ICS 35.240.40
A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0025.3—2018
代替 JR/T 0025.3—2013

中国金融集成电路（IC）卡规范 第3部分：与应用无关的IC卡与终端接口规范

China financial integrated circuit card specifications—
Part 3: Specification on application independent ICC to terminal interface requirements

2018－11－28 发布　　2018－11－28 实施

中国人民银行　发布

目　次

前　言

JR/T 0025—2018《中国金融集成电路（IC）卡规范》分为14部分：

——第1部分：总则；

——第3部分：与应用无关的IC卡与终端接口规范；

——第4部分：借记/贷记应用规范；

——第5部分：借记/贷记应用卡片规范；

——第6部分：借记/贷记应用终端规范；

——第7部分：借记/贷记应用安全规范；

——第8部分：与应用无关的非接触式规范；

——第10部分：借记/贷记应用个人化指南；

——第12部分：非接触式IC卡支付规范；

——第13部分：基于借记/贷记应用的小额支付规范；

——第14部分：非接触式IC卡小额支付扩展应用规范；

——第15部分：电子现金双币支付应用规范；

——第16部分：IC卡互联网终端规范；

——第18部分：基于安全芯片的线上支付技术规范。

本部分为JR/T 0025—2018的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替JR/T 0025.3—2013《中国金融集成电路（IC）卡规范　第3部分：与借记/贷记应用无关的IC卡与终端接口需求》，与JR/T 0025.3—2013相比主要技术变化如下：

对于原规范第17部分的引用修改为对现有规范第7部分的引用。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC 180）归口。

本部分起草单位：中国人民银行、中国工商银行、中国银行、中国建设银行、中国农业银行、交通银行、中国邮政储蓄银行、中国银联股份有限公司、中国金融电子化公司、银行卡检测中心、中金金融认证中心有限公司、北京中金国盛认证有限公司、中钞信用卡产业发展有限公司、捷德（中国）信息科技有限公司、惠尔丰（中国）信息系统有限公司、福建联迪商用设备有限公司。

本部分主要起草人：李伟、王永红、李晓枫、陆书春、潘润红、李兴锋、宋汉石、渠韶光、邵阔义、邬向阳、杨倩、聂丽琴、杜宁、周玥、张宏基、程胜、汤沁莹、黄本涛、陈则栋、吴晓光、李春欢、刘志刚、张永峰、李新、张栋、王红剑、李一凡、洪隽、胡吉晶、吴潇、魏猛、余沁、尚可、周新衡、张步、冯珂、李建峰、向前、涂晓军、齐大鹏、陈震宇、郑元龙、聂舒、丁吉、白雪晶、李子达、沈卓群、刘世英、于海涛、翁秀诚、张行、刘文其、王飞宇、章盼、张波波、汪小八、毛瑞红、叶昀。

本部分代替了JR/T 0025.3—2013。

JR/T 0025.3—2013的历次版本发布情况为：

JR/T 0025.3—2005、JR/T 0025.3—2010。

引　言

与应用无关的IC卡与终端接口规范是与应用无关的规范，发卡机构可以根据实际需求将接触式接口与借记/贷记应用相结合，形成接触式的借记/贷记应用；还可以与未来出现的新支付应用结合，具有较高的灵活性。

中国金融集成电路（IC）卡规范
第3部分：与应用无关的IC卡与终端接口规范

1 范围

本部分规定了与应用无关的IC卡与终端接口方面的内容，包括卡片的机电接口、卡片操作过程、字符的物理传输、复位应答、传输协议、文件、命令及应用选择机制等。

本部分适用于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 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2659 世界各国和地区名称代码

GB/T 4880.1 语种名称代码 第1部分：2字母代码

GB/T 15120.1 识别卡 记录技术 第1部分：凸印

GB/T 15120.3 识别卡 记录技术 第3部分：ID-1型卡上凸印字符的位置

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

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

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

GB/T 16649.4—2010 识别卡 集成电路卡 第4部分：用于交换的结构、安全和命令

GB/T 16649.5—2002 识别卡 带触点的集成电路卡 第5部分：应用标识符的国家编号体系和注册规程

GB/T 16711 银行业 银行电信报文 银行标识代码

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

GB/T 20543.1—2011 金融服务 国际银行账号（IBAN） 第1部分：IBAN的结构

GB/T 20543.2—2011 金融服务 国际银行账号（IBAN） 第2部分：注册机构的角色和职责

JR/T 0025—2018（所有部分） 中国金融集成电路（IC）卡规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

块 block

包含两个或三个域（头域、信息域和尾域）的字符组。

3.2

字节 byte

由指明的8位数据b1到b8组成，从最高有效位（MSB，b8）到最低有效位（LSB，b1）。

3.3

冷复位 cold reset

当提供给IC卡的电源电压和其他信号从静止状态中复苏且收到复位信号后，IC卡产生的复位。

3.4

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。

3.5

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。

3.6

凸印 embossing

在卡片正面凸起的字符。

3.7

尾域 epilogue field

块的最后一部分，包括错误校验码（EDC）。

3.8

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0.5伏时，则称电源电压和这些信号处于静止状态。

3.9

接口设备 interface device

终端上插入IC卡的部分，包括其中的机械和电气部分。

3.10

磁条 magnetic stripe

包括磁编码信息的条状物。

3.11

半字节 nibble

一个字节的高四位或低四位。

3.12

填充 padding

向数据串某一端添加附加位。

3.13

路径 path

没有分隔的文件标识符的连接。

3.14

支付系统 payment system

JR/T 0025—2018中指相关清算组织的银行卡转接系统。

3.15

头域 prologue field

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

3.16

信号幅度 signal amplitude

信号高、低电压的差值。

3.17

模板 template

结构数据对象的值域，定义为数据对象的逻辑分组。

3.18

类型ABC class ABC

卡片和终端支持的供电电压值类型。有三种可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。

4 缩略语

下列缩略语适用于本文件。

ACK——确认（Acknowledgment）
ADF——应用定义文件（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——应用选择指示器（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）
℃——摄氏或摄氏度（Degree Celsius）
C-APDU——命令 APDU（Command APDU）
C_{IN}——输入电容（Input Capacitance）
CLA——命令报文的类别字节（Class Byte of the Command Message）
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——目的节点地址（Destination Node Address）
DC——直流（Direct Current）
DDF——目录定义文件（Directory Definition File）
DF——专用文件（Dedicated File）
DIR——目录（Directory）
EDC——错误校验码（Error Detection Code）
EF——基本文件（Elementary File）
Etu——基本时间单元（Elementary Time Unit）
F——频率（Frequency）
FCI——文件控制信息（File Control Information）
GND——地（Ground）
I/O——输入/输出（Input/Output）
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）
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）
INF——信息域（Information Field）
INS——命令报文的指令字节（Instruction Byte of Command Message）
I_{OH}——高电平输出电流（High Level Output Current）
I_{OL}——低电平输出电流（Low Level Output Current）
ISO——国际标准化组织（International Organization for Standardization）
LRC——纵向冗余校验（Longitudinal Redundancy Check）
M——必备（Mandatory）
m.s.——最高位（Most Significant Bit）
m/s——米/秒（Metres per Second）
mA——毫安（Milliampere）
MAC——报文鉴别码（Message Authentication Code）
Max——最大值（Index to Define a Maximum Value）
MF——主文件（Master File）

Min——最小值（Index to Define a Minimum Value）
mm——毫米（Millimeter）
MΩ——兆欧（Megaohm）
N——数字型（Numeric）
NAD——节点地址（Node Address）
NAK——否定确认（Negative AcKnowledgement）
nAs——纳安秒（Na An SEC）
Ns——纳秒（Nanosecond）
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（Picofarads）
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）
RFU——预留（Reserved for Future Use）
RID——注册的应用提供商标识（Registered Application Provider Identifier）
RST——复位（Reset）
SAD——源节点地址（Source Node Address）
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_F——信号幅度从 90%下降到 10%的时间（Fall Time Between 90% and 10% of Signal Amplitude）
TPDU——传输协议数据单元（Transport Protocol Data Unit）
t_R——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）
V_{CC}——VCC 触点上的测量电压（Voltage Measured on VCC Contact）
VCC——电源电压（Supply Voltage）
V_{IH}——高电平输入电压（High Level Input Voltage）
V_{IL}——低电平输入电压（Low Level Input Voltage）
V_{OH}——高电平输出电压（High Level Output Voltage）
V_{OL}——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）

Xx——任意值

5 机电接口

5.1 概述

本章包括低电压IC卡迁移、IC卡和终端的电气及机械特性。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 GB/T 16649.1—2006、GB/T 16649.2—2006、GB/T 16649.3—2006、GB/T 16649.4—2010、GB/T 16649.5—2002，并依据实际需要与技术发展，做了一些细小变动。

5.2 低电压 IC 卡迁移

只支持类型A的卡片已在2013年12月底前被类型AB或者类型ABC的卡片所替代。当使用中的卡片都支持类型AB或者类型ABC时，除了配置只支持类型A的终端，还有可能配置只支持类型B的终端。

下面描述的是由于发生这种迁移而引起对卡片和终端的要求。表1用符号表明了不同点。

表1 低电压卡迁移

符号	信息	值
在 2013 年 12 月底前的类型 A 卡片	应用于类型 A 卡片	在 2013 年 12 月底前被允许用于流通中的卡片。从 2014 年 1 月份起流通中的卡片要么是类型 AB，要么就是类型 ABC。
从 2014 年 1 月开始的新卡值	应用于下列卡片： ● 类型 A（2013 年 12 月底前） ● 类型 AB ● 类型 ABC	立即被应用直到进一步的通知。从 2014 年 1 月起类型 A 卡片不再流通；从 2014 年 1 月起只有类型 AB 或者类型 ABC 可以流通。
2013 年 12 月底前的类型 A 终端	应用于类型 A 终端（或者是多类型终端的类型 A 部件）	在 2013 年 12 月底前应被应用于类型 A 终端。从 2014 年 1 月起，对于使用中的采用这些值的终端不要求做升级。
从 2014 年 1 月起的新终端值	应用于类型 A、类型 B 和类型 C 终端	在 2013 年 12 月底前不能被应用于终端。从 2014 年 1 月起，应被应用于新的类型 A 或类型 B 终端。在 JR/T 0025—2018 规定之前不能配置类型 C 终端（除非是 JR/T 0025—2018 范围外的特定目的）。

