(TTL)，数据总是采用高字节先送方式(m.s.)在 I/O 上传输。一个字节内部二进制位的传输顺序(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 4.3 节)。

#### 4. 复位应答

如 2.1.3 节所述，终端发出复位信号以后，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片和终端之间即将建立的通讯的特性。传输这些字节的方法及字节的含义在下面描述。

注：在第 4 节和第 5 节中，一个字符的最高位指的是 b8 位，最低位是 b1 位。在单引号中的值表示以十六进制值编码，例如：‘3F’。

##### 4.1 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。

位持续时间在 3.1 节定义，字符帧在 3.2 节定义。

在复位应答过程中，两个连续字节的起始位下降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。

在复位应答期间，IC 卡应在 19,200 个初始 etu<sup>4</sup>内发送完所有要回送的字符。发送时间应从第一个字符(TS)起始位的下降沿开始，到最后一个字符起始位下降沿后的 12 个初始 etu 为止。

##### 4.2 复位应答期间 IC 卡回送的字符

在复位应答期间，IC 卡回送字符的数目和编码随传输协议和所支持的传输控制参数值的不同而不同。本节中描述了两基本的复位应答：一种是针对支持 T=0 协议的 IC 卡，另一种是针对 T=1 协议的 IC 卡(卡片只支持其中一种)。本节还规定了回送字符和传输控制参数值的允许范围。IC 卡回送两种复位应答的任何一种，均能保证操作的正确性和与符合本规范的终端的互操作性。

<sup>4</sup> 因为 etu 代表的周期与频率相关（见 3.1），复位应答的最大时间会随时钟频率的变化而变化。

根据特殊需要，IC 卡可以选择支持多种传输协议，但其中之一必须是 T=0 或 T=1，且首选协议必须是 T=0 或 T=1。除非终端因为特殊需要而支持选择 IC 卡提供的其它协议的机制，终端必须使用首选协议对卡片进行操作。对这种机制的支持不作要求，亦不在本规范的规定之列。

注：本规范不支持同时支持 T=0 和 T=1 协议的 IC 卡。这种 IC 卡的读写只能通过专用的方法完成，而这不在本规范规定之列。

基于同样的考虑，IC 卡还可以选择支持由发卡行确定的其它传输控制参数值，但这已超出本规范的范围。符合本规范的终端可以拒绝这种卡片，且不必为支持这种卡片而增加相应的特殊功能。

在两种基本复位应答中，IC 卡回送的字符如表 11 和表 12 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(基于字符的异步半双工传输协议)的 IC 卡，其回送字符如表 11 所示：

字符	值	备 注
TS	‘3B’或‘3F’	指明正向或反向约定
T0	‘6X’	TB1 和 TC1 存在，X 表示历史字节的存在个数
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 4.3.3.3 节)

表 11 — T=0 时的基本 ATR

对于采用 T=1 协议(基于块的异步半双工传输协议)的 IC 卡，其回送字符如表 12 所示：

字符	值	备 注
TS	‘3B’或‘3F’	指明正向或反向约定
T0	‘Ex’	TB1 到 TD1 存在，x 表示历史字节的存在个数
TB1	‘00’	不使用 VPP
TC1	‘00’到‘FF’	表明所需额外保护时间的数量，‘FF’值为特定含义值(见 4.3.3.3)
TD1	‘81’	TA2 到 TC2 不存在，TD2 存在；使用 T=1 协议
TD2	‘31’	TA3 和 TB3 存在，TC3 和 TD3 不存在，使用 T=1 协议
TA3	‘10’到 ‘FE’	返回 IFSI, 表示 IC 卡信息域大小的初始值且具有 16~254 字节的 IFSC
TB3	高位半字节‘0’到‘4’，低位半字节‘0’到‘5’	BWI=0 到 4 CWI=0 到 5
TCK	见 4.3.4 节	校验字符

表 12 — T=1 时的基本 ATR

4.3 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“基本应答”信息指明。基本应答描述既不排除其它字符值的使用，也不排斥发卡行增加或删减字符。例如，如果 IC 卡支持多个传输协议，它可以

回送附加字符(见第 5 节)。但是,只有在 IC 卡返回一个基本 ATR,或返回一个下面描述的满足最低功能需求的终端所支持的 ATR 时,才能保证字符的正确交换。

符合本规范的终端仅需支持本部分描述的基本 ATR(最小功能)及一些附加要求。终端可以拒绝不按此要求返回 ATR 的 IC 卡。此外,终端可以具备正确解释不符合本规范但由专用 IC 卡(如:国内专用)返回的 ATR 的能力。这种功能并非强制性要求,且超出了本规范的范围。作为一个基本原则,终端应接受回送非基本 ATR 的 IC 卡,只要终端能正确处理该 ATR 即可。

终端必须能对复位应答返回的字符进行奇偶校验,但不必即时校验。如果终端检测到校验错,它必须拒绝 IC 卡。

在以下描述中,如果指明终端必须

- 拒绝复位应答,则意味着终端必须在拒绝冷复位后执行热复位,或在拒绝热复位后释放触点以结束卡片操作过程。
- 拒绝 IC 卡,则意味着终端必须释放触点以结束卡片操作过程。
- 接受复位应答,则意味着终端必须在本节规定的对其它所有字符的要求都满足的情况下接受复位。

每个字符的描述按以下结构组织:

- 标题
- ISO/IEC 7816-3 描述的用途
- EMV 基本应答。为保证互操作性,热复位应答中必须包括这些字符。
- 如果终端收到 EMV 规定范围之外的字符,终端的规定动作。

#### 4.3.1 TS—初始字符

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

使用反向逻辑约定时,I/O 的低电平状态等效于逻辑‘1’,且该数据字节的最高位在起始位之后首先发送。

使用正向逻辑约定时,I/O 的高电平状态等效于逻辑‘1’,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 为以下两个值之一:

- (H)LHLLLLLLLLH—反向约定,值为‘3F’
- (H)LHHLHHHLLH—正向约定,值为‘3B’

冷复位和热复位的约定可能不同。

终端要求:终端必须能够同时支持反向和正向约定,并接收 IC 卡回送的值为‘3B’或‘3F’的 TS,但应拒绝接受其它 TS 值。

注:强烈推荐使用‘3B’作为 IC 卡的回送值,因为在以后的版本中可能不再支持‘3F’。

#### 4.3.2 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 13—T0 字符的基本应答编码)。

基本响应：当仅选择 T=0 时，IC 卡应回送 T0='6x'，表示字符 TB1 和 TC1 存在；当仅选择 T=1 时，IC 卡应回送 T0='Ex'，表示字符 TB1 到 TD1 存在。‘x’的值表示要回送的可选历史字符的数目。

终端要求：在 T0 回送值正确且包含了所需的接口字符(TA1 到 TD1)和历史字符时，终端应接受包含任何 T0 值的 ATR。

	b8	b7	b6	b5	b4	b3	b2	b1
T=0	0	1	1	0	x	x	x	x
T=1	1	1	1	0	x	x	x	x

表 13 — T0 的基本响应编码

#### 4.3.3 TA1 到 TC3—接口字符

在复位应答后的终端和 IC 卡信息交换期间，TA1 到 TC3 表示传输控制参数 F、D、I、P、N、IFSC、块等待时间整数（BWI）及字符等待时间整数（CWI）的值。这些参数用于 ISO/IEC 7816-3 中定义的 T=1 协议。TA1, TB1, TC1, TA2 和 TB2 传送的信息将用于后续数据交换且与所使用的协议类型无关。

##### 4.3.3.1 TA1

TA1 传送 FI 和 DI 的值，其中：

- 高半字节 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。
- 低半字节 DI 用于确定 D 的值，D 为位速率调节因子。用于调整复位应答之后所使用的位持续时间。

ATR 后的位持续时间(当前 etu)的计算方法见 3.1。

在复位应答期间使用的缺省值 FI=1 和 DI=1，分别表示 F=372 和 D=1。

基本响应：ATR 不包括 TA1，因而在后续交换中使用缺省值 F=372 和 D=1。

终端要求：如果 ATR 中存在 TA1(T0 的 b5 设为‘1’)且 TA2 的 b5='0'(具体模式、参数由接口字符定义)，则

- 如果 TA1 的值在‘11’到‘13’之间，终端必须接收 ATR，且必须立即采用指明的 F 和 D 值(F=372, D=1, 2, 4)。
- 如果 TA1 的值不在‘11’到‘13’之间，终端必须拒绝 ATR，除非它可以支持并立即采用指明的条件。

如果 ATR 中返回 TA1(T0 的 b5 设为‘1’)且 TA2 没有返回(协商模式)，终端必须接收 ATR 且继续在后续信息交换过程中使用缺省值 D=1 和 F=372，除非它支持使用协商参数的特殊方法。

如果 ATR 中没有返回 TA1，则后续交换中使用缺省值 D=1 和 F=372。

#### 4.3.3.2 TB1

TB1 传送 PI1 和 II 的值，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。PI1=0 表示不使用此参数。
- b8 位不使用，置为逻辑‘0’。

基本响应：ATR 中必须包含 TB1=‘00’，表示 IC 卡不使用 VPP。

终端要求：在冷复位应答中，终端只能接收 TB1=‘00’的 ATR。在热复位应答中，终端必须能够接收 TB1 为任何值的 ATR(只要 T0 的 b6 置为‘1’)或不包括 TB1 的 ATR(如果 T0 的 b6 设为‘0’)；此时终端必须当作 TB1=‘00’，继续后续操作。终端不提供编程电压 VPP。

注：终端可以保持 Vpp 为静止状态 (见 1.3.3)。

字符 TB1 的基本响应代码如表 14 所示：

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

表 14 — TB1 的基本响应编码

#### 4.3.3.3 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下降沿之间的时间。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下降沿之间的最小延迟时间可减少到 12 个 etu，而在使用 T=1 协议时可减小到 11 个 etu。

注：TC1 只适用于终端向 IC 卡发送的两个连续字符间的时序，而不适用于 IC 卡向终端发送字符的情况，也不适用于在相反方向发送字符的情况，见 5.2.2.1 节和 5.2.4.2.2 节。

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，额外保护时间必须在 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，使用 T=1 协议时为 11 个 etu。

基本响应：IC 卡必须回送‘00’到‘FF’之间的 TC1 值。

终端要求：终端必须能够接收不包含 TC1 的 ATR(只要 T0 的 b7 置为‘0’)，如果接收了这样的 ATR，则它必须继续卡片操作过程，就象回送了 TC1=‘00’一样。

字符 TC1 的基本响应代码如表 15 所示：

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

表 15 — TC1 的基本响应编码

注：强烈推荐将 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 卡之间的通讯缓慢，这样会延长交易时间。

4.3.3.4 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：当仅选用 T=0 协议时，IC 卡不回送 TD1，且以 T=0 协议作为后续传输类型的缺省值。当选用 T=1 协议时，IC 卡将回送 TD1=‘81’，表示 TD2 存在，且后续传输协议类型为 T=1 协议。

终端要求：如果回送值正确且包含了所需的接口字符 TA2 到 TD2，则终端必须接受这样的 ATR，即其所回送的 TD1 的高半字节为任意值且低半字节的值为‘0’或‘1’。终端必须拒绝包含其它 TD1 值的 ATR。

字符 TD1 的基本响应编码如表 16 所示：

b8	b7	b6	b5	b4	b3	b2	b1
1	0	0	0	0	0	0	1

表 16 — TD1 的基本响应编码(T=1)

4.3.3.5 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 卡不回送 TA2，TA2 不存在表示以协商模式工作。

终端要求：如果在复位应答期间 TA2 的 b5=0,且终端能够支持 IC 卡返回的接口参数所指明的确切条件，终端应该接受包含 TA2 的 ATR，并立即使用这些条件。否则，终端应拒绝接受含有 TA2 的 ATR。

4.3.3.6 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 卡不回送 TB2。

终端要求：终端应该拒绝包含 TB2 的 ATR。

注：终端可以保持 Vpp 为空闲状态(见 1.3.3)。

4.3.3.7 TC2

TC2 专用于 T=0 协议，传输工作等待时间整数(WI)，WI 用来确定由 IC 卡发送的任意一个字符起始位下降沿与 IC 卡或终端发送的前一个字符起始位下降沿之间的最大时间间隔。工作等

待时间为：960×D×WI。

基本响应：IC 卡不回送 TC2，且后续通讯中使用缺省值 WI=10。

终端要求：终端必须：

- 拒绝包含 TC2='00'的 ATR。
- 接收包含 TC2='0A'的 ATR。
- 拒绝 TC2 为其它任何值的 ATR，除非它可以支持。

#### 4.3.3.8 TD2

TD2 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 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；
- 低半字节用于表示后续信息交换所使用的协议类型，当选用 T=1 协议类型时，该低半字节值为'1'。

基本响应：当选用 T=0 协议时，IC 卡不回送 TD2，且以 T=0 协议作为后续传输类型的缺省值。当选用 T=1 协议时，IC 卡将回送 TD2='31'，表示 TA3 和 TB3 存在，且后续传输协议类型为 T=1。

终端要求：如果回送值正确且包含了所需的接口字符 TA3 到 TD3，则终端不能拒绝这样的 IC 卡。即，其所回送 TD2 的高半字节为任意值且低半字节的值为'1'或'E'（如果 TD1 的低半字节为 '0'）。终端应拒绝 IC 卡回送其它的 TD2 值。

字符 TD2 的基本响应编码如表 17 所示：

b8	b7	b6	b5	b4	b3	b2	b1
0	0	1	1	0	0	0	1

表 17 — TD2 的基本响应编码(T=1)

#### 4.3.3.9 TA3

TA3(如果 TD2 中指明 T=1)回送 IC 卡的信息域大小整数(IFSI)，IFSI 决定了 IFSC，并指明了卡片可接收的块信息区域的最大长度(INF)。TA3 以字节形式表示 IFSC 的长度，其取值范围从'01'到'FE'。'00'和'FF'保留为将来使用。

基本响应：如果选用 T=1 协议则 IC 卡应回送'10'到'FE'之间的 TA3 值，表明初始 IFSC 在 16 到 254 字节范围内。

终端要求：如果 TD2 的 b5 位为'0'，则终端不能拒绝不回送 TA3 的 IC 卡，但如果终端接受了这样的 IC 卡，则应令 TA3='20'来继续卡片操作过程。终端应拒绝那些回送的 TA3 值在'00'到'0F'之间或为'FF'的 IC 卡。