5.3 IC 卡的机械特性

5.3.1 概述

本条描述了IC卡的物理特性和触点的分配。

5.3.2 物理特性

除本条的特殊规定外，IC卡应满足GB/T 16649.1—2006中规定的物理特性。在模块高度方面还应满足：

——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。

5.3.3 触点的尺寸和位置

触点的尺寸和位置见图1。

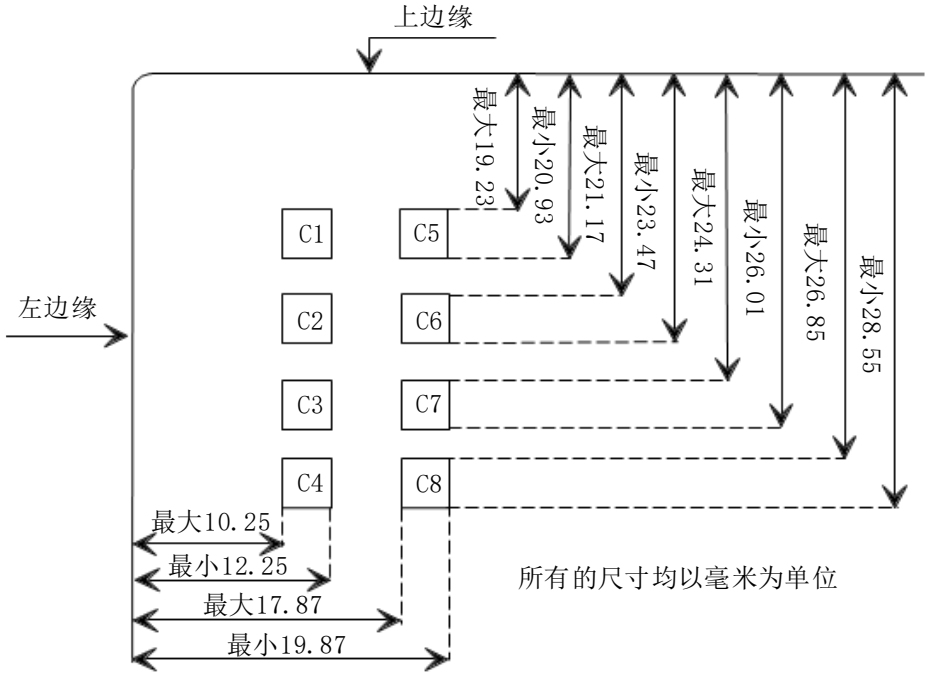

图1 IC 卡触点的尺寸和位置

区域C1、C2、C3、C5和C7表面应用导电层完全覆盖，构成IC卡的基本触点。区域C4、C6、C8和GB/T 16649.2—2006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，则他们应和集成电路（IC）、相互之间以及其他触点区域在电路上隔离[1)]。同时，任何两个导电区域之间除了通过IC都不能导通。基本触点的分配，见表2。

触点相对于凸印及磁条的布局应如图2。

1) 电路上隔离意味着：在此触点和任何其他导电表面上施以 5V DC 电压时在二者上测得的电阻应≧10MΩ。

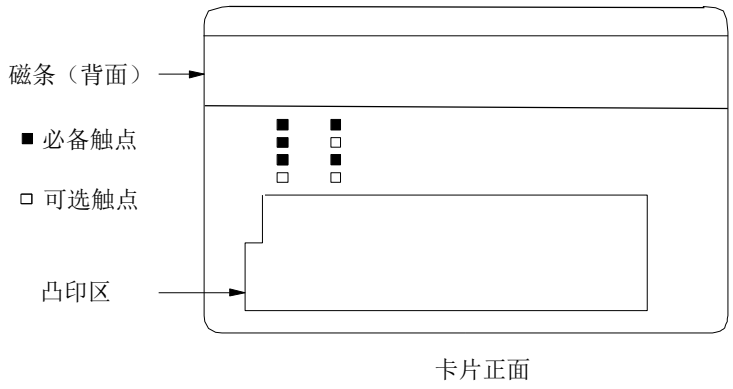

图2　触点的布局

应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。

5.3.4　触点的分配

IC卡上触点的分配遵循GB/T 16649.2—2006的规定，见表2。

表2　IC卡触点的分配

C1	电源电压（VCC）	C5	地（GND）
C2	复位信号（RST）	C6	未使用
C3	时钟信号（CLK）	C7	输入/输出（I/O）
注：C6在GB/T 16649定义为编程电压（VPP）。			

C4和C8未使用，可以不作实际设置。

5.4　IC卡的电气特性

5.4.1　概述

本条描述了在IC卡触点上测量出的信号的电气特性。

5.4.2　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卡应能够在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。

5.4.3　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（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。

5.4.3.1　接收模式

在接收模式下，当电源电压（VCC）在5.4.7中规定的范围内时，IC卡应能正确地解释特性如表3所示的来自终端的信号。

表3　接收模式下 IC 卡 I/O 的电气特性

2014 年 1 月起的新卡值			
符号	最小值	最大值	单位
V_{IH}	0.7×Vcc	Vcc	V
V_{IL}	0	0.2×V_{CC}	V
t_R 和 t_F	—	1.0	μs
在-0.3V 到 Vcc+0.3V 范围内的 I/O 信号干扰不应损坏 IC 卡。			

5.4.3.2　发送模式

在发送模式下，IC卡应向终端传送特性见表4所示的数据。

表4　发送模式下 IC 卡 I/O 的电气特性

2014 年 1 月起的新卡值				
符号	条件	最小值	最大值	单位
V_{OH}	-20μA＜IOH＜0，Vcc=min.	0.7×Vcc	Vcc	V
V_{OL}	类型 A： 0＜I_{OL}＜1mA 类型 B 和类型 C： 0<I_{OL}<0.5mA	0 0	0.08×V_{CC} 0.15×V_{CC}	V
tR 和 tF	C_{IN}（terminal）=30pF max.	—	1.0	μs

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。

5.4.4　编程电压（VPP）

IC卡不需要编程电压VPP（见5.3.4的注）。

5.4.5　时钟（CLK）

当VCC在5.4.7所规定的范围内时，IC卡应能在具有表5所示特性的时钟信号作用下正常工作。

表5　IC 卡 CLK 的电气特性

2014 年 1 月起的新卡值				
符号	条件	最小值	最大值	单位
V_{IH}		0.7×Vcc	Vcc	V
V_{IL}		0	0.2×V_{CC}	V
t_R 和 t_F		_	9%的时钟周期	μs
在-0.3V 到 Vcc+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卡应能正常工作。

当时钟频率处于1MHz到5MHz之间时，IC卡应能正常工作。

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

5.4.6 复位（RST）

当VCC在5.4.7所规定的范围内时，IC卡应能正确解释具有表6所示电气特性的复位信号。

表6 IC卡RST的电气特性

2014年1月起的新卡值				
符号	条件	最小值	最大值	单位
V_{IH}		0.7×Vcc	Vcc	V
V_{IL}		0	0.2×V_{CC}	V
t_R 和 T_F	Vcc=min 到 max.	_	1.0	μs
注：在-0.3V到Vcc+0.3V范围内的RST端的干扰信号不应损坏IC卡。				

IC卡应利用激活的低复位信号，采用异步方式进行复位应答。

5.4.7 电源电压（VCC）

在电源电压VCC为5V±0.5V直流电的情况下，IC卡应能正常工作。此时，时钟频率应在5.4.5中所规定的范围内，最大电流为50mA。

在给IC卡提供规定的电压基础上定义了三种类型的操作，见表7定义。IC卡应支持类型A，也可以可选地支持一个或者多个连续类型。如果提供了在该类型支持范围内的电压，则IC卡要能正确工作。

表7 IC卡电压和电流

2014年1月份起的新卡值				
符号	条件	最小值	最大值	单位
V_{CC}	类型A	4.50	5.50	V
	类型B	2.70	3.30	
	类型C	1.62	1.98	
I_{CC}	类型A		50	mA
	类型B		50	
	类型C		30	

当IC卡在他不支持的类型下操作时不应被损坏（如果IC卡不再按规定操作，或者他包含错误数据，则认为IC卡已被损坏）。

如果IC卡不只支持一个类型，在给他提供所支持类型规定范围内的电压时，他应能正确操作，见表8。

表8 IC卡必备和可选操作电压范围

2014年1月起的新卡值			
支持类型	IC卡应操作于	IC卡可操作于	单位
A和B	4.50-5.50	3.30-4.50	V
	2.70-3.30		
A、B和C	4.50-5.50	3.30-4.50	V

	2.70-3.30 1.62-1.98	1.98-2.70	

出于特定原因，终端可以支持与IC卡协商所使用电压的能力，但是这超出了JR/T 0025—2018的范围，因此不要求满足该规范的IC卡支持这种协商。如果IC卡在ATR中返回了如GB/T 16649.3—2006所定义的类型指示符，那么遵循JR/T 0025—2018的终端可以拒绝这个ATR。为了避免互操作性的问题，应在冷复位ATR中返回任何使用的类型指示符；为了保证冷复位ATR被拒绝后该IC卡能被终端接受，则热复位的ATR应为基本ATR。

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。

5.4.8 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）应小于500mΩ。（见GB/T 17554.3—2006的测试方法）

注：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。

5.5 终端的机械特性

5.5.1 概述

本条描述了终端接口设备的机械特性。

5.5.2 接口设备

用于插入IC卡的接口设备应具备接收IC卡的能力，并具有以下特性：

——物理特性满足 GB/T 16649.1—2006 的规定；

——正面触点位置应满足 GB/T 16649.2—2006 中图 2 的规定；

——凸印应满足 GB/T 15120.1 和 GB/T 15120.3 的规定。

接口设备的触点分布应保证如图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，接口设备不应有其他触点。

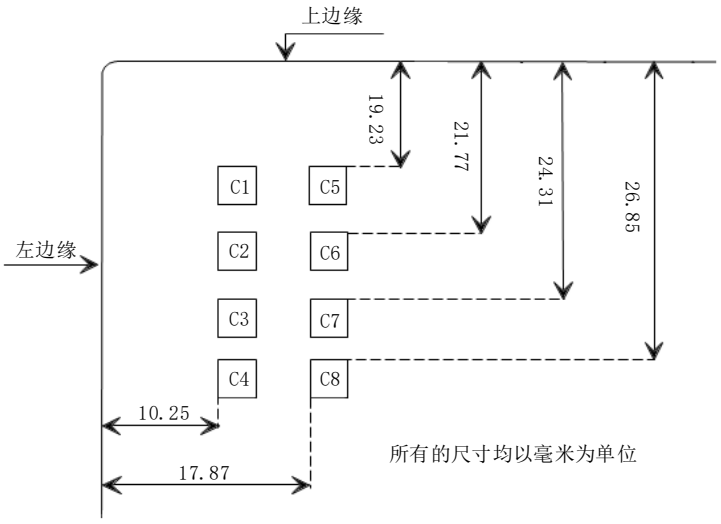

图3　终端触点分布和尺寸

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。

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。

5.5.3　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。

5.5.4　触点分配

接口设备触点的分配，见表9。

表9　接口设备触点的分配

C1	电源电压（VCC）	C5	地（GND）
C2	复位信号（RST）	C6	未使用
C3	时钟信号（CLK）	C7	输入/输出（I/0）
注：C6在GB/T 16649定义为编程电压（VPP）。			

C4和C8不使用，在物理上可以不存在。

5.6　终端的电气特性

5.6.1　概述

本条描述了在接口设备（IFD）触点上测量出的信号的电气特性。

5.6.2　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℃。应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。

5.6.3　输入/输出（I/0）

5.6.3.1　发送模式

该触点作为输出端（发送模式）向IC卡传送数据。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。在发送模式下，终端应向IC卡传送具有表10所示特性的数据。

表10　发送模式下的终端 I/0 电气特性

2014 年 1 月起的新终端值				
符号	条件	最小值	最大值	单位
V_{OH}	$0<I_{OH}<20\mu A$	0.8×Vcc	Vcc	V
V_{OL}	$-0.5mA<I_{OL}<0$	0	$0.15\times xV_{CC}$	V
t_R 和 t_F	$C_{IN\ (ICC)}$ =30pF max.	—	0.8	μs

信号干扰	低电平	-0.25	$0.15\times V_{CC}$	V
	高电平	0.8×Vcc	Vcc+0.25	V

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。

5.6.3.2 接收模式

该触点作为输入端（接收模式）从IC卡接收数据。当终端和IC卡都处于接收模式时，触点应处于高电平状态。除非VCC加电并稳定在5.6.7中允许的范围内，终端不应将I/O置于高电平状态。见6.2.3有关触点激活的内容。在接收模式下，终端应能正确解释从IC卡发来的具有表11所示特性的信号。

表11 接收模式下的终端 I/O 电气特性

2014年1月份起的新终端值			
符号	最小值	最大值	单位
V_{IH}	0.6×Vcc	Vcc	V
V_{IL}	0	$0.20\times V_{CC}$	V
t_R 和 T_F	—	1.2	μs

5.6.3.3 输入/输出补充说明

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。

5.6.4 编程电压（VPP）

C6应在电气上隔离。电气隔离意味着在C6和其他任何触点上施以5V的直流电压时，二者之间的电阻应≥10MΩ。如果在终端中导通，则C6应在整个卡片操作过程中保持在GND和1.05×Vcc之间。

注：在新终端中隔离C6可以把他用于JR/T 0025—2018未来版本可能规定的其他用途上。

5.6.5 时钟（CLK）

终端应产生具有表12所示特性的时钟信号。

表12 终端 CLK 的电气特性

2014 年 1 月起的新终端值				
符号	条件	最小值	最大值	单位
V_{OH}	$0<I_{OH}<50\mu A$	0.8xVcc	Vcc	V
V_{OL}	$-50\mu A<I_{OL}<0$	0	$0.15\times xV_{CC}$	V
t_R 和 t_F	$C_{IN\ (ICC)}$ =30pF max.	—	8%的时钟周期	μs
信号干扰	低电平	-0.25	$0.15\times V_{CC}$	V
	高电平	0.8xVcc	Vcc+0.25	V

稳定运行时，时钟占空因数应在其周期的45%～55%之间。

频率范围应在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%。

5.6.6 复位（RST）

终端应产生具有表13所示特性的复位信号。

表13　终端 RST 的电气特性

2014 年 1 月起的新终端值				
符号	条件	最小值	最大值	单位
V_{OH}	$0<I_{OH}<50\mu A$	0.8xVcc	Vcc	V
V_{OL}	$-50\mu A<I_{OL}<0$	0	$0.15\times V_{CC}$	V
t_R 和 t_F	$C_{IN\ (ICC)}$ =30pF max.	—	0.8	μs
信号干扰	低电平	-0.25	$0.15\times V_{CC}$	V
	高电平	0.8xVcc	Vcc+0.25	V

5.6.7　电源电压（VCC）

终端应提供5V±0.4V的直流电压，并应能稳定输出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及通讯链路故障等。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。脉冲的最大包络见图4。

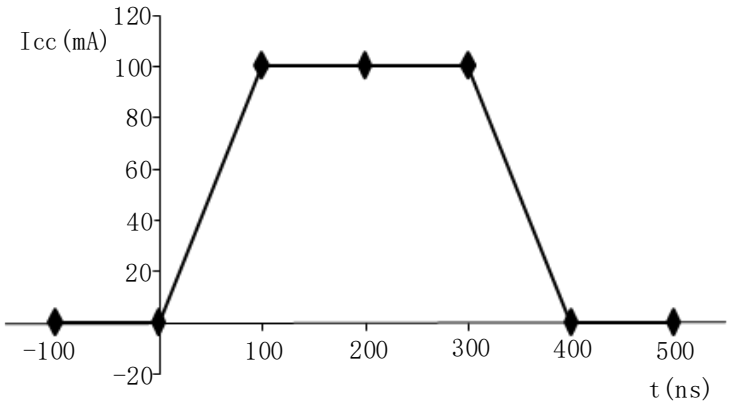

图4　最大电流脉冲包络

终端应为所支持的类型产生一个满足表14定义范围内的VCC，并且能在VCC维持的该范围内释放相应稳定的输出电流。如果终端不只支持一种类型，他应从包含最大电压值范围的类型中产生一个VCC。

基于特定的原因，终端可以支持与IC卡协商所使用电压的能力，但是这已经超出了JR/T 0025—2018的范围，符合JR/T 0025的IC卡不支持这种协商能力。企图与这样的IC卡进行类型协商将导致该IC卡不被接受。

所提供的电压应被保护，以避免由于终端的内部操作和从电源线及通信线路等引入的外部干涉而引起的短暂冲击和振荡的影响。VCC不应低于-0.25V（相对地）。

表14　终端电压和电流

符号	条件	最小值	最大值	单位
V_{CC}	类型 A	4.60	5.40	V
	类型 B	2.76	3.24	
	类型 C	1.66	1.94	
I_{CC}	类型 A	55		mA
	类型 B	55		
	类型 C	35		

在IC卡的正常操作中，测量IC卡触点上由于电流脉冲引起的V_{CC}电压波动。所提供的电能应能抵消IC卡消耗电流中的波动，这种IC卡应处于图5所示的类型操作最大电流脉冲包络中，确保Vcc维持在所规定的范围内。

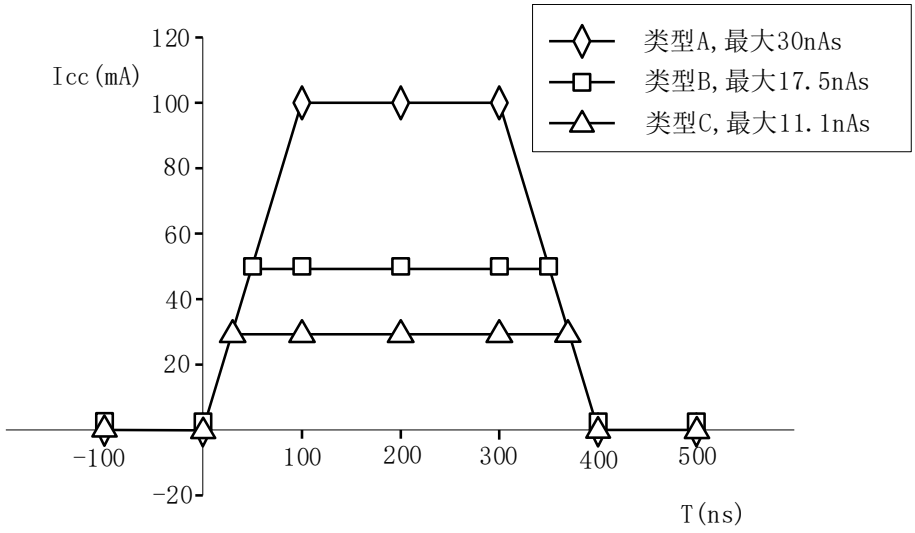

图5　最大电流脉冲包络

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。

5.6.8　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。（见GB/T 17554.3—2006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。

5.6.9　短路保护

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

5.6.10　终端插入 IC 卡后的加电和断电

插入IC卡后，当对终端进行加电或断电时，所有的信号电压应保持在5.5规定的范围之内，触点激活和释放的时序应分别符合6.2.3和6.2.6的规定。

6 卡片操作过程

6.1 概述

本章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。

6.2 正常卡片操作过程

6.2.1 概述

本条描述了执行一个正常交易的操作过程。

6.2.2 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。

6.2.3 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5.6的规定，VCC在触点接触时应小于或等于0.4V）。当IC卡正确插入接口设备后，触点应按如下方式激活（见图6）：

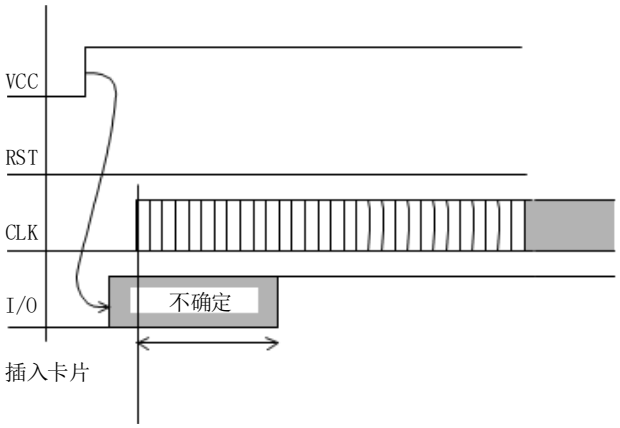

图6 触点激活时序

——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 激活之前给 VCC 加电；

——终端确认 VCC 稳定在 5.6.7 所规定的范围内以后，应将 I/O 置于接收模式并提供 5.6.5 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他方式来确定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。

6.2.4 IC 卡复位

6.2.4.1 冷复位

在6.2.3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7），过程如下：

——终端应在 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 7 中的 t1 所示）内开始；

——终端应在 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，终端应在不早于 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。

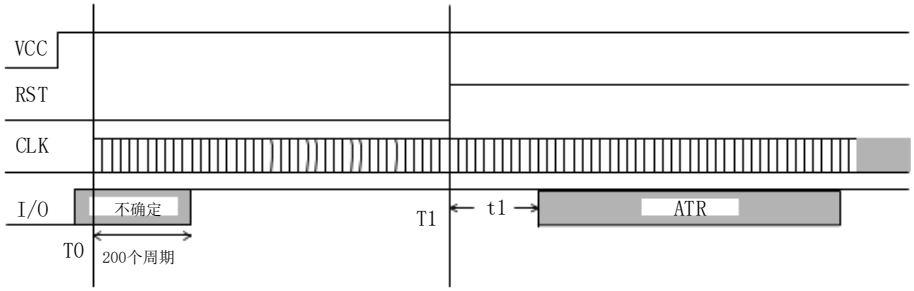

图7　冷复位时序

6.2.4.2　热复位

在6.2.4.1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第8章的规定，终端将启动热复位并从IC卡获得复位应答，见图8。其过程如下：

——热复位应从 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，终端应根据 5.6.7 和 5.6.5 的规定保持 VCC 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 8 中的 t1’所示）内开始；

——终端应在 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 8 中 T1’所示）。如果没有收到来自 IC 卡的复位应答信息，终端应在不早于 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。