字符 TA3 的基本响应编码如表 18 所示：

	b8	b7	b6	b5	b4	b3	b2	b1
T=1	x	x	x	x	x	x	x	x
'00'到'0F'和'FF'不允许								

表 18 — TA3 的基本响应编码

## 4.3.3.10 TB3

TB3(如果 TD2 中指明 T=1)表明了用来计算 CWT 和 BWT 的 CWI 和 BWI 值, TB3 由两部分组成。低半字节(b1-b4)用于表明 CWI 值, 而高半字节(b5-b8)用于表明 BWI 值。

基本响应: 在选用 T=1 协议的前提下, IC 卡应回送这样的 TB3: 低半字节取值为‘0’到‘5’, 高半字节取值为‘0’到‘4’。即: CWI 的值在 0 到 5 之间, BWI 的值在 0 到 4 之间。

字符 TB3 的基本响应编码如表 19 所示:

	b8	b7	b6	b5	b4	b3	b2	b1
T=1	0	x	x	x	0	y	y	y
xxx 取值范围为 000 到 100								
yyy 取值范围为 000 到 101								

表 19 — TB3 的基本响应编码

终端要求: 终端应拒绝以下的 ATR: 不包含 TB3, 包含 BWI 大于 4 和/或 CWI 大于 5 的 TB3, 或包含使  $2^{CWI} \leq (N + 1)$  的 TB3。终端应接受包含其它 TB3 值的 ATR。

注: N 为 TC1 中指定的额外保护时间。若 TC1=255, N 的值必须置为 -1。当 T=1 时, 由于 CWI 所规定的最大值是 5, TC1 的值应在‘00’与‘1E’之间或等于‘FF’, 以避免 TC1 与 TB3 之间的矛盾。

## 4.3.3.11 TC3

TC3(如果 TD2 中指明 T=1)指明了所用的块错误检测代码的类型, 所用代码类型用 b1 位表示, b2 到 b8 位未使用。

基本响应: ATR 不应包含 TC3, 表明用纵向冗余校验(LRC)作为错误代码。

终端要求: 终端必须能够接收包括 TC3=‘00’的 ATR, 而拒绝 TC3 为其它任何值的 ATR。

## 4.3.4 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的结果为零。

基本响应: 在使用 T=0 协议时, IC 卡不回送 TCK。而在其它情况下, IC 卡应回送 TCK。

终端要求: 当 TCK 正确返回时, 终端必须能校验它。如果仅选择 T=0 协议, 终端必须能够接受不包含 TCK 的 ATR。其它情况下, 终端必须拒绝不包含 TCK 或 TCK 不正确的 ATR。

## 4.4 复位应答过程中终端的行为

在 IC 卡的触点如 2.1.2 节所描述的那样激活之后, 终端应启动一个如 2.1.3.1 节所定义的冷复位。然后执行以下步骤:

- 如果终端如 4.3 节的描述拒绝 IC 卡, 则它必须在 ATR 的 TS 起始位的下降沿开始的 24,000 个初始 etu(19,200 + 4,800 初始 etu)之内启动下电时序。

- 如果终端根据 4.3 节的描述拒绝接受冷复位应答，则它不应立即终止卡片操作过程，而必须在冷复位的 TS 起始位的下降沿开始的 24,000 个初始 etu( $19,200 + 4,800$  初始 etu)之内置 RST 为低电平，启动热复位。
- 如果终端如 4.3 节的描述拒绝热复位应答，则它必须在热复位的 TS 起始位的下降沿开始的 24,000 个初始 etu( $19,200 + 4,800$  初始 etu)之内启动下电时序。
- 终端必须能够接收两个连续字符的起始位下降沿的最小间隔为 11.8etu 的 ATR。
- 终端必须能够接收两个连续字符的起始位下降沿的最大间隔为 10,080 初始 etu( $9,600$  初始 etu + 480 初始 etu)的 ATR。如果某个字符没有接收到，则终端必须在最后一个接收到的字符(之后发生超时的字符)的起始位下降沿开始的 14,400 个初始 etu( $9,600$  初始 etu + 4,800 初始 etu)之内启动下电时序，结束卡片操作。
- 终端必须能够接收总持续时间小于或等于 20,160 初始 etu 的 ATR。如果 ATR(热复位或冷复位)未完成，则终端必须在 TS 的起始位的下降沿开始的 24,000 个初始 etu( $19,200 + 4,800$  初始 etu)之内启动下电时序，结束卡片操作。
- 如果终端在 ATR 中接收到的字符里检测到校验错，则它必须在 TS 的起始位下降沿开始的 24,000 个初始 etu( $19,200 + 4,800$  初始 etu)之内启动下电时序，结束卡片操作。
- 在接收到了符合上述时序的有效冷复位或热复位应答后，终端必须使用接收到的参数继续卡片操作过程。终端可以在有效 ATR 的最后一个字符(由位图字符 T0 和/或 TDi 指明)和 TCK(如果存在)接收到以后继续卡片操作过程。在继续传输之前，终端必须从有效 ATR 最后一个字符起始位的下降沿开始至少等待所用协议规定的保护时间( $T=0$  为 16etu， $T=1$  为 BGT)。

#### 4.5 复位应答—终端流程

图 10 显示了 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第 4 节中规定的实例。

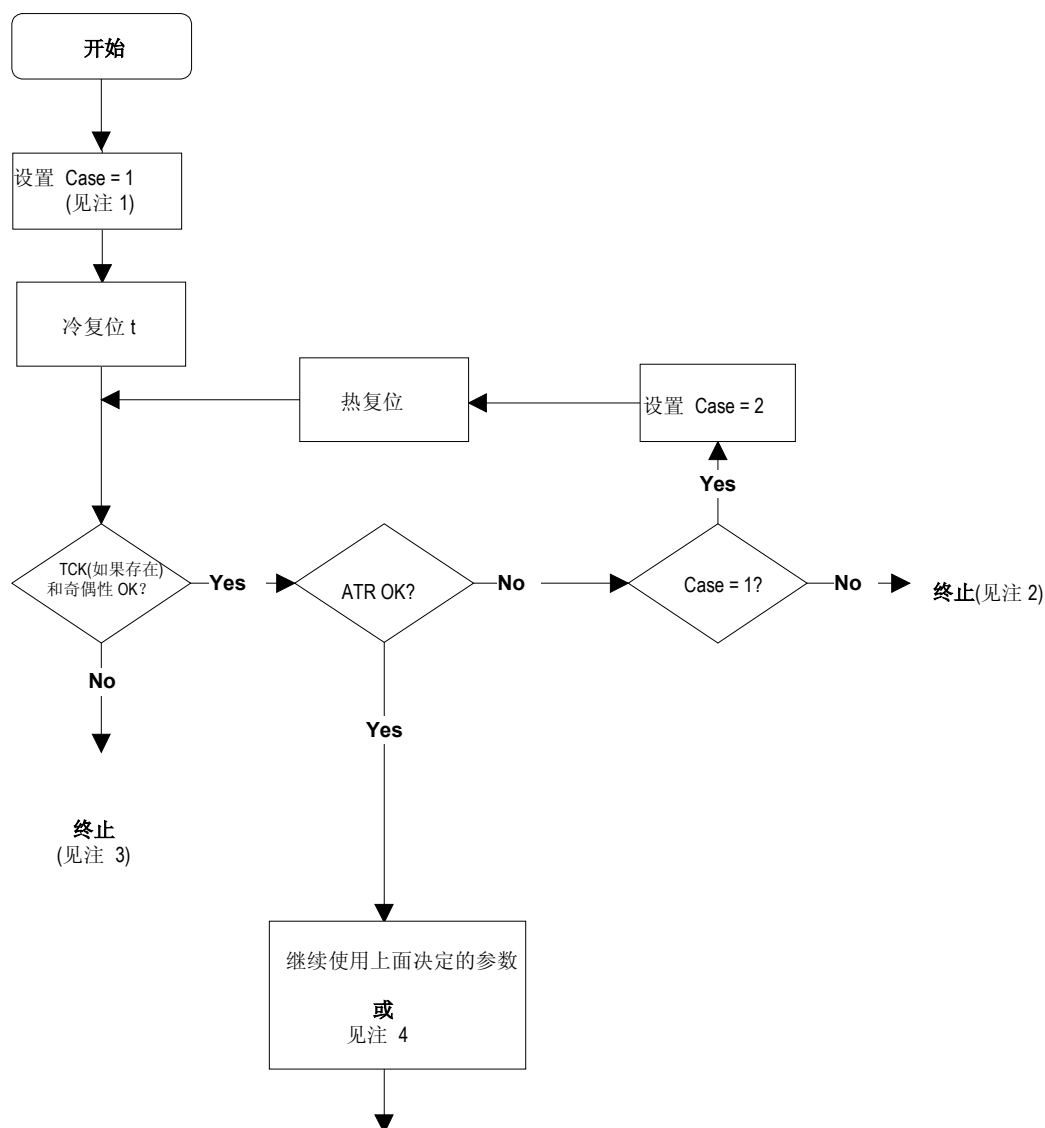


图 10 ATR—终端上的流程图

注 1: “case”是一个过程变量，用来表示是执行冷复位还是执行热复位。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 卡可能根据商业协议在此终端接受。终端应在卡片插入前事先做好准备，以便接受这种卡。随后的处理过程也是专用的，不在本规范之列。

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

注 4: 本规范以外的专用交易操作可以通过使用协议选择程序而在此处被启动。

## 5. 传输协议

本章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。

这里定义了两种协议：字符传输协议(T=0)和块传输协议(T=1)。IC 卡必须支持 T=0 协议或 T=1 协议。终端必须支持两种协议。TD1 规定了后续传输中采用的传输协议(T=0 或 T=1)，如果 TD1 在 ATR 中不存在，则假定 T=0。由于没有 PTS 过程，在复位应答之后，由 IC 卡指明的协议将立即被采用。在 ATR 中提供的其它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，是两个协议的公共部分。
- 数据链路层，包含以下定义：
  - 字符帧，定义了字符交换，是两种协议的公共部分。
  - T=0，定义了 T=0 时的字符交换。
  - 对 T=0 的检错与纠错。
  - T=1，定义了 T=1 时的块交换。
  - 对 T=1 的检错与纠错。
- 传输层，定义了针对每个协议的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。

### 5.1 物理层

T=0 与 T=1 协议均使用了物理层和第 3 节中定义的字符帧。

### 5.2 数据链路层

本节描述了传输协议 T=0 和 T=1 的时序、具体选项和错误处理。

#### 5.2.1 字符帧

在 3.2 节中定义的字符帧适用于 IC 卡与终端之间所有的报文交换。

#### 5.2.2 字符协议 T=0

##### 5.2.2.1 具体选项 — 用于 T=0 的时序

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下降沿之间的最小时间间隔在 12 和 266 个 etu 之间(见 4.2 和 4.3 节)。这一时间间隔可以小于在相反方向发送的两个连续字符之间的最小间隔 16etu。如果 TC1 返回的值是 N，IC 卡必须能够正确解释从终端传来的相邻字符起始位下降沿最小间隔为  $11.8 + N \text{ etu}$  的连续字符。

IC 卡发送到终端的两个连续字符起始位下降沿之间的最小时间间隔为 12 个 etu。终端必须能够正确解释从 IC 卡传来的相邻字符起始位下降沿最小间隔为 11.8etu 的连续字符。

IC 卡发送的任意字符的起始位下降沿与 IC 卡或终端发送的前一个字符的起始位下降沿之间的最大时间间隔(工作等待时间)不能超过  $960 \times D \times W1 = 9600$  个 etu。(D 和 W1 分别在 TA1 和 TC2 中返回。)

终端必须能够正确解释 IC 卡发送的起始位下降沿与 IC 卡或终端发送的上一个字符的起始位下降沿最大间隔为  $WWT + (D \times 480)$  etu 的字符。如果没有接收到字符,终端必须在发生超时的字符起始位下降沿开始的  $WWT + (D \times 9600)$  etu 内启动下电时序。

对于 IC 卡和终端,在相反方向发送的两个连续字符的起始位下降沿之间的最小时间间隔不能小于 16 个 etu。IC 卡或终端必须能够正确解释接收到的其起始位下降沿和最后发送的字节起始位下降沿间隔为 15etu 的字符。此处的时序不适用于重发字符。

### 5.2.2.2 命令头

命令均由终端应用层(TAL)发出,它用 5 个字节组成的命令头通过 TTL 向 IC 卡发送指令。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;
- P3: 根据不同的 INS, P3 指明发送给 IC 卡的命令中数据的字节长度或期待 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-TPPU), 命令应用协议数据单元(C-APPU)到 C-TPPU 的映射将在 5.3 节中描述。

TTL 传送 5 个字节的命令头给 IC 卡并等待一个过程字节。

### 5.2.2.3 命令处理

IC 卡收到命令头以后向 TTL 回传过程字节或状态字节 SW1 SW2(以后简称“状态”)。TTL 和 IC 卡在二者之间的命令和数据交换的任何时刻都必须知道数据流的方向和 I/O 线路由谁驱动。

#### 5.2.2.3.1 过程字节

过程字节向 TTL 表明它必须执行的动作。其编码与 TTL 动作的对应关系如表 20 所示:

过程字节值	动作
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。
与 INS 字节值的补码相同( $\overline{INS}$ )	下一个数据字节将由 TTL 传送或者 TTL 将准备接收来自 IC 卡的下一个数据字节。
‘60’	TTL 提供根据本条所定义的额外工作等待时间

‘61’	TTL 必须等待另一个过程字节然后再以最大长度‘xx’向 IC 卡发送取应答（GET RESPONSE）命令头，其中‘xx’是第二个过程字节的值。
‘6C’	TTL 必须等待另一个过程字节然后再以最大长度‘xx’向 IC 卡立即重发命令头，其中 ‘xx’是第二个过程字节的值。

表 20 — 终端对过程字节的响应

在任何情况下，完成指定的动作后，TTL 必须等待下一个过程字节或状态字节。

5.2.2.3.2 状态字节

状态字节向 TTL 表明 IC 卡对命令的处理已经完成。状态字节的意义与处理的命令有关。具体参见本规范第三册第 7 节的定义。表 21 显示了 TTL 必须采取的动作和第一个状态字节的对应关系。