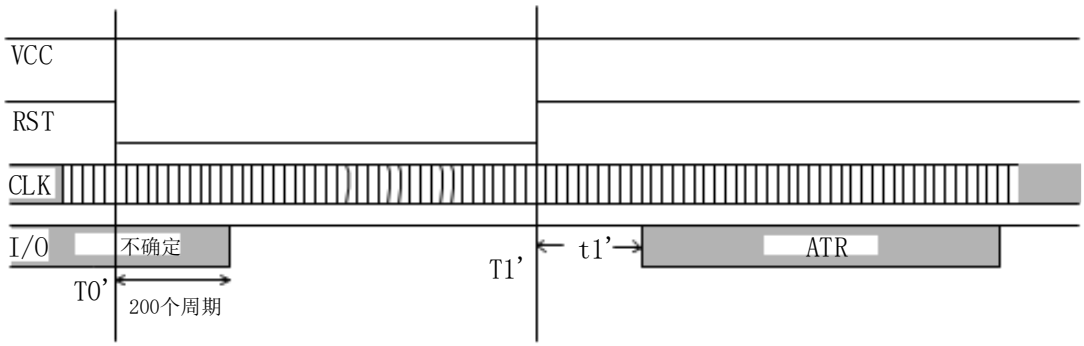

图8　热复位时序

6.2.4.3　IC卡复位补充说明

IC卡应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7章中描述，而其内容在8.3和8.4中描述。

6.2.5　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第8章及JR/T 0025.4—2018、JR/T 0025.5—2018、JR/T 0025.6—2018、JR/T 0025.7—2018中描述。

6.2.6　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），终端应如下释放接口设备触点（见图9）：

——终端应通过把 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 VCC 断电之前，终端应将 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，终端应切断 VCC 电源。此时的 VCC 应小于或等于 0.4V；

——释放过程应在 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。

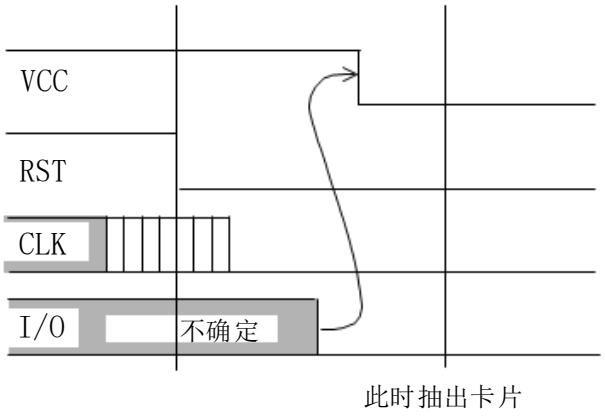

图9　触点释放时序

6.3　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，终端应能够检测到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6.2.5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应释放触点。

7 字符的物理传输

7.1 概述

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9章中描述的两种传输协议中使用。

7.2 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：

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

复位应答（和全局参数F和D的确定，见第8章）后的位持续时间称为当前etu，由下列方程给出：

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

注：JR/T 0025—2018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372/f。除非另有说明，以后所提到的etu，均为当前etu。

7.3 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8.4.2）。

字符传输之前，I/O应被置为高电平状态。

每个字符由10个连续位组成（见图10）：

——1 个低电平状态的起始位；

——组成数据字节的 8 个数据位；

——1 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。

字符中的逻辑‘1’的数目应是偶数，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，起始位的存在应在0.7etu之内验证，后续各位应在（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9.3.4）。

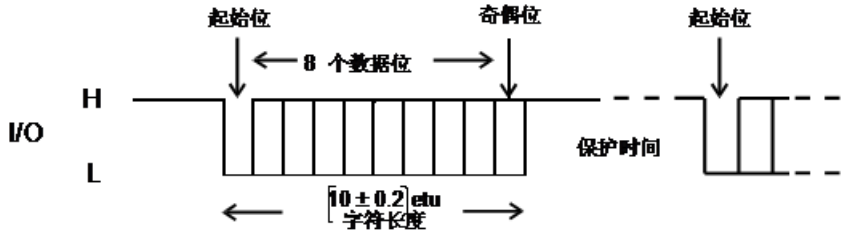

图10　字符帧

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8.4）。

8　复位应答

8.1　概述

如6.2.4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8章和第9章中，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’。

8.2　复位应答期间回送字符的物理传输

本章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7.2定义，字符帧在7.3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[2)]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。

8.3　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。本条中描述了针对支持T=0协议或针对T=1协议的IC卡（卡片只支持其中一种）复位应答期间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JR/T 0025—2018的终端的互操作性。

2)　因为 etu 代表的周期与频率相关（见 7.2），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，但其中之一应是T=0或T=1，且首选协议应是T=0或T=1。除非终端因为特殊需要而支持选择IC卡提供的其他协议的机制，终端应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JR/T 0025—2018的规定之列。

注：JR/T 0025—2018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JR/T 0025—2018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他传输控制参数值，但这已超出JR/T 0025—2018的范围。符合JR/T 0025—2018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15和表16，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，其回送字符见表15。

表15 T=0 时的基本 ATR

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 8.4.4.4）

对于采用 T=1 协议（基于块的异步半双工传输协议）的 IC 卡，其回送字符见表 16。

表16 T=1 时的基本 ATR

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 8.4.4.4）
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 8.4.5	校验字符

8.4 字符定义

8.4.1 概述

本条对复位应答中可能回送的字符进行了详细描述。

每个字符的描述按以下结构组织：

——名称；

——GB/T 16649.3—2006 描述的用途；

——基本应答。为保证互操作性，热复位应答中应包括这些字符；

——如果终端收到 JR/T 0025—2018 规定范围之外的字符，终端的规定动作。

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斥其他字符值的使用，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，他可以回送附加字符（见第9章）。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JR/T 0025—2018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JR/T 0025—2018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JR/T 0025—2018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。

终端应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，他应拒绝IC卡。

在以下描述中，如果指明，终端应采取以下动作：

——拒绝复位应答，则意味着终端应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，则意味着终端应释放触点以结束卡片操作过程；

——接受复位应答，则意味着终端应在本章规定的对其他所有字符的要求都满足的情况下接受复位。

8.4.2 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）LHHLLLLLLLH—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：终端应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，但应拒绝接受返回包含其他TS值的ATR的IC卡。

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’。

8.4.3 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17－T0的基本响应编码）。

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。

注：JR/T 0025—2018既不使用历史字符，也不禁止使用历史字符。历史字符的使用方法、结构和含义并不在JR/T 0025—2018的讨论范围内。但是，一旦使用了历史字符，JR/T 0025—2018强烈建议历史字符的结构和含义宜遵循GB/T 16649.4的定义。遵循本部分的终端，应忽略历史字节的存在，不应因无法识别或无法解释的

历史字符而终止交易。因此，是否使用历史字符是发卡机构所决定的，发卡机构有责任意识到使用了历史字符，可能造成的潜在冲突，应谨慎地使用历史字符。

表17　T0 的基本响应编码

	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

8.4.4　TA1 到 TC3－接口字符

8.4.4.1　概述

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和N以及GB/T 16649.3—2006中定义的T=1协议适用的参数IFSC、块等待时间整数（BWI）及字符等待时间整数（CWI）的值。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。

8.4.4.2　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7.2。

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，终端应接收 ATR，且应立即采用指明的 F 和 D 值（F=372，D=1，2，4）；

——如果 TA1 的值不在‘11’到‘13’之间，终端应拒绝 ATR，除非他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），终端应接收ATR且继续在后续信息交换过程中使用缺省值D=1和F=372，除非他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。

某些早期版本的国际终端，可能拒绝TA1存在且其值不为‘11’的ATR。而在本部分中，TA1的值为‘12’和‘13’是被允许的。因此，为了确保支持高速率的卡片能够获得更好的兼容性，宜将指明支持高速率的TA1的值仅放置在冷复位的ATR中，并且在热复位的ATR中不包含TA1或包含TA1的值为‘11’。

8.4.4.3　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中应包含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，终端应能够接收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’）；此时终端应当作TB1=‘00’，继续后续操作。终端不提供编程电压VPP。

终端可保持VPP为静止状态 （见5.4.4）。

字符TB1的基本响应编码见表18。

表18 TB1 的基本响应编码

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

8.4.4.4 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。TC1=‘FF’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。

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9.3.3.1和9.3.5.6.3。

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，额外保护时间应在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卡应回送‘00’到‘FF’之间的TC1值。

终端要求：终端应能够接收不包含TC1的ATR（只要T0的b7置为‘0’），如果接收了这样的ATR，则他应继续卡片操作过程，就像回送了TC1=‘00’一样。

字符TC1的基本响应编码见表19。

表19 TC1 的基本响应编码

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

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。

8.4.4.5 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，则终端应接受这样的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’。终端应拒绝包含其他TD1值的ATR。

字符TD1的基本响应编码，见表20。

表20　TD1 的基本响应编码（T=1）

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

8.4.4.6　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。

当提供TA2，TA2传输有关特定模式操作的信息：

——b8 表明 IC 卡是否有能力改变他的操作模式。如果 b8 置 0 则表明具有这样的能力，而如果 b8 置 1 则表明不具有这样的能力；

——b7-b6 预留（设置为 00）；

——b5 表明在复位应答后是按接口字节提供的传输参数进行，还是按终端默认的传输参数进行。如果 b5 置 0，则按照接口字节定义的传输参数进行；如果 b5 置 1，则按照终端默认的传输参数进行；

——b4-b1 表明特定模式下所采用的协议。

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：TA2的低半字节表明的协议类型正是ATR中第一次表明的协议类型，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。

8.4.4.7　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，他将取代TB1中回送的PI1的值。

基本响应：IC卡不回送TB2。

终端要求：终端应拒绝包含TB2的ATR。

注：终端可以保持VPP为静止状态（见5.4.4）。

8.4.4.8　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。

要求终端应：

——拒绝包含 TC2=‘00’的 ATR；

——接受包含 TC2=‘0A’的 ATR；

——拒绝 TC2 为其他任何值的 ATR，除非他可以支持。

8.4.4.9　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卡回送其他的TD2值。

字符TD2的基本响应编码见表21。

表21　TD2 的基本响应编码（T=1）

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

8.4.4.10　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’预留（RFU）。

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，见表22。

表22　TA3 的基本响应编码

	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								

8.4.4.11　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卡回送低半字节取值为‘0’到‘5’且高半字节取值为‘0’到‘4’的TB3。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，见表23。

表23　TB3 的基本响应编码

	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								

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}≤（N+1）的TB3。终端应接受包含其他TB3值的ATR。

N为TC1中指定的额外保护时间。若TC1＝255，N的值应置为–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。

8.4.4.12 TC3

TC3（如果TD2中指明T=1）指明了所用的块错误校验码的类型，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：终端应能够接受包括TC3=‘00’的ATR，拒绝TC3为其他任何值的ATR。

8.4.5 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。而在其他情况下，IC卡应回送TCK。

终端要求：当TCK正确返回时，终端应能校验他。如果仅选择T=0协议，终端应能够接受不包含TCK的ATR。其他情况下，终端应拒绝不包含TCK或TCK不正确的ATR。

8.5 复位应答过程中终端的行为

IC卡的触点如6.2.3所描述的那样激活之后，终端应启动一个如6.2.4.1所定义的冷复位，然后执行以下步骤：

——如果终端如 8.4 的描述拒绝 IC 卡，则他应在 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 8.3 的描述拒绝接受冷复位应答，则他不应立即终止卡片操作过程，而应在冷复位的 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，直到接收完 TO 字符，终端才能启动热复位；

——如果终端如 8.4 的描述拒绝热复位应答，则他应在热复位的 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；

——终端应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；

——终端应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，则终端应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；

——终端应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，则终端应在 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，则他应在 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，终端应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，终端应从有效 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）。

8.6 复位应答－终端流程

图11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8章规定的实例。

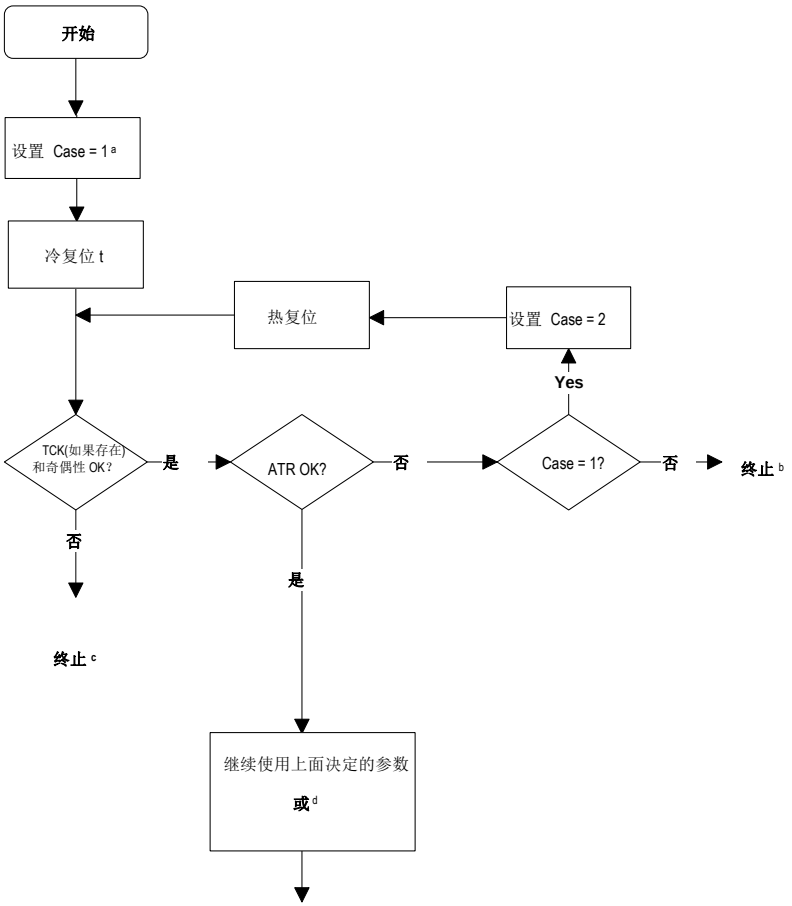

图11 ATR－终端上的流程图

注：

[a]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。

[b]如果过程在此处结束，则IC卡可能根据商业协议被此终端接受。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JR/T 0025—2018之列。

[c]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。

[d]JR/T 0025—2018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。

9 传输协议

9.1 概述

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卡应支持T=0协议或T=1协议。终端应支持两种协议。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中提供的其他参数和与特定协议相关的参数将在本章相应的部分定义。

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。

9.2 物理层

T=0与T=1协议均使用了物理层和第7章定义的字符帧。

9.3 数据链路层

9.3.1 概述

本条描述了传输协议T=0和T=1的时序、具体选项和错误处理。

9.3.2 字符帧

在7.3中定义的字符帧适用于IC卡与终端之间所有的报文交换。

9.3.3 字符协议 T=0

9.3.3.1 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8.3和8.4）。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卡应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+Netu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。终端应能够正确解释从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×D×WI个etu。（D和WI分别在TA1和TC2中返回。）

终端应能够正确解释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×480）etu的字符。如果没有接收到字符，终端应在发生超时的字符起始位下降沿开始的WWT+（D×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卡或终端应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15个etu以内接收到的字符。此处的时序不适用于重发字符。

9.3.3.2 命令头

命令均由终端应用层（TAL）发出，他用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协议，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9.4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。

9.3.3.3 命令处理

9.3.3.3.1 概述

IC卡收到命令头以后向TTL回传过程字或状态字SW1SW2（以后简称“状态字”）。TTL和IC卡在二者之间的命令和数据交换的任何时刻都应知道数据流的方向和I/O线路由谁驱动。

9.3.3.3.2 过程字

过程字向TTL表明他应执行的动作。其编码与TTL动作的对应关系，见表24。

表24 终端对过程字的响应

过程字节值	动作
与 INS 字节值相同	所有余下的数据将由 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 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 应等待另一个过程字然后再以最大长度‘xx’向 IC 卡发送取应答（GET RESPONSE）命令头，其中‘xx’是第二个过程字的值。
‘6C’	TTL 应等待另一个过程字然后再以最大长度‘xx’向 IC 卡立即重发命令头，其中‘xx’是第二个过程字的值。

在任何情况下，完成指定的动作后，TTL应等待下一个过程字或状态字。

9.3.3.3.3 状态字

状态字向TTL表明IC卡对命令的处理已经完成。状态字的意义与处理的命令有关。表25显示了TTL应采取的动作和第一个状态字的对应关系。

表25 状态字编码

第一个状态字的值	动作
‘6x’或‘9x’（除‘60’、‘61’和‘6C’）－状态字 SW1	TTL 应等待另一个状态字（状态字 SW2）

接收到第二个状态字后，TTL应在R-APDU中向TAL回送状态字（及其他数据－见9.4.2），然后等待下一个C-APDU。

9.3.3.4 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（9.4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（9.4中情况1和4）的C-APDU将通过9.4定义的T=0的C-TPDU传输规则进行传输。

9.3.4 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，接收方应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。

发送方应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。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，终端应在接收到最后一个无效字符的起始位的下降沿开始的（Dx960）个etu内启动下电时序（如果他是接收方）；或者在IC卡显示有校验错开始的（Dx960）个etu内启动下电时序（如果他是发送方）。

图12显示了字符重发的时序。

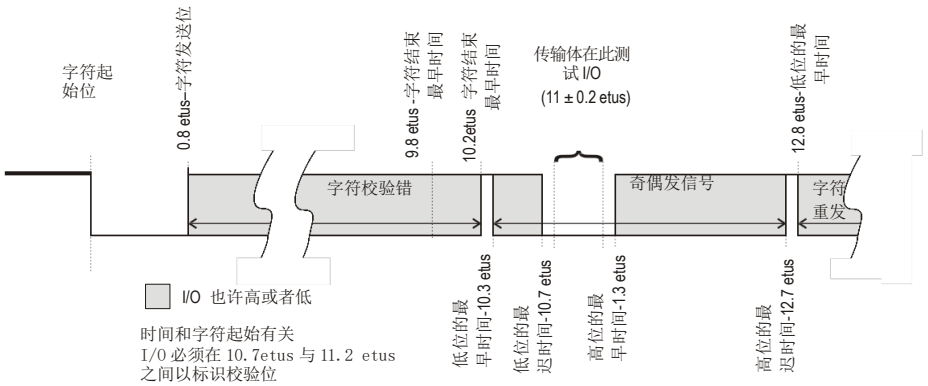

图12　字符重发时序

在等待过程字或状态字时，如果IC卡返回的字节的值未在9.3.3.3.2和9.3.3.3.3中定义，则终端应在接收到的（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。

9.3.5　块传输协议 T=1

9.3.5.1　概述

T=1协议在TAL和IC卡之间传送C-APDU/R-APDU和传输控制信息（如确认信息）的块。

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）。

9.3.5.2　块帧结构

9.3.5.2.1　概述

字符帧采用7.3中的定义。

块帧结构见表26。

表26　块帧结构

头域（M）			信息域（O）	尾域（M）
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

9.3.5.2.2　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。

9.3.5.2.2.1　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[3)]不用，应设定为0。

JR/T 0025—2018不支持节点寻址。终端在ATR之后发送的块及其后终端和IC卡发送的块应把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，应使用9.3.6中描述的错误检测和纠错技术。

9.3.5.2.2.2　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）的接收准备块（R 块）；

——用于交换控制信息的管理块（S 块）。

3)　GB/T 16649 定义为 VPP 控制。0 值表示 VPP 应维持在静止状态。

PCB的编码取决于其类型，见表27、表28和表29。

表27 I 块的 PCB 编码

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

表28 R 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 其他值预留（RFU）

表29 S 块的 PCB 编码

b8	1
b7	1
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 其他值预留（RFU）
注：b5-b1 取值为 4 时表明 VPP 错误，符合 JR/T 0025—2018 要求的 IC 卡和终端未使用。	

9.3.5.2.2.3 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：JR/T 0025—2018不支持LEN=0的I块。

9.3.5.3 信息域

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

9.3.5.4 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。JR/T 0025—2018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_i（i>2）指明要使用的错误校验码类型，IC卡在ATR中并不回送。因此，LCR的正常缺省状态可用作EDC。

9.3.5.5 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。

9.3.5.6 具体选项

9.3.5.6.1 概述

本条定义了用于T=1传输协议的信息域的大小和时序。

9.3.5.6.2 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应为254字节，此值应在随后的整个卡片操作过程中使用。

9.3.5.6.3 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小时间间隔为11到42个etu，由复位应答回送的TC1值决定（见8.3和8.4）。如果TC1返回的值是N，IC卡应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小时间间隔应为11个etu。终端应能够正确解释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8.3.3.10中规定，取值为0～5，所以CWT的取值范围是12到43个etu。接收方应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时间间隔为（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}×960）+11}个etu。在8.3.3.10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。

终端应能够正确解释IC卡在BWT+（Dx960）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）应为22etu。IC卡或终端应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21个etu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：

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

9.3.5.7 无错操作

协议规则的无错操作如下：

——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）；

——IC 卡应向终端返回 S 块（IFS 应答），确认 IFSD 的改变。S 块（IFS 应答）的 PCB 值应为‘E1’，INF 域应和请求块相同；

——若 IC 卡希望改变在复位应答后指定的 IFSC 的大小，则应向终端发送一个 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’。终端应向 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；

——在卡片操作过程中，只有本条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；

——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；

——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）；

——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，则发送方即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 块序列号应是 0；

——接收到 R 块后，应验证 b5。接收方不必验证 PCB 的 b4-b1。对 b4-b1 的可选验证不能与 JR/T 0025—2018 的规定冲突；

——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；

——若 IC 卡需要比 BWT 更长的时间来处理已收到的 I 块，则应发送一个等待时间延迟请求 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。终端应发送一个 INF 中具有相同值的等待时间延迟请求 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，并且只在本次示例中替换 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，IC 卡仍然使用原来的 BWT 作为允许的时间来处理 I 块；

——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9.3.6中描述的过程。

9.3.5.8 链接

9.3.5.8.1 概述

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9.3.5.2中的规定，包含b6=1的任何I块都应由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。

9.3.5.8.2 链接规则

TTL应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，终端应能够接收 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 卡应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 卡应用 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，则应使每个发送 I 块的长度≤IFSD；

——当终端是发送方时，终端应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）；

——在链接过程中，IC 卡不能企图向终端发送 S（IFSC 请求）块而采用新的 IFSC 值。

9.3.5.8.3 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9.4.3）。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字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。