第一个状态字节的值	动作
‘6x’或‘9x’(除了 ‘60’, ‘61’, ‘6C’)— 状态字节 SW1	TTL 必须等待另一个状态字节(状态字 节 SW2)

表 21 — 状态字节编码

接收到第二个状态字节后，TTL 必须在应答 APDU(R-APDU)中向 TAL 回送状态字节(及其它数据—参见 5.3.1)，然后等待下一个 C-APDU。

5.2.2.4 C-APDU 的传输

采用 T=0 协议时，只包含传向 IC 卡的命令数据或只包含 IC 卡响应数据的 C-APDU,可直接映射到 C-TPDU(5.4 节中的情况 2 和情况 3)。无数据且不要求回送数据的 C-APDU，或者要求 IC 卡接收/发送数据(5.4 节中情况 1 和 4)的 C-APDU 将通过 5.4 节定义的 T=0 的 C-TPDU 传输规则进行传输。

5.2.3 T=0 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。

若接收到校验不正确的字符，接收方必须在字符起始位的下降沿之后的 10.5±0.2 个 etu 内，向 I/O 发送持续 1-2 个 etu 的低电平信号，以表示有错误发生。

发送方必须在字符起始位下降沿脉冲发出后的 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，则必须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。发送方最多再重发三次,即总共五次(最初一次、第一次重复和然后的三次重复)。

如果最后一次重发未成功，终端必须在接收到最后一个无效字符的起始位的上升沿开始的(D x 960) 个 etu 内启动下电时序(如果它是接收方)；或者在 IC 卡显示有校验错开始的(D x 960)

个 etu 内启动下电时序(如果它是发送方)。

图 11 显示了字符重发的时序。

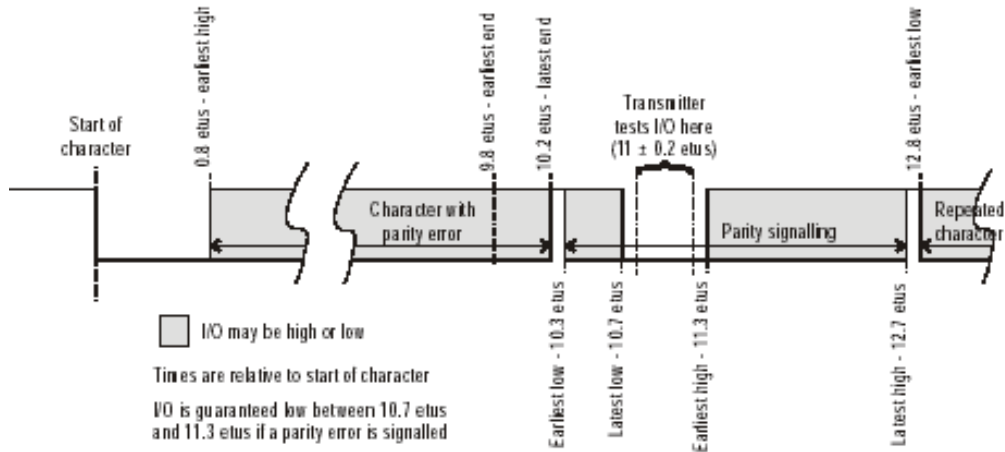


图 11—字符重发时序

在等待过程字节或状态字节时,如果 IC 卡返回的字节的值未在 5.2.2.3.1 节和 5.2.2.3.2 节中定义,则终端必须在接收到的(无效)字符起始位下降沿开始的 9,600 个 etu 以内启动下电时序。

5.2.4 块传输协议 T=1

T=1 协议在 TAL 和 IC 卡之间传送命令、R-APDU 和传输控制信息(如确认信息)。以下定义了数据链路层的块帧结构、协议的具体选项和协议操作(包括错误处理)。

5.2.4.1 块帧结构

字符帧采用 3.2 节中的定义。  
块的结构如下(参见表 21):

- 头域(必备)
- 信息域(可选)
- 尾域(必备)

头域			信息域	尾域
节点地址 (NAD)	协议控制字节 (PCB)	长度 (LEN)	APDU 或控制 信息(INF)	错误校验码 (EDC)
1 字节	1 字节	1 字节	0-254 字节	1 字节

表 22 — 块帧结构

5.2.4.1.1 头域

头域由三个必备字节组成:

- 用于标识数据块的源地址和目的地址，以及提供 VPP 状态控制的节点地址。
- 控制数据传输的协议控制字节。
- 可选的数据域长度。

5.2.4.1.1.1 节点地址

NAD 第 1 至第 3 位表明块的源节点地址(SAD)，而第 5 至第 7 位表明块的目的地址(DAD)，第 4 位和第 8 位<sup>5</sup>不用，必须设定为 0。

本规范不支持节点寻址。终端在 ATR 之后发送的块及其后终端和 IC 卡发送的块必须把 NAD 设为‘00’。

在卡片操作过程中，如果终端或 IC 卡接收到 NAD≠‘00’的块，则可以视为非法块。在这种情况下，必须使用 5.2.5 节中描述的侦错和纠错技术。

5.2.4.1.1.2 协议控制字节

PCB 表明了传输块类型，有以下三种类型：

- 用于传送 APDU 的信息块(I 块)；
- 用于传送确认(ACK 或者 NAK)的接收就绪块(R 块)；
- 用于交换控制信息的管理块(S 块)。

PCB 的编码取决于其类型，见表 23、表 24 和表 25。

b8	0
b7	序列号
b6	链接(更多的数据)
b5-b1	保留 (RFU)

表 23 — I 块的 PCB 编码

b8	1
b7	0
b6	0
b5	序列号
b4-b1	0=无错 1=EDC 或校验出错 2=其他错误 其他值保留为将来使用

表 24 — R 块的 PCB 编码

b8	1
b7	1

<sup>5</sup> ISO/IEC 7816 定义为 VPP 控制。0 值表示 VPP 必须维持在空闲状态。

b6	0=请求 1=应答
b5-b1	0=再同步请求 1=信息域大小请求 2=放弃请求 3=BWT 扩展请求 4=Vpp 错误 <sup>6</sup> 其他值保留为将来使用

表 25 — S 块的 PCB 编码

5.2.4.1.1.3 长度

LEN 指明块的 INF 部分的长度，根据块的类型，其取值范围从 0 到 254。

注：本规范不支持 LEN=0 的 I 块。

5.2.4.1.2 信息域

信息域 INF 是有条件的，当出现在 I 块中时，它传送的是应用数据，当出现在 S 块中时，它传送的是控制信息。R 块不包含 INF。

5.2.4.1.3 尾域

尾域包含所传送块的 EDC，奇偶校验出错和/或 EDC 出错时，块无效。本规范仅支持 LRC 作为 EDC。LRC 长度为一个字节，其值由以 NAD 开始到 INF(如果存在的话)的全部字节作异或运算得到。

注：TC<sub>i</sub>(i>2)指明要使用的错误检测代码类型，IC 卡在 ATR 中并不回送。因此 LCR 的正常缺省状态可用作 EDC。

5.2.4.1.4 块编号

I 块采用在某一位上模 2 数字编码的方式进行编码，IC 卡和终端作为发送方分别处理各自的编码系统。复位应答后，发送方发送的第一个 I 块的编号为零，其后每传送一个 I 块，编号值增加 1。当再同步后，发送方把编号值复位到零。

R 块采用在某一位上模 2 数字编码的方式进行编码，一个 R 块用来确认一个链接的 I 块或者请求一个无效的块重发。在这两种情况下，R 块中 PCB 字节中的 b5 位的值是下一个期望收到的 I 块的序列号。

S 块不携带编号。

<sup>6</sup> 符合本规范要求的 IC 卡和终端未使用。

#### 5.2.4.2 具体选项

本节定义了用于 T=1 传输协议的信息域的大小和时序。

##### 5.2.4.2.1 信息域大小

IFSC 是指 IC 卡能收到的信息域的最大长度，其定义是：在复位应答期间，IC 卡在 TA3 中回送的 IFSI 指明了 IC 卡能够容纳的 IFSC 的大小，IFSI 取值范围是‘10’到‘FE’，对应的 IFSC 大小是 16 到 254 字节。因此 IC 卡能收到的最大数据块长度是(IFSC+3+1)字节，其中包括头域和尾域。复位应答期间建立起来的这个值在整个卡片操作过程中使用，或持续到由于 IC 卡向终端发送 S 块(IFS 请求)而取得新的 IFSC 值为止。

终端信息域大小 IFSD 是指终端能够接收到的块的信息域最大长度。紧接在复位应答后的初始大小必须为 254 字节，此值必须在随后的整个卡片操作过程中使用。

##### 5.2.4.2.2 T=1 协议时序

终端发往 IC 卡的两个连续字符的起始位下降沿之间的最短时间间隔为 11 到 42 个 etu，由复位应答回送的 TC1 值决定(见 4.2 节和 4.3 节)。如果 TC1 返回的值是 N，IC 卡必须能够正确解释终端发送的起始位下降沿最小间隔为(11.8 + N)etu 的连续字符。

由 IC 卡发往终端的两个连续字符的起始位下降沿之间的最短时间间隔必须为 11 个 etu。终端必须能够正确解释 IC 卡发送的起始位下降沿最小间隔为 10.8 个 etu 的连续字符。

同一块中两个连续字符起始位下降沿之间的最大时间间隔(字符等待时间，CWT)不应超过  $(2^{CWI}+11)$  个 etu。其中 CWI 在 4.3.3.10 节中规定，取值为 0~5，所以 CWT 的取值范围是 12 到 43 个 etu。接收方必须能够正确解释起始位下降沿与上一字节起始位下降沿最大间隔为(CWT + 4) etu 的字符。

终端发送给 IC 卡的最后一个字符的起始位下降沿与由 IC 卡发出的第一个字符起始位下降沿之间的最大时间间隔(块等待时间，BWT)不应超过  $\{2^{BWI} \times 960\} + 11$  个 etu。在 4.3.3.10 节中所规定的 BWI 的取值范围是 0 到 4，所以 BWT 的取值范围是 971 到 15,371 个 etu。

终端必须能够正确解释 IC 卡在 BWT + (D x 960) 个 etu 内发送的块的第一个字节。

对终端或 IC 卡，最后一个接收到的字符的起始位下降沿和在相反方向发送的第一个字符起始位下降沿的最小时间间隔(块保护时间，BGT)必须为 22etu。IC 卡或终端必须能够正确解释和最后一个发送的字符的起始位下降沿间隔 21etu 以内接收到的字符。

注：通常，对于 FI 和 DI 不是 1 的情况，BWT 采用以下公式计算：

$$BWT = \{[2^{BWI} \times 960 \times 372D/F] + 11\} \text{ etu}$$

##### 5.2.4.3 无错操作

协议规则的无错操作如下：

1. 复位应答后，第一个数据块是由终端发往 IC 卡的，而且只能是一个 PCB=‘C1’，IFSD=254(单字节 INF 域中指定的值)的 S 块(IFS 请求)。卡片操作过程中，终端不能再发送 S 块(IFS 请求)。

2. IC 卡必须向终端返回 S 块(IFS 应答), 确认 IFSD 的改变。S 块(IFS 应答)的 PCB 值应为‘E1’, INF 域应该和请求块相同。
  3. 若 IC 卡希望改变在复位应答后指定的 IFSC 的大小, 则必须向终端发送一个 S 块(IFS 请求), S 块(IFS 请求)的 PCB 应具有值 C1 以表明是一个改变 IFSC 的请求, INF 域包含一个字节, 其值表示所要求的新 IFSC 的字节数, 该字节的取值范围从‘10’到‘FE’。终端必须向 IC 卡回送一个 S 块(IFS 响应), 确认卡片改变 IFSC 长度。其中 S 块(IFS 响应)的 PCB 值应是‘E1’, 且 INF 域与请求改变 S 块的 INF 域有相同的值。
  4. 在卡片操作过程中, 只有本节中定义的块才能改变。在半双工传输协议下, 终端和 IC 卡交替发送传输块。发送方完成块发送以后即转入接收状态。
  5. 当接收方所收到的字符数与 LEN 和 EDC 的值一致时, 接收方取得发送权。
  6. IC 卡需要确认由终端传来的 I 块。确认在 IC 卡回送给终端的 I 块序列号中指明。若使用链接, 则在 R 块的序列号中指明(链接的最后一个数据块除外)。
  7. 若响应中收到的 I 块序列号与前一个已收到的 I 块序列号不同, 则发送方可认为发送的非链接 I 块或链接 I 块的最后一块已被确认。若前面没有收到过 I 块, 响应中的 I 块序列号应该是 0。
  8. 接收到 R 块后, 必须验证 b5。接收方不必验证 PCB 的 b4-b1。对 b4-b1 的可选验证不能与本规范的规定冲突。
  9. 在链接的情况下, 如果在应答中发送的 R 块的序列号和响应的 I 块的序列号不同, 则链接的 I 块(链中的最后一个 I 块除外)可以视为已经确认。
  10. 若 IC 卡需要比 BWT 更长的时间来处理已收到的 I 块, 则必须发送一个等待时间扩展请求 S 块(WTX 请求), 其中的 INF 域包含有一个字节的二进制整数, 其值为所请求的 BWT 值的倍数。终端必须发送一个 INF 中具有相同值的等待时间扩展请求 S 块(WTX 响应), 以表示对延时请求的确认。取得的时间(就是在 S(WTX 请求)块中请求, 并且只在本次实例中替换 BWT)从 S 块(WTX 响应)的最后一个字符的起始位下降沿开始采用。在卡片响应结束后, ICC 卡仍然使用原来的 BWT 作为允许的时间来处理 I 块。
  11. S 块总是配对使用, 一个 S 请求块后总是跟随一个 S 响应块。
- 如果以上的同步过程失败, 则采用 5.2.5 节中描述的过程。

#### 5.2.4.4 链接

当发送方需要传送的数据长度超过 IFSC 或 IFSD 所定义的字节数时, 就要将其分成几个连续的 I 块。传送多个 I 块数据时, 使用以下规定的链接功能。

I 块的链接由 PCB 的 b6 控制。b6 的编码定义如下:

- b6=0, 链的最后一块;
- b6=1, 后面还有后续块。

根据 5.2.4.1 节中的规定, 包含 b6=1 的任何 I 块都必须由 R 块确认。

终端发送的链中的最后块如果正确接收, 则以 I 块确认; 如果未正确接收, 则以 R 块确认。IC 发送的链的最后块如果未正确接收, 则以 R 块确认; 如果正确接收且还要处理另一条命令, 则终端只能继续发送 I 块。

5.2.4.4.1 链接规则

- TTL 必须支持发送和接收块的链接。IC 卡是否支持发送到终端的链接块是可选的。链接在一个时刻只能在同一个方向进行。其规则如下：
- 当终端是接收方时，终端必须能够接收 IC 卡发送的每块长度≤IFSD 字节的链接 I 块。
  - 当 IC 卡是接收方时, IC 卡必须能够接收终端发送的除最后一块外每块长度 LEN=IFSC 的链接 I 块。最后一块的长度为 1 到 IFSC(包括)。
  - 当 IC 卡是接受方时，IC 卡必须用 R 块拒绝终端发送的长度>IFSC 的 I 块。
  - 如果 IC 卡作为发送方链接发送到终端的块，则必须使每个发送 I 块的长度≤IFSD。
  - 当终端是发送方时，终端必须能够发送除最后一块外每块长度 LEN=IFSC 的链接 I 块。最后一块的长度为 1 到 IFSC(包括)。

5.2.4.4.2 链接块的构造

C-APDU 包含在 I 块的 INF 域中，从 TTL 传送到 IC 卡(见 5.3.2 节)。如果一个 C-APDU 因太长而不能放在一个数据块中时，可通过如下的方法用几个链接块传送。

Block (1)					
CLA	INS	P1	P2	Lc	Data Data
Block (2)					
Data Data Data					
Block (n)					
Data Data				Le	

如果由 IC 卡回送的数据和状态码因太长而不能放在一个块中，可以按照下述方法通过几个 I 块来处理。

Block (1)					
Data Data Data					
Block (2)					
Data Data Data					
Block (n)					
Data Data				SW1	SW2

注：上面是针对命令情况 4 的举例，仅显示链接块的 INF 域。每个块还有一个头域和一个尾域。如果 IC 卡是发送方，全部链接块都应包含一个长度范围 1 到 IFSD 字节的 INF 域。如果终端是发送方，则包含一个长度范围 1 到 IFSC 字节的 INF 域。

5.2.5 T=1 协议的错误检测和纠正

- TTL 应能检测到以下错误：
- 传输错误(错误的奇偶校验和/或 EDC 错误)或 BWT 超时。
  - 实际块大小和 LEN 表明的大小不同，导致同步失调。
  - 协议错误(违背协议规则)；
  - 终止链接块请求。

如果检测到一个奇偶校验错误, T=1 协议下不能实现字符重发。

按照下述方法进行错误恢复:

TTL 以下列的次序按照下述技术方法纠错:

- 块重发;
- 释放 IC 卡触点。

IC 卡必须重发块, 以恢复错误。

如果重发块, 则重发的块必须和原发送块一致。

注: 某些终端上, 出错处理不完全由 TTL 承担。这种情况下, ‘TTL’表示终端中可用的所有相关功能。

以下类型的块视为非法:

- 包含传输错误的块, 例如校验/EDC 错误
- 包含格式错误的块, 例如发送方错误地组成了块(语法错误)
- 在交换过程中出现了违背协议规则的块。如在 I 块的应答中收到了 S(应答)块。

表明错误条件的 R 块不能视为非法块。

#### 5.2.5.1 错误处理的协议规则

下述规则用于错误处理和更正。在任意一种情况下, 当发送一个 R 块时, 错误码的 b4-b1 是否验证是可选的, 但不能引发和本规范定义的规则冲突的动作。

1. 当 IC 卡在复位应答后接收到的第一个块无效时, 就应回送一个 R 块给 TTL, 并置 b5=0 和 NAD=0。
2. 如果接收不到 TTL 发送给 IC 卡的块的应答, 终端必须:
  - a) 启动下电序列。
  - 或
  - b) 如果未应答的块为 I 块、R 块或 S(应答)块, 终端必须根据 5.2.4.1.4 节的规定传送一个带有序列号的 R 块。
  - 或
  - c) 如果未应答的块为 S(请求)块, 终端必须重新传送 S(请求)块。以上动作必须在未收到应答的块的最后一个字节的起始位下降沿开始的  $\{BWT + (D \times 960)\}$  个 etu 到  $\{BWT + (D \times 4800)\}$  个 etu 之间完成。如果使用了等待时间扩展, 则必须在  $\{BWT + (n \times D \times 960)\}$  个 etu 到  $\{BWT + (n \times D \times 4800)\}$  个 etu 内完成。
3. 如果终端在接收块的过程中没有收到期望的字符, 终端必须:
  - a) 启动下电时序
  - 或
  - b) 如果未应答的块为 I 块、R 块或 S(应答)块, 终端必须根据 5.2.4.1.4 节的规定传送一个带有序列号的 R 块。
  - 或
  - c) 如果未应答的块为 S(请求)块, 终端必须重新传送 S(请求)块。以上动作必须在最后一个接收到的字符的起始位下降沿开始的  $(CWT + 4)$  个 etu 到  $(CWT + 4,800)$  个 etu 之内完成。
4. 如果在 I 块的应答中收到了非法块, 发送方必须按 5.2.4.1.4 节的规定传送带有序列号

的 R 块。

5. 如果在 R 块的应答中收到了非法块，发送方必须重发 R 块。
6. 如果响应 S 块(...请求)的 S(...响应)块没有收到，发送方必须重发一个 S(...请求)块。
7. 如果响应 S(...响应)块的应答中收到无效块，发送方必须按 5.2.4.1.4 节的规定传送带有序列号的 R 块。
8. 如果 TTL 连续发送三个任何块，而没有得到有效的响应，则 TTL 必须在请求重发的块的最后一个字节的起始位下降沿开始的 $\{BWT + (D \times 14,400)\}$ 个 etu 内启动下电序列。

注：本规范中不要求再同步。如果终端需要支持再同步，它可以通过发送一个 S(再同步)块，相关操作在 ISO7816-3 中定义。

如果 IC 卡最多连续发送两次而没有收到有效应答，则它必须保持在接收状态。

9. TTL 不能发送 S(放弃请求)块。如果 TTL 从 IC 卡收到一个 S(放弃请求)块，TTL 必须在 S(放弃请求)块的最后一个字节的起始位下降沿开始的 $(D \times 9,600)$ 个 etu 内启动下电时序。

注：本规范不要求交易终止。如果因特殊原因要求 IC 卡或终端支持交易终止功能，它可以发出一个 S(放弃请求)块。但要注意，如接收方不支持终止功能时，它只会收到一个无效的响应，卡片将按照上述规则结束卡片操作过程。如果终端收到来自 IC 卡的 S(放弃请求)块，且支持终止功能，则它可以回送一个 S(放弃响应)块，而不是主动结束卡片操作过程。

### 5.3 终端传输层(TTL)

本节描述了在终端和 IC 卡之间传输命令和响应 APDU 的机制。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 5.4 节中定义的命令的四种格式。C-APDU 和 R-APDU 的组成将在 5.4.1 节和 5.4.2 节中描述。

TAL 向 TTL 传送 C-APDU。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)和状态码回送给 TTL。

#### 5.3.1 T=0 协议下 APDU 的传送

本节描述了 C-APDU 和 R-APDU 的映射方式，TTL 和 IC 卡之间的数据交换机制以及在命令情况 2 或 4 中如何使用取应答命令取回 IC 卡的数据。

##### 5.3.1.1 C-APDU 和 R-APDU 的映射方式和数据交换

C-APDU 到 T=0 命令头的映射取决于命令情况。将 IC 卡回送的数据(如果存在)和状态码映射到 R-APDU 的形式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。

注：因为某些特殊原因，TTL 可能接收除'61'和'6C'以外的来自 IC 卡的其它过程字节。这些功能不在本规范定义的范围之内。

如果 IC 卡回送给 TTL 的状态码是 SW1 SW2='9000'，则表示正常完成了命令的处理。TTL

在接收到任何其它的状态(不包括过程字节‘61xx’和‘6Cxx’)时,都必须中断命令的处理(例如向 TAL 传送 R-APDU,等待来自 TAL 的 C-APDU)。(当是第四种形式的命令时,在向 IC 卡成功传输命令数据以后,如果收到警告字节(‘62xx’或‘63xx’)或应用相关的状态字节(‘9xxx’除‘9000’外),则 TTL 必须继续处理命令。)

以下描述的是将 IC 卡回送的数据和状态字节映射到 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。

IC 卡返回的状态字和最后一条收到的命令相关;当在情况 2 或情况 4 时,一个 GET RESPONSE 命令用来完成一条命令的处理,ICC 卡在接收到 GETRESPONSE 命令后返回的任何状态字和 GET RESPONSE 命令相关,而与它要完成的情况 2 或情况 4 的命令无关。

#### 5.3.1.1.1 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:

1. TTL 发送 T=0 的命令头到 IC 卡;
2. IC 卡收到命令头后,无论正常或非正常处理,IC 卡都必须向 TTL 回送状态码。  
(IC 卡必须分析 T=0 命令头,判断是在处理情况 1 命令还是在处理请求最大长度数据的情况 2 命令。)
3. 收到来自 IC 卡的状态字节以后,TTL 必须中止该命令的处理。

TTL 和 IC 卡交换的具体细节参见附录 A 的 A1 节。

命令处理结束后从 IC 卡返回到 TTL 的状态必须原封不动地映射到 R-APDU 的结尾。

#### 5.3.1.1.2 情况 2

C-APDU 头映射到 T=0 命令头的前四个字节,长度字节‘Le’从 C-APDU 的条件体映射到 T=0 命令头的 P3。在应用选择中发出的读记录(READ RECORDED)命令和按本规范第三册发出的所有情况 2 的命令的 Le 都必须为‘00’。

交换流程如下:

1. TTL 发送 T=0 的命令头到 IC 卡。
2. IC 卡收到命令头以后:
  - a) 正常处理以后必须向 TTL 返回数据和状态。IC 卡必须用状态字节‘6Cxx’(如果需要,亦可用‘61xx’)控制返回的数据。
  - 或
  - b) 在非正常处理后仅向 TTL 返回状态。
3. 接收到来自 IC 卡的数据(如果存在)和状态之后,TTL 必须中止该命令的处理。

TTL 和 IC 卡的交换细节,包括过程字节‘61xx’和‘6Cxx’的使用,请参考附录 A 的 A2 节。

命令处理完成后从 IC 卡返回 TTL 的数据(如果存在)和状态或 IC 卡返回的导致 TTL 终止命令处理的状态按以下规则与 R-APDU 映射:

返回的数据(如果存在)映射到 R-APDU 的条件体。如果没有数据返回,则 R-APDU 的条件体留空。

返回的状态原封不动地映射到 R-APDU 的结尾。

#### 5.3.1.1.3 情况 3

C-APDU 头映射到 T=0 命令头的前四个字节,C-APDU 条件体的长度字节'Lc'映射到 T=0 命令头的 P3。

交换流程如下:

1. TTL 发送 T=0 的命令头到 IC 卡。
2. 收到命令头后,如果 IC 卡:
  - a) 回送一个过程字节,则 TTL 必须在此过程字节的控制下向 IC 卡发送 C-APDU 条件体的部分数据。
  - 或
  - b) 如果 IC 卡回送状态码,TTL 必须中止命令处理过程。
3. 如果处理过程没有在步骤 2(b)中断,则 IC 卡必须在接收到 C-APDU 的条件体之后返回命令处理结束后的状态。
4. 收到来自 IC 卡的状态码之后,TTL 必须中止该命令的执行。

TTL 和 IC 卡之间的交换细节,请参见附录 A 的 A3 节。

IC 卡处理命令结束后返回到 TTL 的状态或导致 TTL 终止命令执行的状态原封不动地映射到 R-APDU。

#### 5.3.1.1.4 情况 4

C-APDU 头映射到 T=0 命令头的前四个字节,C-APDU 条件体的长度字节'Lc'映射到 T=0 命令头的 P3。应用选择中发出的选择(SELECT)命令和本规范第三册规定的所有情况 4 命令的 Le 都必须为'00'。

交换流程如下:

1. TTL 发送 T=0 命令头到 IC 卡。
2. 接收到命令头以后,IC 卡必须:
  - a) 返回一个状态字节,TTL 必须在此状态字节的控制下向 IC 卡发送 C-APDU 条件体的数据部分。
  - 或
  - b) 如果 IC 卡回送状态码,TTL 将中止命令处理过程。
3. 如果处理过程在步骤 2 中没有中止,IC 卡在接收到 C-APDU 的条件体之后必须: a) 在正常处理下,回送过程字节'61xx'给 TTL,请求 TTL 发出取应答(GET RESPONSE)命令从 IC 卡取回数据。- 或
- b)在非正常处理下,只向 TTL 返回状态。
4. 收到第 3 步返回的过程字节或状态后,如果 IC 卡:
  - a) 返回 3(a)中的'61xx'过程字节,TTL 必须向 IC 卡发送 P3 小于或等于过程字节

‘61xx’中的‘xx’的取应答(GET RESPONSE)命令头

或

b) 返回 3(b)中的警告状态(‘62xx’或‘63xx’)或应用相关的警告状态(‘9xxx’但不包括‘9000’), TTL 必须发送 Le=‘00’的取应答(GET RESPONSE)命令。

或

c) 返回 3(b)中出现的但未在 4(b)中描述的状态, TTL 必须中止命令的处理。

5. 如果 4(c)中没有中止处理, 则必须按照 5.3.1.1.2 节情况 2 的描述处理取应答命令。  
TTL 和 IC 卡的交换细节包括过程字节‘61xx’和‘6Cxx’的使用, 请参考附录 A 的 A4。  
IC 卡完成命令处理之后返回 TTL 的数据(如果存在)和状态或 IC 卡返回的导致 TTL 中止命令执行的状态, 按以下规则与 R-APDU 映射:  
返回的数据(如果存在)映射到 R-APDU 的条件体。如果无返回数据, 则 R-APDU 的条件体留空。  
整个情况 4 的命令处理过程中返回的第一个状态, 包括可能使用到的取应答命令, 原封不动地映射到 R-APDU 的结尾。