9.3.6 T=1 协议的错误检测和纠错

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，在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卡应重发块，以恢复错误。如果重发块，则重发的块应和原发送块一致。

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，例如奇偶校验/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。

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JR/T 0025—2018定义的规则冲突的动作：

a) 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。

b) 如果接收不到 TTL 发送给 IC 卡的块的应答，终端应：

1) 如果未应答的块为 I 块、R 块或 S（应答）块，终端应根据 9.3.5.5 的规定传送一个带有序列号的 R 块；

或

2) 如果未应答的块为 S（请求）块，终端应重新传送 S（请求）块；

或

3) 启动下电时序。

以上动作应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×960）}个 etu 到{BWT+（D×4800）}个 etu 之间完成。如果使用了等待时间延迟，则应在{WTX+（n×D×960）}个 etu 到{WTX+（n×D×4800）}个 etu 内完成。

c) 如果终端在接收块的过程中没有收到期望的字符，终端应：

1) 如果未应答的块为 I 块、R 块或 S（应答）块，终端应根据 9.3.5.5 的规定传送一个带有序列号的 R 块；

或

2) 如果未应答的块为 S（请求）块，终端应重新传送 S（请求）块；

或

3) 启动下电时序。

以上动作应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。

d) 如果在 I 块的应答中收到了非法块，发送方应按 9.3.5.5 的规定传送带有序列号的 R 块。

e) 如果在 R 块的应答中收到了非法块，发送方应重发 R 块。

f) 如果响应 S（...请求）块的 S（...响应）块没有收到，发送方应重发一个 S（...请求）块。

g) 如果响应S（…响应）块的应答中收到无效块，发送方应按9.3.5.5的规定传送带有序列号的R块。

h) 如果TTL连续发送三个任何块，而没有得到有效的响应，则TTL应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×14,400）}个etu内启动下电时序。

注：JR/T 0025—2018中不要求再同步。如果终端需要支持再同步，他可以通过发送一个S（再同步）块，相关操作在GB/T 16649.3—2006中定义。

如果IC卡最多连续发送两次而没有收到有效应答，则他应保持在接收状态。

i) 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应在S（放弃请求）块的最后一个字节的起始位下降沿开始的（D×9,600）个etu内启动下电时序。

注：JR/T 0025—2018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，他可以发出一个S（放弃请求）块。但要注意，如接收方不支持终止功能时，他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，则他可以回送一个S（放弃响应）块，而不是主动结束卡片操作过程。

9.4 终端传输层

9.4.1 概述

本条描述了在终端和IC卡之间传输C-APDU/R-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9.5中定义的命令的四种格式。C-APDU和R-APDU的组成将在9.5.2和9.5.3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）和状态字回送给TTL。

9.4.2 T=0 协议下 APDU 的传送

9.4.2.1 概述

本条描述了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。

9.4.2.2 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）和状态字映射到R-APDU的形式取决于回送数据的长度。

由IC卡回送的过程字SW1 SW2=“61xx”和SW1 SW2=“6Cxx”用来控制IC卡和TTL之间的数据交换，他不会回送给TAL。过程字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卡的其他过程字。这些功能不在JR/T 0025—2018定义的范围之内。

如果IC卡回送给TTL的状态字是SW1 SW2=“9000”，则表示正常完成了命令的处理。TTL在接收到任何其他的状态（不包括过程字“61xx”和“6Cxx”）时，都应中断命令的处理（例如向TAL传送R-APDU，等待来自TAL的C-APDU）。（当在情况4时，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（“9xxx”除“9000”外），则TTL应继续处理命令。）

以下描述的是将IC卡回送的数据和状态字映射到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“61xx”和“6Cxx”的控制下已被IC卡返回的情况。INS、$\overline{INS}$和‘60’过程字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，IC卡在接收到GET RESPONSE命令后返回的任何状态字和GET RESPONSE命令相关，而与他要完成的情况2或情况4的命令无关。

9.4.2.2.1 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：

a) TTL 发送 T=0 的命令头到 IC 卡；

b) IC 卡收到命令头后，无论正常或非正常处理，IC 卡都应向 TTL 回送状态字；

（IC 卡应分析 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。）

c) 收到来自 IC 卡的状态字以后，TTL 应中止该命令的处理。

TTL和IC卡交换的具体细节参见附录A.1。

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

9.4.2.2.2 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 RECORED）命令和按JR/T 0025—2018发出的所有情况2的命令的Le都应为‘00’。

交换流程如下：

a) TTL 发送 T=0 的命令头到 IC 卡；

b) IC 卡收到命令头以后：

1) 正常处理以后应向 TTL 返回数据和状态。IC 卡应用状态字‘6Cxx’（如果需要，亦可用‘61xx’）控制返回的数据；

或

2) 在非正常处理后仅向 TTL 返回状态。

c) 接收到来自 IC 卡的数据（如果存在）和状态之后，TTL 应中止该命令的处理。

TTL和IC卡的交换细节，包括过程字“61xx”和“6Cxx”的使用，参见附录A.2。

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。

9.4.2.2.3 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：

a) TTL 发送 T=0 的命令头到 IC 卡；

b) 收到命令头后，如果 IC 卡：

1) 回送一个过程字，则 TTL 应在此过程字的控制下向 IC 卡发送 C-APDU 条件体的部分数据；

或

2) 如果 IC 卡回送状态字，TTL 应中止命令处理过程。

c） 如果处理过程没有在步骤 b（2）中断，则 IC 卡应在接收到 C-APDU 的条件体之后返回命令处理结束后的状态；

d） 收到来自 IC 卡的状态字之后，TTL 应中止该命令的执行。

TTL和IC卡之间的交换细节参见附录A.3。

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。

9.4.2.2.4 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JR/T 0025—2018规定的所有情况4命令的Le都应为‘00’。

交换流程如下：

a） TTL 发送 T=0 命令头到 IC 卡。

b） 接收到命令头以后，IC 卡应：

1） 返回一个过程字，TTL 应在此过程字的控制下向 IC 卡发送 C-APDU 条件体的数据部分；

或

2） 如果 IC 卡回送状态字，TTL 将中止命令处理过程。

c） 如果处理过程在 b）的 2）中没有中止，IC 卡在接收到 C-APDU 的条件体之后应：

1） 在正常处理下，回送过程字‘61xx’给 TTL，请求 TTL 发出取应答（GET RESPONSE）命令从 IC 卡取回数据；

或

2） 在非正常处理下，只向 TTL 返回状态。

d） 收到 c）返回的过程字或状态后，如果 IC 卡：

1） 返回 c）的 1）中的“61xx”过程字，TTL 应向 IC 卡发送 P3 小于或等于过程字‘61xx’中的‘xx’的取应答（GET RESPONSE）命令头；

或

2） 返回 c）的 2）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 应发送 Le=‘00’的取应答（GET RESPONSE）命令；

或

3） 返回 c）的 2）中出现的但未在 d（2）中描述的状态，TTL 应中止命令的处理。

e） 如果 d）的 3）中没有中止处理，则应按照 9.4.2.2.2 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“61xx”和“6Cxx”的使用，参见附录 A.4。

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。若无返回数据，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。

9.4.2.3 过程字“61xx”和“6Cxx“的使用

9.4.2.3.1 概述

由IC卡回送到TTL的过程字“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，这些过程字仅仅用在命令情况2和4中。

过程字“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“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的规定如下。发生错误时，IC卡回送错误或警告状态字而不是“61xx”或“6Cxx”。

9.4.2.3.2 情况 2 命令

a) 如果 IC 卡收到一个情况 2 的命令头并且 Le=‘00’或 Le>Licc，则他应返回
   1) 过程字“6C Licc”，要求 TTL 以 P3=Licc 立即重发命令头；
   或
   2) 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，则他应按以下Le=Licc的规则处理。

b) 如果 IC 卡收到情况 2 的命令头并且 Le=Licc，他应
   1) 在 INS、$\overline{INS}$ 或‘60’及相关过程字的控制下返回长度为 Le（=Licc）的数据；
   或
   2) 返回状态字“61xx”，要求 TTL 发出最大长度为“xx”的取应答命令；
   或
   3) 返回表明警告或错误条件的状态（SW1 SW2=“9000”除外）。

c) 如果 IC 卡收到情况 2 的命令头并且 Le<Licc，他应
   1) 返回过程字“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
   2) 返回过程字“6C Licc”要求 TTL 以 P3=Licc 立即重发命令头；
   或
   3) 返回表明警告或错误条件的状态（SW1 SW2=“9000”除外）。

   注：c）的2）不是IC卡对取应答命令的合法应答。

9.4.2.3.3 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，他应：

a) 返回过程字“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字（SW1 SW2=“9000”除外）。

此时发出的取应答命令的处理方法见 9.4.2.3.2 对情况 2 命令中的描述。

9.4.2.4 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，见表30。

表30 命令报文结构

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卡回送状态字SW1 SW2=“9000”和Licc字节的数据。

在错误情况发生时，错误状态字（SW1 SW2）的编码，见表31。

表31 取应答错误响应

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

9.4.3 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）和状态字。如果IC卡返回表明正常处理（“9000”）、一个警告（“62xx”或“63xx”），与应用相关（“9xxx”）状态字，则他应同时返回与命令处理相关的数据（如果有）。其他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。

如果终端发送的APDU中Le=0，而命令执行后IC卡返回状态字为“0x9000”或者“0x61La”时，则都认为该命令得到成功执行，且状态字均为“0x9000”。

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

9.5 应用层

9.5.1 概述

应用协议由TAL和TTL之间一组有序的数据交换组成，本条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32。

表32 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，因此仅适用于命令情况3和情况4。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。		

9.5.2 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：完成 INS 的参数字节。

注：每一个命令头的完整定义将在第11章中描述。

条件体包括如下定义的字节串：

——Lc 占一个字节，定义了在 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第11章中描述。

可能的C-APDU结构的四种情况，见表33。

表33 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

9.5.3 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字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。

必备的状态字表明IC卡在处理完命令后的状态。

SW1 SW2的编码在第11章规定。

10 文件

10.1 概述

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，他是可以用名称、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），则应终止卡片操作过程。

表B.1定义了可能在应用选择中使用到的数据元。未在表B.1中定义的用于应用选择的数据元不在JR/T 0025—2018的范围之内。

10.2 文件结构

10.2.1 概述

JR/T 0025—2018中的文件组织结构来自且符合GB/T 16649.4的基本组织结构。

本部分描述了符合JR/T 0025—2018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定义文件（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。

10.2.2 应用定义文件（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，见表43。

10.2.3 应用基本文件（AEF）

AEF所使用的结构是应用相关的。JR/T 0025.4—2018中描述了借记/贷记应用的文件结构。

10.2.4 文件到 GB/T 16649.4—2010 的文件结构的映射

使用下列到GB/T 16649.4—2010的映射：

——一个 GB/T 16649.4—2010 定义的专用文件（DF）映射为一个 ADF 或一个 DDF。可以通过他来访问基本文件和 DF。在卡片中处于最高层的 DF 称为主文件（MF）；

——GB/T 16649.4—2010 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JR/T 0025—2018中，如果嵌入了DF，对与之相连的EF的访问是透明的。