#### 5.3.1.2 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 发出取应答(GET RESPONSE)命令到 IC 卡。取应答命令头的 P3 置为≤‘xx’。

过程字节‘6Cxx’通知 TTL 立即重发上一条命令, 同时命令头置为 P3=‘xx’。

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

##### 5.3.1.2.1 情况 2 命令

1. 如果 IC 卡收到一个情况 2 的命令头并且 Le=‘00’或 Le>Licc, 则它必须返回
  - a) 过程字节‘6C Licc’, 要求 TTL 以 P3=Licc 立即重发命令头
  - 或
  - b) 表明警告或错误条件(除 SW1 SW2 = ‘9000’)的状态。  
注: 如果 Le=‘00’且 IC 卡需要返回 256 个字节, 则它必须按以下 Le=Licc 的规则处理。
2. 如果 IC 卡收到情况 2 的命令头并且 Le=Licc, 它必须
  - a) 在 INS、 $\overline{INS}$  或‘60’及相关过程字节的控制下返回长度为 Le(=Licc)的数据
  - 或
  - b) 返回状态字节‘61xx’, 要求 TTL 发出最大长度为‘xx’的取应答命令。
  - 或
  - c) 返回表明警告或错误条件的状态(SW1 SW2 = ‘9000’除外)。
3. 如果 IC 卡收到情况 2 的命令头并且 Le < Licc, 它必须
  - a) 返回过程字节‘61xx’, 要求 TTL 发送最大长度为‘xx’的取应答命令, 然后在 INS、 $\overline{INS}$  或‘60’的控制下返回长度为 Le(=Licc)的数据,

- 或
- b) 返回过程字节‘6C Licc’要求 TTL 以 P3=Licc 立即重发命令头
- 或
- c) 返回表明警告或错误条件的状态(SW1 SW2 = ‘9000’除外)
- 3(b)不是 IC 卡对取应答命令的合法应答。

5.3.1.2.2 情况 4 命令

如果 IC 卡收到一个情况 4 的命令，处理完随 C-APDU 一同发送来的数据之后，它必须

- a) 返回过程字节‘61xx’，通知 TTL 按最大长度‘xx’发出取应答命令。
- 或
- b) 返回表明警告或错误情况的状态码(SW1 SW2=‘9000’除外)。

此时发出的取应答命令的处理方法参见 5.3.1.2.1 节对情况 2 命令中的描述。

5.3.1.3 取应答(GET RESPONSE)命令

TTL 发出取应答命令,是为了从 IC 卡取得对应于情况 2 和 4 的命令的数据。取应答仅适用于 T=0 协议类型。

命令报文的结构如表 26:

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

表 26 — 命令报文结构

正常处理结束后，IC 卡回送状态码 SW1 SW2=‘9000’和 Licc 字节的数据。  
在错误情况发生时，错误状态码(SW1 SW2)的编码见表 27:

SW1	SW2	含义
‘62’	‘81’	返回的部分数据可能已破坏
‘67’	‘00’	长度域错误
‘6A’	‘86’	P1 P2≠‘00’
‘6F’	‘00’	无准确诊断

表 27 — 取应答错误响应

5.3.2 T=1 协议下 APDU 的传送

C-APDU 从 TAL 传送到 TTL，TTL 将其不加变化地映射到 C-APDU 的一个 I 块的 INF 域中，然后把这个 I 块发送到 IC 卡。

IC 卡在 I 块的 INF 域中向 TTL 回送响应数据(如果存在)和状态码。如果 IC 卡返回表明正常处理(‘61xx’)、一个警告(‘62xx’或‘63xx’)，与应用相关(‘9xxx’)或‘9000’状态码，则它必须同时返回与命令处理相关的数据(如果有)。其它状态下不能返回数据。块的 INF 域的内容原封不动地映射到 R-APDU，然后返回给 TAL。

注：如果有必要，C-APDU 和响应数据/状态码可以分成多个数据块的 INF 域的链接。

5.4 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的情况，见表 28 所示：

情况	命令数据	响应数据
1	无	无
2	无	有
3	有	无
4	有	有

表 28 — APDU 中数据存在的情况

注：由于安全报文传送总有数据(至少是 MAC)要送往 IC 卡，因此仅适用于命令情况 3 和 4 的情况。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。

5.4.1 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：指令类型的指令码。只有在低半字节为 0，且高半字节既不是‘6’也不是‘9’时，INS 才有效。
- P1 P2：完成 INS 的参数字节。

注：每一个命令头的完整定义将在本规范第 7 章中描述。

条件体包括如下定义的字节串：

- 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 R-APDU 中期望返回的最大字节数。Le 的取值范围从 0 到 255；如果 Le=0，则期望返回数据的字节数的最大长度是 256。

注：每个命令的条件体数据域的完整定义将在本规范的第 7 章中描述。

可能的 C-APDU 结构的四种情况见表 29：

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

表 29 — C-APDU 的情况

5.4.2 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。  
必备的状态码表明 IC 卡在处理完命令后的状态。  
SW1 SW2 的编码在本规范第 7 章规定。

## 第 II 部分

### 文件、命令和应用选择

## 6. 文件

IC卡中的每个应用都包括一系列信息项(通常以文件形式存在)，终端成功地完成应用选择后就可以访问这些信息。

一个信息项称为一个数据元，数据元是信息的最小单位，它是可以用名称、逻辑内容描述、格式及代码来标识的最小信息单元。

由发卡行保证数据项在卡片中存储格式的正确性。但是，如果终端在常规处理的过程中发现数据格式不正确(例如，结构数据对象的解析有误)，则必须终止卡片操作过程。

附录B中表B-1定义了可能在应用选择中使用到的数据元。未在附录B表B-1中定义的用于应用选择的数据元不在本规范的范围之内。

### 6.1 文件结构

本规范中的文件组织结构来自且符合ISO/IEC 7816-4的基本组织结构。

本部分描述了符合本规范的应用文件结构。

从终端的角度来看，IC卡上的文件是一种树形结构。树的每一个分支是一个应用数据文件(ADF)或一个目录定义文件(DDF)。一个ADF是一个或者多个应用基本文件(AEF)的入口点。一个ADF及其相关的数据文件处于树的同一分支上。一个DDF是其他ADF或者DDF的入口点。

#### 6.1.1 应用数据文件(ADF)

ADF的树形结构：

- 能够将数据文件与应用联系起来；
- 确保应用之间的独立性；
- 可以通过应用选择实现对其逻辑结构的访问。

从终端的角度看，ADF是一个只包含封装在其文件控制信息(FCI)中的数据对象的文件，参见表40。

#### 6.1.2 应用基本文件(AEF)

AEF所使用的结构是应用相关的。本规范第三册中描述了针对EMV借记/贷记应用的文件结构。

#### 6.1.3 文件到 ISO/IEC 7816-4 的文件结构的映射

使用下列到ISO/IEC 7816-4的映射：

- 一个ISO/IEC 7816-4定义的专用文件(DF)映射为一个ADF或一个DDF。可以通过它来访问基本文件和DF。在卡片中处于最高层的DF称为主文件(MF)。
- ISO/IEC 7816-4定义的一个基本文件(EF) 对应一个AEF。EF永远不会成为另一个

文件的入口点。

在本规范中，如果嵌入了DF，对与之相连的EF的访问是透明的。

#### 6.1.4 目录结构

当存在8.2.2节中描述的支付系统环境(PSE)时，IC卡必须为PSE中发卡行希望通过目录选择的应用列表提供一个目录结构。在这种情况下，目录结构由一个支付系统目录文件(DIR文件)和符合本章中描述的目录定义文件(DDF)结构的可选附加目录组成。

目录结构允许以应用标识符(AID)检索一个应用，或以AID的前n个字节作为DDF名检索一组应用。

在选择PSE的响应报文中必须有DIR文件存在的编码(参见选择(SELECT)命令)。

根据ISO/IEC7816-5的定义，DIR文件是一个AEF(亦即EF)和含下列数据对象的记录结构：

- 本规范第8章描述的一个或多个应用模板(标签为‘61’)。
- 可能在目录自定义模板(标签为‘73’)中出现的其他数据对象，此模板中包含的数据对象不在本规范的范围内容义。

IC卡中的目录是可选的，但对可能存在的目录数目没有限制。其中每个目录的位置由每个DDF中的FCI的目录SFI数据对象指定。

#### 6.2 文件引用

根据其类型，文件可以通过文件名或SFI引用。

##### 6.2.1 通过文件名引用

卡片中的任何ADF或DDF都可以通过其DF名引用。ADF的DF名与其AID对应或包含AID作为DF的开始字符。在一张给定的卡片内，每个DF名必须唯一。

##### 6.2.2 通过短文件标识符(SFI)引用

SFI用于选择AEF。在给定应用中的任何AEF都可以通过SFI(5位编码，取值范围从1到30)引用。SFI的编码在每一个用到它的命令中进行描述。在一个应用中SFI必须是唯一的。

## 7. 命令

### 7.1 报文结构

报文根据ATR所选择的传输协议(参见本规范第一部分)在终端和卡片之间传输。终端和卡片必须按第I部分的定义实现物理层、数据链路层和传输层。

为了运行一个应用，在终端上还要实现一个附加的应用协议层。它包括向卡片发送命令、卡片内处理命令和返回IC卡处理应答等步骤。本部分和本规范后续部分定义的所有命令和应答都定义在应用层。

应用层发出的命令报文和卡片回送到应用层的应答报文统称为应用协议数据单元(APDU)。应答是和命令相对应的，通常被称为APDU命令-应答对。在一个APDU命令-应答对中，命令报文或应答报文都可能包含数据。

本章描述了在应用选择功能中所必需的APDU命令-应答对的结构，这些结构是本规范第一卷所定义的应用层所必需的。其它所有的命令由特定的应用来实现，但是也应该遵循此处定义的APDU结构(格式)。

#### 7.1.1 命令 APDU 格式

命令APDU由一个4字节长的必备头后跟一个变长的条件体组成，见图12：

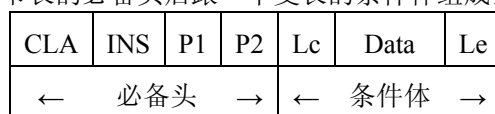


图 12 - 命令 APDU 结构

命令APDU中发送的数据长度用Lc(命令数据域的长度)表示。

应答APDU中期望返回的数据字节数用Le(期望数据长度)表示。当Le存在且值为0时，表示要求可能的最大字节数(≤256)。在应用选择中所给出的读记录(READ RECORD)命令、选择(SELECT)命令以及本规范第三册中所给出的所有情况2和第情况4命令中，Le应该等于‘00’。

命令APDU报文的内容见表30：

代码	描述	长度
CLA	命令类别	1
INS	指令代码	1
P1	指令参数1	1
P2	指令参数2	1
Lc	命令数据域中存在的字节数	0或1
Data	命令发送的数据位串(=Lc)	变长
Le	应答数据域中期望的最大数据字节数	0或1

表 30 – 命令 APDU 内容

命令APDU结构的不同类别在本规范第I部分中描述。

7.1.2 应答 APDU 格式

应答APDU格式由一个变长的条件体和后随两字节长的必备尾组成，见图13：

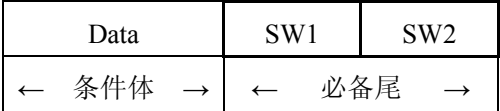


图 13 – 应答 APDU 结构

应答APDU中接收到的数据字节数用Lr(应答数据域长度)表示。Lr不通过传输层返回，应用层在需要时可以依靠应答报文数据域对象结构计算出Lr。

应答结尾的2个字节代码是命令的处理状态，它们通过传输层回送。

应答APDU的内容见表31：

代码	描述	长度
Data	应答中接收的数据位串	变长(=Lr)
SW1	命令处理状态	1
SW2	命令处理限定	1

表 31 – 应答 APDU 内容

7.1.3 命令-应答 APDU 约定

在一个APDU命令-应答对中，命令报文和应答报文都可能包含数据，4类命令的数据包含情况见表32：

类别	命令数据	应答数据
1	不存在	不存在
2	不存在	存在
3	存在	不存在
4	存在	存在

表 32 — 命令-应答对APDU 的数据

这4类命令使用本规范第I部分所描述的传输协议进行处理。

7.2 读记录(READ RECORD)命令-响应 APDU

7.2.1 定义和范围

读记录命令用于读取线性文件中的记录。  
IC卡的应答由回送记录组成。

7.2.2 命令报文

读记录命令报文编码见表33：

代码	值
----	---

CLA	‘00’
INS	‘B2’
P1	记录号
P2	引用控制参数(见表34)
Lc	不存在
Data	不存在
Le	‘00’

表33 – 读记录命令报文

表34定义了命令报文的引用控制参数。

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X				SF1
					1	0	0	P1为记录号

表34 – 读记录命令引用控制参数

7.2.3 命令报文数据域

命令报文数据域不存在。

7.2.4 应答报文数据域

执行成功的读记录命令的应答报文数据域由读取的记录组成。在应用选择过程中读取的记录是目录记录(格式由8.2.3节定义)。应用处理中读取的记录格式与应用有关。

7.2.5 应答报文状态码

此命令执行成功的状态码是‘9000’。

7.3 选择(SELECT)命令-响应 APDU

7.3.1 定义和范围

选择命令通过文件名或AID来选择IC卡中的PSE、DDF或ADF。应用选择在本规范的第8章中描述。

成功执行该命令设定PSE、DDF或ADF的路径。后续命令作用于与用SFI选定的PSE、DDF或ADF相联系的AEF。

从IC卡返回的应答报文包含回送FCI。

7.3.2 命令报文

选择命令报文编码见表35：

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数(见表36)
P2	选择选项(见表37)
Lc	‘05’ - ‘10’
Data	文件名
Le	‘00’

表 35 - SELECT 命令报文

表36定义了选择(SELECT)命令报文的引用控制参数：

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0				
					1			通过名称选择
						0	0	

表 36 — SELECT命令引用控制参数

表37定义了选择(SELECT)命令报文的选择选项P2：

b8	b7	b6	b5	b4	b3	b2	b1	含义
						0	0	第一个有或仅有一个
						1	0	下一个

表 37 — 选择(SELECT)命令的可选参数

7.3.3 命令报文数据域

命令报文数据域应包括所选择的PSE名、DF名或AID。

7.3.4 应答报文数据域

应答报文中数据域应包括所选择的PSE、DDF或ADF的FCI。表38、表39和表40定义了本规范所应用的标识。对于本规范所不规定的FCI中回送的附加标签应该被忽略。

表38定义了成功选择PSE后回送的FCI：

标识	值	存在性
‘6F’	FCI 模板	M
	‘84’ DF 名	M
	‘A5’ FCI 数据专用模板	M
	‘88’ 目录基本文件的 SFI	M
	‘5F2D’ 语言选择	O
	‘9F11’ 发卡行代码表索引	O
	‘BF0C’ 发卡行自定义数据(FCI)	O

	‘XXXX’ (第 3 册规定的 的标签)	来自从应用提供商、发卡行或 IC 卡供应商的 1 个或多个附加(专 用)数据元。	O
--	-----------------------------	--	---

表 38 — 选择PSE的应答报文 (FCI)

表39定义了成功选择DDF后回送的FCI:

标签	值		存在性
‘6F’	FCI 模板		M
	‘84’	DF 名	M
	‘A5’	FCI 数据专用模板	M
	‘88’	目录基本文件的 SFI	M
	‘BF0C’	发卡行自定义数据(FCI)	O
	‘XXXX’ (第 3 册规定的 标识符)	来自从应用提供商、发卡行或 IC 卡供 应商的 1 个或多个附加(专用)数据元。	O

表 39 – 选择DDF的应答报文 (FCI)

表40定义了成功选择ADF后回送的FCI:

标签	值		存在性
‘6F’	FCI 模板		M
	‘84’	DF 名	M
	‘A5’	FCI 数据专用模板	M
	‘50’	应用标签	O
	‘87’	应用优先指示符	O
	‘9F38’	PDOL	O
	‘5F2D’	首选语言	O
	‘9F11’	发卡行代码表索引	O
	‘9F12’	应用优先名称	O
	‘BF0C’	发卡行自定义数据(FCI)	O
	‘XXXX’ (第 3 册规定的 标识符)	来自从应用提供商、发卡行 或 IC 卡供应商的 1 个或多 个附加(专用)数据元。	O

表 40 – 选择ADF的应答报文 (FCI)

注意：对于多应用卡片，强烈建议在响应报文中包含“应用标签”数据元，使得在终端用“AID列表”方法进行应用选择时，能方便持卡人选择/确认应用。

7.3.5 应答报文状态码

此命令执行成功的状态码是‘9000’。

IC卡是否支持使用部分DF名进行DF文件选择不作强制规定。但是，如果IC卡支持部分名称选择，那么它应该遵守下列规则：

当一个DF成功选中后，终端重复发出选择(SELECT)命令，且P2设置为选择下一个文件的选项(参见表37)及使用相同的部分DF名时，卡片应该选中与部分DF名称匹配的不同的DF文件(如果这样的DF存在)。在没有应用层命令干扰的情况下重复发出相同的选择(SELECT)命令，卡片应该可以找到所有满足条件的DF文件，且每个文件不会被找到两次。当所有满足条件的DF都被选择后，再发出同样的选择(SELECT)命令，应该得到没有文件被选择的结果，卡片应该响应SW1SW2='6A82'(文件未找到)。

## 8. 应用选择

### 8.1 应用选择概述

应用选择是卡片复位之后、在第一个应用功能之前执行的处理过程。

本章从卡片和终端两个角度描述了应用选择的过程。首先描述了该过程所需要的卡片上的数据和文件的逻辑结构，之后描述了处理这种卡片结构的终端逻辑。

IC卡和终端可以支持应用隐含选择，但由于在交互环境中并不有用，这里就不描述了。

终端按本章所描述的应用选择过程，根据这里所定义的协议使用IC卡上的数据来决定选择哪个终端程序和IC卡应用进行交易，其过程分为两个步骤：

1. 建立终端支持的IC卡应用列表(这个列表在下面使用名称“候选列表”指代)。这个过程在8.3节中描述。
2. 在步骤1生成的候选列表选择一个将要运行的应用。这个过程在8.3.4节中描述。

本章描述了为完成正确的应用选择所需的卡上的信息以及两个终端选择算法。其它能够实现同样结果的终端选择算法也可用来代替本章描述的算法。

一个支付系统应用应该包括以下内容：

- IC卡上一组已由发卡行定制的数据文件。
- 终端上由收单行或商户提供的的数据。
- 一套卡片和终端共同遵守的应用协议。

所有应用都唯一地由一个应用标识符(AID)标识。应用标识符格式符合ISO/IEC 7816-5(参见8.2.1节)的有关规定。

这里描述的支付系统所采用的技术在设计上应能满足下列主要目标：

- 在很大范围上能支持具有各种不同功能的IC卡。
- 在很大范围上具有各种不同功能的终端，能根据本规范支持所有包含支付系统应用的IC卡。
- 符合ISO标准。
- IC卡支持多个应用，但不要求所有的应用都是支付系统应用。
- IC卡能够提供被单个终端程序支持的多组应用(例如：一张卡可以包含多个借记/贷记应用，每个应用代表了不同的服务类型、服务级别或不同帐户)。
- 尽可能使符合本规范的应用能够与卡上现有应用共存。
- 最小的存储和处理开销。
- 具有允许发卡行优化选择过程的能力。

IC卡上包含的支持给定应用的数据，由终端使用选择(SELECT)命令选择出的ADF和IC卡响应处理选项命令(GET PROCESSING OPTIONS)而返回的AFL所定义。

## 8.2 用于应用选择的 IC 卡数据

### 8.2.1 支付系统应用标识符编码

应用标识符(AID)的结构符合ISO/IEC 7816-5, 包括两个部分:

1. 注册应用提供商标识符(RID)(长度为5字节), 唯一地标识应用提供商, 并根据ISO/IEC 7816-5分配。
2. 最长为11字节的可选域, 由应用提供商定义。这个域被称为“专有应用标识符扩展码 (PIX)”, 可包含应用提供商定义的长度为0到11字节的值。该域的含义只对应于特定的RID, 不同RID下的PIX不需要唯一。

IC卡上允许存在其它应用提供商的应用数据文件(ADF), 但是其RID的定义应该避免与分配给支付系统的RID的范围发生重复。可遵照ISO/IEC 7816-5的规定定义RID, 以确保其编码不发生冲突。

### 8.2.2 支付系统环境结构

在IC卡上, 支付系统环境起始于一个名为“1PAY.SYS.DDF01”的目录定义文件(DDF)。该DDF在IC卡上是否存在是可选的, 但如果存在, 则应遵守本规范的相关规定。如果这个DDF存在, 那么这个DDF被映射到卡中的某个DF, 这个DF可以是MF, 也可以不是。和所有的DDF一样, 该DDF也应该包含一个支付系统目录。该DDF的文件控制信息(FCI)中至少要包含第7章中对所有DDF定义的信息, 另外, 还可以包括语言选择(标识‘5F2D’)和发卡行代码表索引(标识‘9F11’)。

首选语言和发卡行代码表索引是可选的数据项, 可以在两个位置出现: PSE的FCI中和ADF文件的FCI中。如果这些数据项存在, 那么它们将在两个位置都出现, 而且出现的值相同。终端可以使用两个位置中任何一处的值。<sup>9</sup>

初始DDF所附带的目录包含了ADF的入口地址。尽管这些ADF定义的应用既可以符合也可以不符合本规范, 但其入口地址格式是符合本规范定义的。该目录也可以包含其它支付系统DDF的入口地址。同样, 这些入口地址也必须符合本规范。

不要求该目录包含卡上所有的DDF和ADF的入口地址, 也不要求沿着DDF的链接一定能够找到卡片支持的全部应用。当然, 如果PSE存在, 只有从初始目录开始, 沿着DDF的链接能够找到的应用, 才具备国际互通性。

包含PSE的IC卡的内部逻辑结构的举例, 参考附录C。

---

<sup>9</sup> 当终端使用 8.3.2 节中所描述的过程建立候选列表时, 在所要运行的应用被选中之前, 终端只看到 PSE 的 FCI 指明的值, 而看不到 ADF 的 FCI 指出的值; 当终端使用 8.3.3 节中所描述的过程建立候选列表时, 能够看到 ADF 的 FCI 指明的值。为了确保在对持卡人的界面中保持一致, 这些值必须相同。

8.2.3 支付系统目录编码

支付系统目录(以下简称目录)是一个线性EF文件，用1到10的短文件标识符(SFI)标识。该目录附属于DDF，目录的SFI包含在DDF的文件控制信息中。目录可以使用本规范第7章中所定义的读记录(READ RECORD)命令进行读取。一个记录可以包含几个入口地址，但一个入口地址只能封装在一个记录中。

支付系统目录中的每一个记录都是一个结构数据对象，其值由如下所示的一个或多个目录的入口组成。

每个记录的格式参见表41：

标签 '70'	数据域 长度 (L)	标识符 '61'	目录入口1长度	目录入口1 (ADF 或 DDF)	...	标识符 '61'	目录入口 n 长度	目录入口 n (ADF 或 DDF)
------------	------------------	-------------	---------	-------------------------	-----	-------------	-----------------	-----------------------------

表 41 — PSE 目录记录格式

支付系统目录中的每一个入口都是一个应用模板(标签‘61’)，它包含表42或表43所示的信息。

任何没有封装在目录记录的应用模板(标签‘61’)当中的数据对象或其它在目录入口中出现但是没有在表42或表43中列出的数据对象都应该被忽略。

标签	长度	值		存在方式
'9D'	5-16	DDF 名称		M
'73'	变长	目录自定义模板		O <sup>10</sup>
	'XXXX' (第3册规定的标识符)	变长	应用提供商、发卡行或 IC 卡供应商增加的 1 个或多个附加(专用)数据元。	O

表 42 — DDF目录入口格式

标签	长度	值	存在方式
'4F'	5-16	ADF 名称(AID)	M
'50'	1-16	应用标签	M
'9F12'	1-16	应用优先名称	O
'87'	1	应用优先权标识符	O
'73'	变长	目录自定义模板	O <sup>10</sup>

<sup>10</sup> 其它与本规范无关的数据对象也可以用来构造此数据对象。

	‘XXXX’ (第 3 卷规定的标识符)	变长	应用提供商、发行商或 IC 卡供应商增加的 1 个或多个附加(专用)数据元。	O
--	-------------------------	----	--	---

表 43 — ADF目录入口格式

B8	b7-b5	b4-b1	定义
1			需要持卡人确认方可选择应用
0			不需持卡人确认即可选择应用
	x x x		保留
		0 0 0 0	未指定优先权
		x x x x (0 0 0 0 除外)	应用的排列或选择顺序，从 1-15，其中最高优先权为 1

表 44 — 应用优先权标识符格式

8.2.4 其它目录的编码

IC卡上的每个目录都由一个单独的DDF所包含。卡上的DDF和目录是可选的，而且对它们的存在数目没有明确限制。每个目录都由一个目录SFI数据对象来定位，这个SFI必须包含在DDF的FCI中(参见7.3节关于选择(SELECT)命令的描述)。目录SFI的低5位包含了读记录(READ RECORD)命令读取目录所需的SFI。当包含该目录的DDF为当前选定的文件时，SFI可用来读取这个目录。

如8.2.3节所示，包括初始目录在内的所有目录都使用相同的格式。

8.3 建立候选列表

终端应该维护一个终端所支持的应用及其所对应的应用标识符(AID)列表。本节描述了两种应用选择过程。如果卡内不存在PSE，则应遵循8.3.3节所描述的过程。

需要注意的是终端可以通过本节没有描述的其它方式来确定或者排除IC卡上的专有应用。当然这些方式的前提是IC卡上所有的通用应用都可以使用这里所描述的技术来确定其位置。

8.3.1 终端应用与 IC 卡应用的匹配

终端是通过比较IC卡和其本身的应用AID来确定IC卡上的哪些应用是可用的。

在某些情况下，终端只有在IC卡上的AID和其本身的AID的长度和值都相同的时才支持此IC卡应用。这种情况限制了IC卡上至多只有一个匹配的ADF。

在另一些情况下，终端支持IC卡上AID的开始部分与完整的终端AID相同的应用。这允许IC卡可以通过给对应的AID增加唯一的信息而使多个ADF与终端应用匹配。如果卡上只有一个

ADF与终端AID匹配, 那么就用这个为终端所知的AID来标识此ADF。如果IC卡有多个被终端AID所支持的ADF, 那么IC卡必须满足以下要求:

- IC卡必须支持本规范第7章所描述的部分名称选择(参见选择(SELECT)命令)。
- IC卡上所有匹配的AID必须在专有应用标识符扩展码(PIX)中加入唯一的数据标识来区别。IC卡AID中应该没有一个和终端的AID的长度相同。

对于终端所支持的应用列表中的每一个AID, 终端都应有标志表明将使用哪个匹配规则。

### 8.3.2 使用支付系统目录

如果终端选择支持使用支付系统目录方法进行应用选择, 它应该遵循本节所描述的过程来确定卡所支持的应用。图14是如下逻辑描述的流程图。

下面是终端使用目录方法的步骤:

1. 终端通过使用选择(SELECT)命令(参见第7章)来选择文件名为‘1PAY.SYS.DDF01’的支付系统环境而开始, 由此建立支付系统环境并进入初始目录。  
如果卡被锁定或者选择(SELECT)命令不支持(这两种情况都会回送状态码SW1 SW2 = ‘6A81’), 终端必须中断选择过程。  
如果IC卡上没有PSE, 那么IC卡应该对PSE的选择(SELECT)命令回送状态码‘6A82’ (文件没有找到)。在这种情况下, 终端必须使用8.3.3节所描述的使用应用列表的方式。  
如果PSE被锁定, IC卡应该回送状态码‘6283’。在这种情况下, 终端应该使用8.3.3节所描述的使用应用列表的方式。  
如果IC卡回送状态码SW1 SW2 = ‘9000’, 终端则转入步骤2。  
如果卡回送其他状态码SW1 SW2, 终端应该使用8.3.3节所描述的使用应用列表的方式。
2. 终端使用卡片返回的FCI中的目录SFI, 从目录的第1条记录开始, 连续读取后续记录, 直到卡回送状态码SW1 SW2 = ‘6A83’, 表示所请求的记录序号已不存在 (如果读记录(READ RECORD)命令中记录号大于文件的最后一条记录号时, 卡应该回送状态码‘6A83’)。如果在执行读记录(READ RECORD)命令查找第1个记录时, 卡回送状态码‘6A83’, 则表示目录入口为空, 转到下面的步骤6。  
对于目录中的每一条记录, 终端从第一个目录入口地址开始顺序执行步骤3到步骤5所描述的过程。如果记录中不包含目录入口, 终端应处理下一个目录记录。
3. 如果该入口对应某一ADF, 且ADF名与终端支持的一个应用相匹配(如8.3.1节定义), 则将该应用列入最终应用选择的“候选列表”中。
4. 如果该入口对应一个DDF, 则终端将中断当前的目录记录处理过程, 使用该DDF的名称选择该DDF。新的目录将使用步骤2到步骤5的过程进行读出和处理, 完成新的目录处理后, 终端将回到前一个被中断的目录处理的位置继续处理下一个入口。
5. 当终端处理完成第一个目录(PSE)中最后一个记录中的所有入口后, 所有能够按此方法找到的ADF就确定了, 查找和产生候选列表的工作完成。如果发现了至少一个匹配的AID, 终端将继续处理8.3.4节所描述的处理过程。
6. 如果步骤1到步骤5中没有发现与终端支持的应用所匹配的目录入口, 终端应该使用

8.3.3节所描述的使用应用列表的方式来寻找匹配的应用。



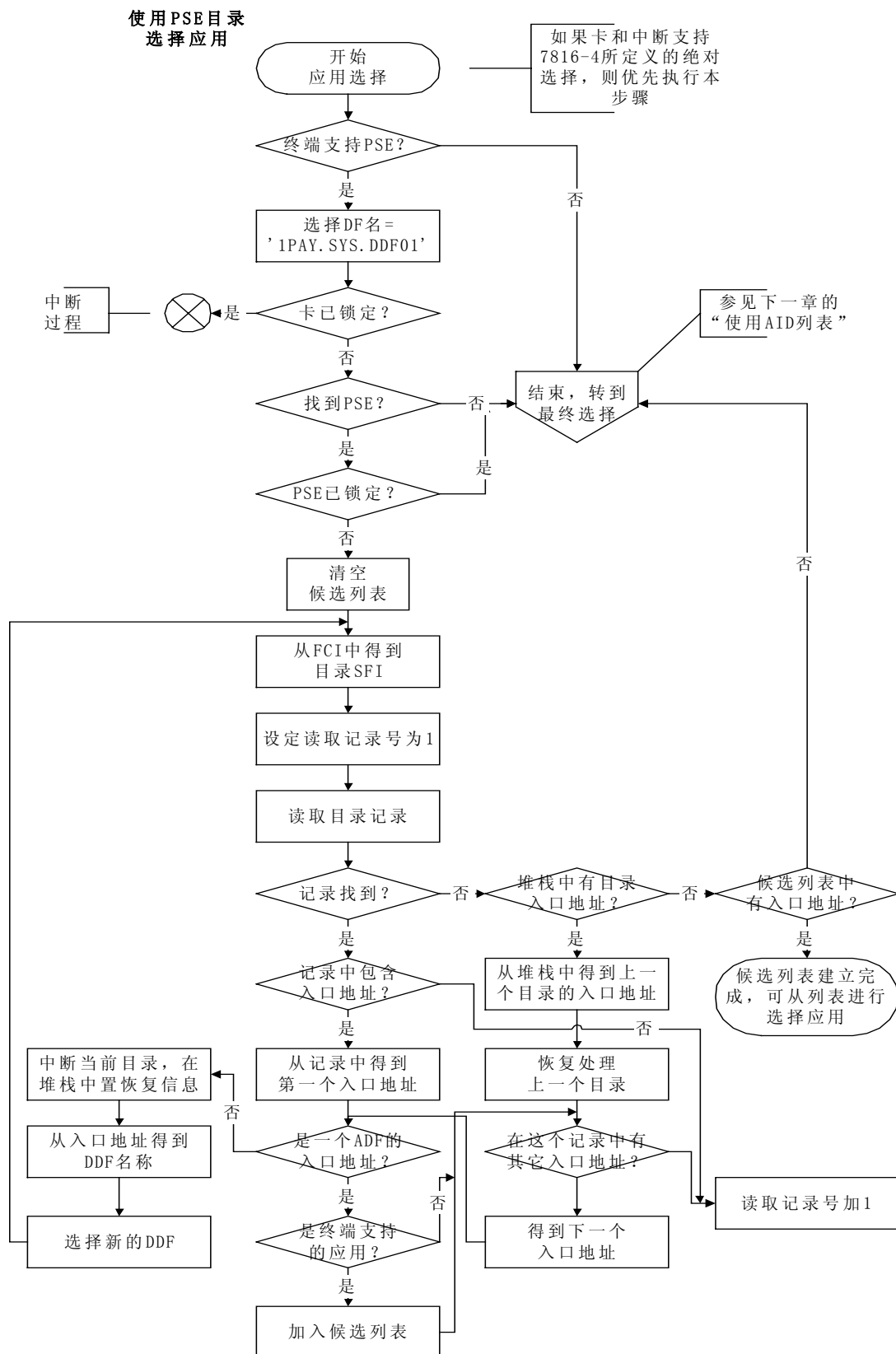


图 14 – 使用目录方法的终端逻辑

### 8.3.3 使用 AID 列表

如果卡片或终端有一方不支持PSE方法或者终端使用PSE目录没有找到匹配的应用，那么终端应使用它所支持的应用列表的方法建立候选列表。图15是如下逻辑描述的流程图。

终端执行以下步骤：

1. 终端使用其列表中的第一个AID<sup>11</sup>作为文件名发出选择(SELECT)命令。
2. 如果卡被锁定或者选择(SELECT)命令不支持导致选择(SELECT)命令失败(IC卡回送状态码SW1 SW2 = ‘6A81’)，终端将中断选择过程。
3. 如果选择(SELECT)命令执行成功(SW1 SW2 = ‘9000’或‘6283’)，终端应比较AID和卡返回的FCI中的DF名。DF名应该同AID相同(包括长度)，或者DF名以AID为开始并且长度大于AID。如果DF名比AID长，卡将进行部分名称选择处理。如果DF名同AID相同，终端应进入到步骤4。如果进行了部分名称选择，终端应进入步骤6。如果终端返回其它状态，应进入步骤5。
4. 如果选择(SELECT)命令成功(SW1 SW2 = ‘9000’)，终端应将所选择文件的FCI信息添加到候选列表中<sup>12</sup>并进入步骤5。如果应用已锁定(SW1 SW2 = ‘6283’)，终端应直接进入步骤5而不将DF名添加到候选列表。
5. 终端使用其列表中的下一个AID发出另一个选择(SELECT)命令，回到步骤3。如果列表中没有剩余的AID，那么候选列表建立完成，终端按照8.3.4节的规定进行后续处理。
6. 对应于AID列表，终端还保存了表明卡是否允许有多个应用匹配的应用选择标识。终端在选择应用时会检查该指示符。如果指示符表明只允许单个应用匹配，那么终端将不会把文件添加到候选列表，而是进入步骤7。  
如果允许多应用匹配，那么部分名称匹配即可。  
如果应用没有锁定(SW1 SW2 = ‘9000’)，终端将会添加FCI信息到候选列表，然后进入步骤7。  
如果允许多应用匹配但是应用已锁定(SW1 SW2 ≠ ‘9000’)，则终端应直接进入步骤7而不将FCI信息添加到候选列表。
7. 终端使用与之前相同的命令数据，但将命令中的P2参数设置为02(“选择下一个”)，重复发出选择(SELECT)命令，然后回到步骤3。

<sup>11</sup> 为了更清楚的帮助理解本节所描述的过程，有必要区别终端上的 AID 和 IC 卡上 AID。可以参见 8.3.1 节，即使在应用匹配时，这两者也不是完全相同的。术语“AID”用于终端上的应用标识符，“DF 名”用于卡上的应用标识符。

<sup>12</sup> 如果在最终选择期间给持卡人提供列表，则应用标签和应用优先名称必须保存。DF 名和应用优先权标识符在任何情况下都可能需要。

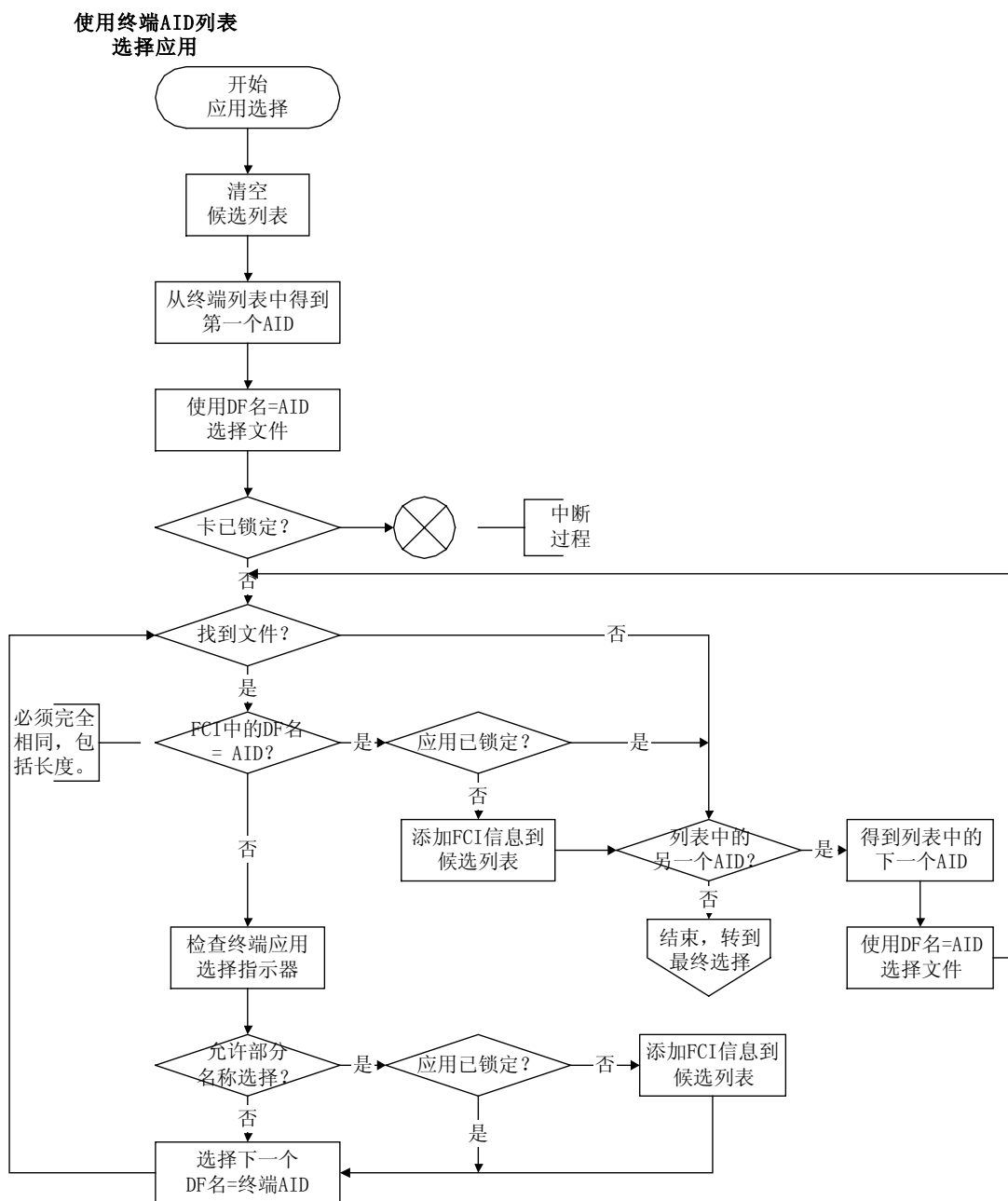


图 15 – 使用终端中的应用列表

### 8.3.4 最终选择

当终端确定了卡与终端共同支持的应用列表之后, 就进行如下处理:

1. 如果没有共同支持的应用, 交易终止。
2. 如果只有一个共同支持的应用, 则终端检查该应用的应用优先级标识符的b8位。如果b8 = '0', 则终端选择该应用。如果b8 = '1'并且终端提供持卡人的确认功能, 终端即请求持卡人确认。如持卡人确认, 则选择该应用。如果终端不提供持卡人的确认功能, 或终端请求确认而持卡人拒绝, 则终端终止该交易过程。
3. 如果有多个共同支持的应用, 则可以按照步骤4中的描述显示列表供持卡人选择, 或者按照步骤5的描述自动完成选择。步骤4是首选的方法。
4. 如果向持卡人显示列表, 则该列表应该按照级别优先的顺序排列, 高优先级的应用应该在前。如果卡上没有指定应用的优先顺序, 则以终端的应用优先顺序为准, 如果终端也没有指定应用的优先顺序, 则按照应用在卡中出现的顺序为准。如果出现多个应用有相同的优先级, 或某个入口缺少应用优先级标识符的情况, 也可采用类似的方法。也就是说, 在这种情况下, 终端可以使用自己的优先顺序, 也可以按卡上应用出现的顺序将有重复优先级或没有优先级的应用显示出来。
5. 终端可以无需持卡人的介入而直接选择应用。在这种情况下, 终端从共同支持的应用列表中选择优先级别最高的应用。如果终端不提供持卡人对选择的应用确认, 则那些不经过持卡人确认就不能选择的应用(应用优先级标识符的b8='1')应从可选列表从删除。

一旦终端或持卡人确定了待执行的应用, 则该应用应被选中。终端向该应用发出选择(SELECT)命令(按照第7章进行编码, 使用建立候选列表时得到的ADF名称(如果采用目录方式)或者FCI中的DF名(如果采用应用列表方式)作为数据域)。如果命令回送的状态码SW1 SW2 ≠ '9000', 则此应用应该从候选列表中删除, 然后回到步骤1。如果持卡人选择或确认了某个应用, 而随后该应用又因为应用锁定或其它原因被从候选列表中删除, 则应用不能在持卡人确认的情况下被选中。