10.2.5 目录结构

当存在12.2.2中描述的支付系统环境（PSE）时，IC卡应为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，所有应用在支付系统目录文件（DIR文件）中列出，支付系统目录文件的位置由PSE的FCI指出。

目录结构允许以应用标识符（AID）检索一个应用。

在选择PSE的响应报文中应有DIR文件存在的编码[见选择（SELECT）命令]。

根据GB/T 16649.4—2010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：

——第 12 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 JR/T 0025—2018 的范围内定义。

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。

10.3 文件引用

10.3.1 概述

根据其类型，文件可以通过文件名或SFI引用。

10.3.2 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名应唯一。

10.3.3 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他的命令中进行描述。在一个应用中SFI应是唯一的。

11 命令

11.1 报文结构

11.1.1 概述

报文根据ATR所选择的传输协议（见第9章）在终端和卡片之间传输。终端和卡片应按本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。他包括向卡片发送命令、卡片内处理命令和返回IC卡处理响应等步骤。本部分和后续部分定义的所有命令和响应都定义在应用层。

应用层发出的命令报文和卡片回送到应用层的响应报文统称为应用协议数据单元（APDU）。响应是和命令相对应的，通常被称为APDU命令-响应对。在一个APDU命令-响应对中，命令报文或响应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-响应对的结构，这些结构是JR/T 0025—2018所定义的应用层所必需的。其他所有的命令由特定的应用来实现，但是也应遵循此处定义的APDU结构（格式）。

11.1.2 C-APDU 格式

C-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13。

CLA	INS	P1	P2	Lc	Data	Le
←必备头→				←条件体→		

图13 命令 APDU 结构

C-APDU中发送的数据长度用Lc（命令数据域的长度）表示。

R-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）命令以及第9章所给出的所有情况2和情况4命令中，Le应等于‘00’。

C-APDU报文的内容见表34。

表34 命令 APDU 内容

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	响应数据域中期望的最大数据字节数	0或1

C-APDU结构的不同类别在第9章中描述。

11.1.3 R-APDU 格式

R-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14。

Data	SW1	SW2
条件体	←必备尾→	

图14 响应 APDU 结构

当使用T=1协议时，对于所有Le=‘00’的命令，状态字SW1 SW2=“90 00”或“61 La”均表示命令的成功执行。但由于可读性的需要，这两种状态字只用了“90 00”作为参考。

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

响应结尾的2个字节代码是命令的处理状态，他们通过传输层回送。R-APDU的内容，见表35。

表35 响应 APDU 内容

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

11.1.4 C-APDU/R-APDU 约定

在一个APDU命令-响应对中，命令报文和响应报文都可能包含数据，4类命令的数据包含情况，见表36。

表36 命令-响应对 APDU 的数据

类别	命令数据	响应数据
1	不存在	不存在
2	不存在	存在
3	存在	不存在
4	存在	存在

这4类命令使用本部分所描述的传输协议进行处理。

11.2 读记录 C-APDU/R-APDU

11.2.1 定义和范围

读记录命令用于读取线性文件中的记录。

IC卡的响应由回送记录组成。

11.2.2 命令报文

读记录命令报文编码，见表37。

表37 读记录命令报文

代码	值
CLA	‘00’
INS	‘B2’
P1	记录号
P2	引用控制参数（见表38）
Lc	不存在
Data	不存在
Le	‘00’

表38定义了命令报文的引用控制参数。

表38 读记录命令引用控制参数

b8	b7	b6	b5	b4	B3	b2	b1	含义
X	X	X	X	X				SFI
					1	0	0	P1为记录号

11.2.3 命令报文数据域

命令报文数据域不存在。

11.2.4 响应报文数据域

执行成功的读记录命令的响应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12.2.3定义）。应用处理中读取的记录格式与应用有关。

11.2.5 响应报文状态字

此命令执行成功的状态字是“9000”。

11.3 选择 C-APDU/R-APDU

11.3.1 定义和范围

选择命令通过文件名或AID来选择IC卡中的PSE或ADF。应用选择在第12章中描述。
成功执行该命令设定PSE或ADF的路径。后续命令作用于与用SFI选定的PSE或ADF相联系的AEF。
从IC卡返回的响应报文包含回送FCI。

11.3.2 命令报文

选择命令报文编码，见表39。

表39 SELECT 命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数（见表40）
P2	选择选项（见表41）
Lc	‘05’-‘10’
Data	文件名
Le	‘00’

表40定义了选择（SELECT）命令报文的引用控制参数。

表40 SELECT 命令引用控制参数

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41定义了选择（SELECT）命令报文的选择选项P2：

表41 选择（SELECT）命令的可选参数

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

11.3.3 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。

11.3.4 响应报文数据域

响应报文中数据域应包括所选择的PSE或ADF的FCI。表42和表43定义了JR/T 0025—2018所应用的标识。在选择命令的响应报文回送的FCI模板中，除了“BF0C”模板中包含的数据元之外，不应有附加数据元。

表42定义了成功选择PSE后回送的FCI。

表42 选择 PSE 的响应报文（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’ （根据附录 B 建立的标签）	来自从应用提供商、发卡行或 IC 卡供应商或 JR/T 0025—2018 定义的专属于’BF0C’标签的 1 个或多个附加（专用）数据元。	O

表43定义了成功选择ADF后回送的FCI。

表43　选择 ADF 的响应报文（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	M
		‘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’ （根据附录 B 建立的标识符）	来自从应用提供商、发卡行或 IC 卡供应商或 11.3.4 中表 42 的 1 个或多个附加（专用）数据元。	O

注：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。

11.3.5　响应报文状态字

此命令执行成功的状态字是“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，那么他应遵守下列规则：

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（见表41）及使用相同的部分DF名时，卡片应选中与部分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，应得到没有文件被选择的结果，卡片应响应SW1SW2=“6A82”（文件未找到）。

12　应用选择

12.1　应用选择概述

应用选择是触点激活/卡片复位之后、在第一个应用功能之前执行的处理过程。如果紧接在卡片操作之前或之后执行了专有的处理操作（包括任何专有的应用选择方式），那么不需要在两个操作之间拔出/重新插入卡片。如果专有的处理操作发生在卡片操作之前，卡片触点需在开始卡片操作前被释放。

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卡和终端可支持应用隐含选择，但由于在交互环境中并不有用，所以不推荐IC卡和终端使用GB/T 16649中定义的隐含选择。如果使用了隐含选择，他应在卡片操作过程（在6.2.2中定义）之外执行。

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：

——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 12.3 中描述；

——在步骤 1 生成的候选列表中选择一个将要运行的应用。这个过程在 12.3.5 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种终端选择算法。其他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GB/T 16649.4—2010（见12.2.1）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 JR/T 0025—2018 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、服务级别或不同账户）；

——尽可能使符合 JR/T 0025—2018 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卡响应取处理选项命令（GET PROCESSING OPTIONS）而返回的AFL所定义。

12.2 用于应用选择的 IC 卡数据

12.2.1 支付系统应用标识符编码

应用标识符（AID）的结构符合GB/T 16649.5—2002，包括两个部分：

——注册的应用提供商标识（RID）（长度为 5 字节），唯一地标识应用提供商，并根据 GB/T 16649.5—2002 分配；

——最长为 11 字节的可选域，由应用提供商定义。这个域被称为“扩展的专用应用标识符（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卡上允许存在其他应用提供商的应用定义文件（ADF），但是其RID的定义应避免与分配给支付系统的RID的范围发生重复。可遵照GB/T 16649.5—2002的规定定义RID，以确保其编码不发生冲突。

12.2.2 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JR/T 0025—2018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。该DDF应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11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。如果这些数据项中的任一个出现在一个位置而不是另一个，那么终端应使用出现的这个数据元。如果他们在这两个位置都出现，但值不同，终端可以使用两个位置中任一处的值[4)]。

PSE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JR/T 0025—2018，但其入口地址格式是符合JR/T 0025—2018定义的。

不要求该目录包含卡上所有的ADF的入口地址。如果PSE存在，只有从初始目录开始能够找到的应用，才具备国际互通性。

包含PSE的IC卡的内部逻辑结构示例参见附录C。

12.2.3 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。目录可以使用第11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，见表44。

表44 支付系统目录记录格式

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）	……	标识符 ‘61’	目录入口n长度	目录入口n （ADF）

支付系统目录记录中应不包含任何通往DDF的入口。如果终端在处理这些记录时遇到了DDF的入口，终端可以忽略这些入口或者处理这些入口，处理入口的方法不在JR/T 0025—2018的讨论范围内。

支付系统目录中的每一个入口都是一个应用模板（标签‘61’），他包含表45所示的信息。除了在模板‘73’中包含的数据元，任何附加数据元都不能在支付系统目录记录（标签‘70’）中出现。

由于终端不支持任何发卡行特定操作而未预期的或不能解释的，在支付系统目录记录中出现的模板‘61’或‘73’数据元，都应被忽略。

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他在目录入口中出现但是没有在表45中列出的数据对象都应被忽略。

4) 当终端使用12.3.3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12.3.4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，这些值应相同。

表45 ADF 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[8]
	‘XXXX’（根据附录 B 建立的标识符）	变长	应用提供商、发行商或 IC 卡供应商、或 JR/T 0025—2018 定义的专属于模板‘73’的标签增加的 1 个或多个附加（专用）数据元。	O

应用优先权标识符格式见表46。

表46 应用优先权标识符格式

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
	‘XXX’		预留
		0000	未指定优先权
		‘XXXX’（0000 除外）	应用的排列或选择顺序，从 1-15，其中最高优先权为 1

12.2.4 FCI 响应数据错误处理

应用标签、应用优先名称、发卡行代码表索引和首选语言这些数据元是为了持卡人的方便而给出的，不是应用选择成功处理的关键数据元。如果在FCI中给出了这些数据元，发卡行将负责他们的正确编码。

终端无需支持这些数据元的正确格式。如果应用优先名称或应用标签中包含了某一无效的格式定义的字符，那么如果终端能显示出这个字符，终端应显示这个字符；如果终端不能显示这个无效字符，终端应忽略该字符或以空格或其他相近字符代替。另外，如果终端检测到这些数据元中任意一个数据元的格式错误，终端应忽略这些错误，就如卡片响应中未包含这些数据元一样。更重要的是，终端不应终止卡片操作，而应继续进行应用选择。

如果终端不能识别“发卡行代码表索引”或“首选语言”的代码，他应将该数据元视为不存在。

12.3 建立候选列表

12.3.1 概述

终端应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。本条描述了两种应用选择过程。如果卡内不存在PSE，则应遵循12.3.4所描述的过程。

需要注意的是终端可以通过本条没有描述的其他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。

12.3.2 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卡应满足以下要求：

——IC 卡应支持第 11 章所描述的部分名称选择[见选择（SELECT）命令]；

——IC 卡上所有匹配的 AID 应在扩展的专用应用标识符（PIX）中加入唯一的数据标识来区别。IC 卡 AID 中应没有一个和终端的 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。

12.3.3 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，他应遵循本条所描述的过程来确定卡所支持的应用。图15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（见第11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字SW1 SW2 =“6A81”），终端应中断选择过程。