在任何情况下, 终端应该在适当的时候提示持卡人相关动作的完成。

## 附录

## 附录 A 使用 T=0 协议交换的示例

以下示例说明了使用 T=0 协议在 TTL 和 IC 卡之间数据和过程字节的交换。请注意：

- 过程字节‘60’和 $\overline{INS}$ 的用法没有说明。
- [Data(x)]表示 x 个字节的数据。
- 情况 2 和 4 中 Le = ‘00’的命令要求从 IC 卡返回可能的最多数据。这些示例中使用 Le= ‘00’来说明执行本规范第三册中定义的应用时观察到的典型交换。

A1 到 A4 的示例说明了使用情况 1 到情况 4 的典型交换。A5 和 A6 中的示例说明了在情况 2 和 4 的命令中使用过程字节‘61xx’的交换。A7 说明了一个情况 4 的命令的警告条件。

## A1 情况 1 下的命令

一个形如 {CLA INS P1 P2} 的 C-APDU 从 TAL 传送到到 TTL(注意 C-TPDU 的 P3 置为‘00’)。

TTL	ICC
{CLA INS P1 P2 00}==>	
	<=90 00

TTL 向 TAL 返回形如 {90 00} 的 R-APDU。

## A2 情况 2 下的命令

一个形如 {CLA INS P1 P2} 的 C-APDU 从 TAL 传到到 TTL。

TTL	ICC
[ CLA INS P1 P2 00]=>	
	<=6C Licc
[CLA INS P1 P2 Licc]=>	
	<=INS[Data(Licc)] 90 00

TTL 向 TAL 返回形如 {[Data(Licc)]90 00} 的 R-APDU。

## A3 情况 3 下的命令

TAL 向 TTL 传递一个形如 {CLA INS P1 P2 Lc [Dara(Lc)]} 的 C-APDU

TTL	ICC
[ CLA INS P1 P2 Lc] =>	
	<=INS
[Data(Lc)]=>	
	<=90 00

TTL 向 TAL 返回一个形如 {90 00} 的 R-APDU。

#### A4 情况 4 下的命令

TAL 向 TAL 传送一个形如 {CLA INS P1 P2 Lc [Data(Lc)]00} 的 C-APDU。

TTL	ICC
[CLA INS P1 P2 Lc]=>	
	<=[INS]
[Data(Lc)]=>	
	<=61 Licc
[00 C0 00 00 Licc]=>	
	<=C0 [Data(Licc)]90 00

TTL 向 TAL 传送形如 {[Data(Licc)90 00]} 的 R-APDU。

#### A5 采用过程字节‘61’和‘6C’的情况 2 命令

TAL 向 TTL 传送形如 {CLA INS P1 P2 00} 的 C-APDU。

TTL	ICC
[CLA INS P1 P2 00]=>	
	<=6C Licc
[CLA INS P1 P2 Licc]=>	
	<=61 XX
[00 C0 00 00 yy]=>	
	<=C0 [Data(yy)] 61 zz
[00 C0 00 00 zz]=>	
	<=C0[Data(zz)] 90 00

当  $yy \leq xx$  时

TTL 向 TAL 传送形如 {[Data(yy+zz)]90 00} 的 R-APDU。

#### A6 采用过程字节‘61’的情况 4 命令

TAL 向 TTL 传送形如 {CLA INS P1 P2 Lc[Data Lc] 00} 的 C-APDU。

TTL	ICC
[CLA INS P1 P2 Lc]=>	
	<=[INS]
[Data(Lc)]=>	
	<=61xx
[00 C0 00 00 xx]=>	
	<=C0 [Data(xx)] 61 yy

[00 C0 00 00 yy]=>

<=C0 [Data(yy)] 90 00

TTL 向 TAL 返回形如 {[Data(xx+yy)] 90 00} 的 R-APDU。

#### A7 带警告条件的情况 4 命令

TAL 向 TTL 传送形如 {CLA INS P1 P2 Lc[Data Lc]00} 的 C-APDU。

TTL  
[CLA INS P1 P2 Lc]=>

ICC

<=[INS]

[Data(Lc)]=>

<=62 xx

[00 C0 00 00 00]=>

<=6C Licc

[00 C0 00 00 Licc]=>

<=C0 [Data(Licc)] 90 00

TTL 向 TAL 返回形如 {Data(Licc)} 62 xx} 的 R-APDU，其中包含了与警告状态字节一起的返回的数据。

## 附录 B 数据元表

表 B1 定义了可能用于应用选择和它们在数据对象和文件的映射的数据元。

名 称	描 述	来源	格式	模板	标签	长度
应用标识符(AID)- 卡片	标示了在 ISO/IEC 7816-5 中描述的应用	IC 卡	B	‘61’或 ‘A5’	‘4F’	5-16
应用标识符(AID) —终端	标示了在 ISO/IEC 7816-5 中描述的应用	终端	B	没有	‘9F06’	5-16
应用标签	与 ISO/IEC 中的 AID 相关的记忆符号	IC 卡	ans 1-16	‘61’或‘A5’	‘50’	1-16
应用优先名称	与 AID 相关的优先记忆符号	IC 卡	ans 1-16	‘61’或‘A5’	‘9F12’	1-16
应用优先指示符	指明了在一个目录下一个给定应用或一组应用的优先权	IC 卡	B	‘61’或 ‘A5’	‘87’	1
应用选择标识	对于被终端应用支持的 IC 卡应用,应用选择标识指明了终端上相关的 AID 是否一定正好符合卡上的 AID,这包括 AID 的长度,或仅仅等于终端 AID 的长度。 终端支持的每个 AID 仅仅有一个应用选择标识。	终端	由终端判定。 这个数据不通过接口发送。	没有	没有	看格式
专用文件(DF)名称	表明了 ISO/IEC 7816—4 中描述的 DF 名称	IC 卡	B	‘6f’	‘84’	5-16
目 录 定 义 文 件 (DDF)名称	标明与目录相关的 DF 名称	IC 卡	B	‘61’或‘A5’	‘9D’	5-16
目录自定义模板	ISO/IEC 7816-5 的目录的发卡行自定义部分	IC 卡	Var.	‘61’或‘A5’	‘73’	Var.一直到 252
文 件 控 制 信 息 (FCI)发卡行自定	FCI 的发卡行自定义部分	IC 卡	Var.	‘A5’	‘BF0C’	Var.一直到 222

义数据						
文件控制信息 (FCI)专有模板	按照与 ISO/IEC 7816-4 相关的 FCI 模板中的规范来标识数据对象专有的	IC 卡	Var.	‘6f’	‘A5’	Var.
文件控制信息 (FCI)模板	标识与 ISO/IEC7816-4 相关的 FCI 模板	IC 卡	Var.	-	‘6F’	Var.到 252
发卡行的应用数据	包含专有的应用数据，这些数据在联机交易中传输给发卡行	IC 卡	B	‘77’或‘80’	‘9F10’	Var.到 32
发卡行的代码表格 检索	指明了与 ISO8859 相关的代码表格来显示应用优先名称	IC 卡	N2	‘A5’	‘9F11’	1
首选语言	1-4 种语言按优先选择的次序来储存，每一种语言用 2 个数字字符按照 ISO639 来表示	IC 卡	an2	‘A5’	‘5F2D ,	2-8
处理选项数据对象 列表(PDOL)	包括终端常驻数据对象(标签和长度)的列表，这些数据对象被卡用在处理 GET PROCESSING OPITONS 命令或其它应用特殊的命令中	IC 卡	B	‘A5’	‘9F38’	Var.
短文件标识符 (SFI)	用在与应用基本文件或目录定义文件相关的命令中标识了 SFI。SFI 数据对象是二进制，其中高三位置为 0	IC 卡	B	‘A5’	‘88’	1

表 B1 — 数据元字典

当数据对象定义的长度大于实际数据长度时，应遵守下列规则：

- 格式 n 数据元右对齐并在前面填充 16 进制的 00
- 格式 an 的数据元左对齐并在后面填充 16 进制的 00

当数据从一处传递到另一处(例如，从卡片到终端)时，应按照从高位到低位的顺序传输，而不管数据内部是如何储存的。同样的规则也适用于连接。

分配给数据元的标签参照表 B2:

名称	模板	标签
应用标识符(AID)－卡片	‘61’或‘A5’	‘4F’
应用标识符(AID)－终端	没有	‘9F06’
应用标签	‘61’或‘A5’	‘50’
优先语言	‘A5’	‘5F2D’
文件控制信息(FCI)模板	—	‘6F’
命令自定义模板	‘61’或‘A5’	‘73’
专用文件(DF)名称	‘6F’	‘84’
语言优先级指示符	‘61’或‘A5’	‘87’
短文件标识符(SFI)	‘A5’	‘88’
目录定义文件(DDF)名称	‘61’或‘A5’	‘9D’
发卡行代码表索引	‘A5’	‘9F11’
应用首选名称	‘61’或‘A5’	‘9F12’
处理选项数据对象列表(PDOL)	‘A5’	‘9F38’
文件控制信息(FCI)专有模板	‘6F’	‘A5’
文件控制信息(FCI)发卡行自定义数据	‘A5’	‘BF0C’

表格 B2 数据元标签

## 附录 C 目录结构示例

### C1 目录结构示例

本附录中的示例描述了可能的 IC 卡文件逻辑结构。示例说明了目录结构层次，但没有涉及到 ISO 描述的文件层次。

图 C1 图示了一个简单的应用卡片，它仅有单层目录。在这个示例中，主文件(在 ISO/IEC 7816-4 中定义的文件标识符为‘3F00’)是卡上唯一的一个目录定义文件。主文件必须按照 8.2 定义的赋予首层 DDF 的唯一支付系统名。主文件的 FCI 必须包含 SFI 数据对象。

本例中的‘DIR A’不一定是 ISO 的 DIR 文件，但它必须遵循本规范，包括它必须包含一个范围为 1—10 的 SFI 的要求。ISO DIR 文件的标识符为‘2F00’，这表明 SFI 可能未在正确的范围之内。

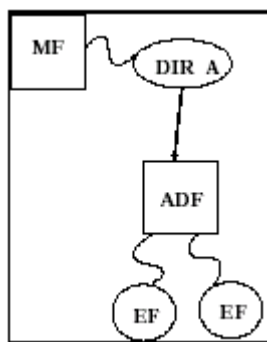


图 C1 - 最简单的卡结构 单应用

图 C2 举了一个具有单个目录的多应用卡的示例。在这个示例中根文件(MF)不支持符合本规范的应用，因而对主文件的功能没有限制。根据 ISO/IEC 7816-4，可能存在 DIR 文件，但第 8 节中定义的应用选择算法没有用到。同时注意目录没有到达所有 ADF(ADF2 到 ADF5)的入口，因为 ADF5 被忽略了。ADF5 只能被“知道”ADF5 可能在卡片上存在的终端选择。终端搜索 ADF5 的方法不在本规范返回之内。

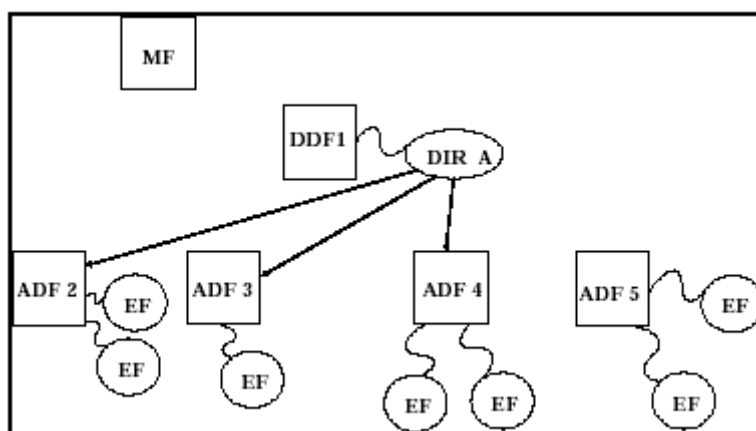


图 C2 - 单级目录

图 C3 是一个有 n 层目录结构的多应用卡的示例。第一层目录(‘DIR A’)有两个 ADF 的入口—ADF3 和 ADF4 和一个 DDF 的入口—DDF2。与 DDF2 相连的目录(‘DIR B’)有两个

ADF 的入口—ADF21 和 ADF22 和一个 DDF 的入口—DDF6。DDF5 在根目录中没有入口，因而只能被“知道”DDF5 存在的终端找到。终端找到 DDF5 的方法不在本规范范围之内。但是连到 DF5 的目录结构(‘DIR C’)也可以遵循本规范，且如果被终端找到，可以把终端引到 DF51、DF52 和 DF53。连到 DDF6 的 DIR D 是第三层的目录且指向四个文件(未显示)，它们可能是 ADF 和更多的 DDF。

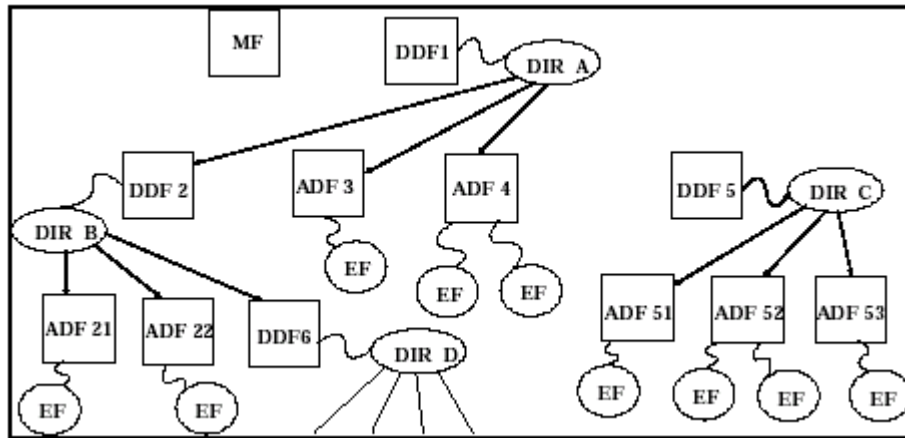


图 C3 - 三级目录