如果IC卡上没有PSE，那么IC卡应对PSE的选择（SELECT）命令回送状态字“6A82”（文件没有找到）。在这种情况下，终端应使用12.3.4所描述的使用应用列表的方式。

如果PSE被锁定，IC卡应回送状态字“6283”。在这种情况下，终端应使用12.3.4所描述的使用应用列表的方式。

如果IC卡回送状态字SW1 SW2 =“9000”，终端则转入步骤2。

如果卡回送其他状态字SW1 SW2，终端应使用12.3.4所描述的使用应用列表的方式。

如果在步骤2到步骤5中出现任何错误（包括SW1 SW2 ≠“90 00”，“6A 83”），终端应清除候选列表并使用12.3.4描述的应用列表方式重新进行应用选择，以寻找匹配的应用。

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，直到卡回送状态字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，卡应回送状态字“6A83”）。如果在执行读记录（READ RECORD）命令查找第1个记录时，卡回送状态字“6A83”，则表示目录入口为空，转到下面的步骤5。

对于目录中的每一条记录，终端从第一个目录入口开始，依次对每个目录入口顺序执行步骤3和步骤4所描述的过程。如果某条记录中不含有目录入口，则终端处理下一条记录。

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（见12.3.2定义），则在应用选择指示器（ASI）（保存在终端中，与该AID对应）的控制下将该应用列入最终应用选择的“候选列表”中。

应用选择指示器（ASI）表明终端的应用标识符应完整匹配（长度和值都相同）还是只需部分匹配卡片中相关的ADF名（标签为‘4F’）。

在下面任一种情况下，该应用将被选入候选列表：

——获得的入口中的 ADF 是完整匹配，或者

——对应终端中该 AID 的应用选择指示器（ASI）表明允许部分名称匹配。

如果得到的ADF入口不是完整匹配，并且终端AID的应用选择指示器表明须要完整匹配时，应用不能被加入候选列表。

4) 当终端处理完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就被确定了，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ADF，终端将继续处理12.3.5所描述的处理过程。

5) 如果步骤1到步骤4中没有发现与终端支持的应用所匹配的目录入口，终端应使用12.3.4所描述的使用应用列表的方式来寻找匹配的应用。

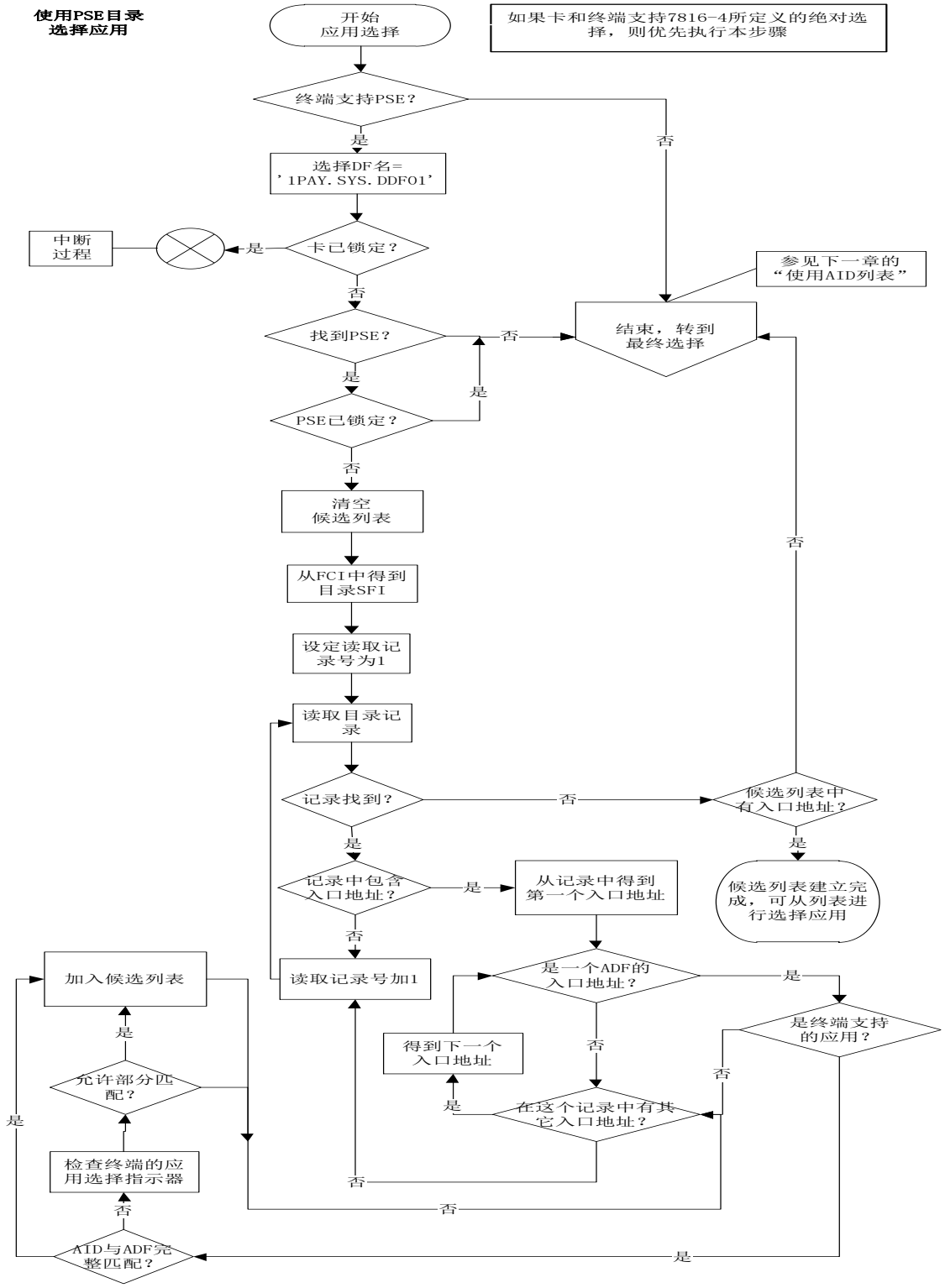

图15　使用目录方法的终端逻辑

12.3.4　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，那么终端应使用他所支持的应用列表的方法建立候选列表。图16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[5)]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卡回送状态字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。如果终端返回其他状态，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[6)]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12.3.5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指示器。终端在选择应用时会检查该指示符。如果指示符表明需要完整匹配（包括长度和名称），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，如果IC卡返回状态字SW1 SW2=“9000”，“62XX”或者“63XX”，然后回到步骤3。如果返回其他状态字，终端转到步骤5。

5） 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。可以见 12.3.2 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。

6） 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应保存。DF 名和应用优先权标识符在任何情况下都可能需要。

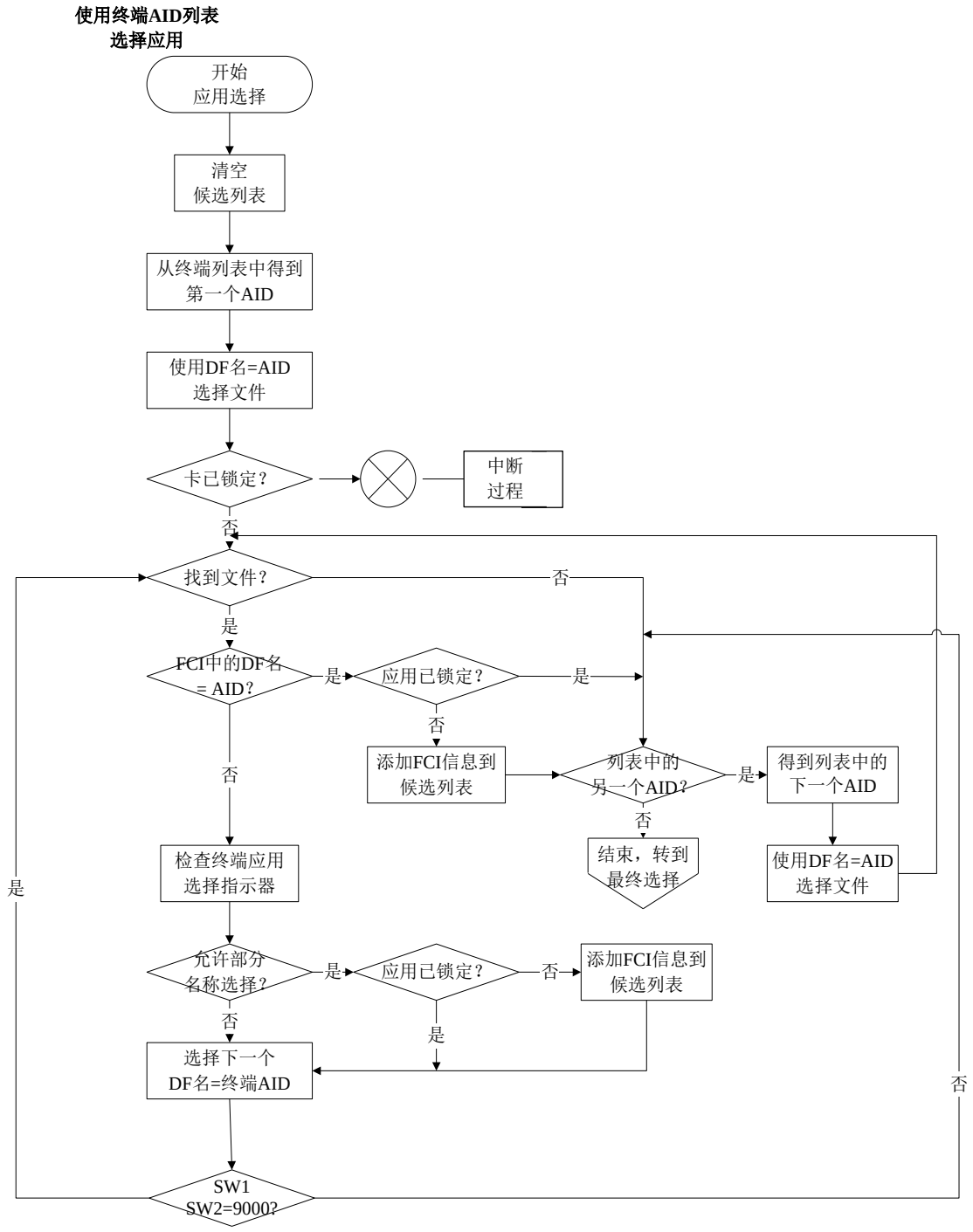

图16　使用终端中的应用列表

12.3.5　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，则如果有应用优先级标识符（API），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，则该列表应按照级别优先的顺序排列，高优先级的应用应在前。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11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字SW1 SW2≠“9000”，或者选择命令的响应中有不同于12.2.所描述的格式错误，则此应用应从候选列表中删除，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他原因被从候选列表中删除，则应用不能在没有持卡人确认的情况下被选中。

在任何情况下，终端应在适当的时候提示持卡人相关动作的完成。

13 AID的预留与使用

13.1 应用标识符（AID）结构与长度

本规范采用GB/T 16649.5—2002规定的应用标识符（AID）基本结构，应用标识符（AID）长度为5-16个字节，由5个字节的注册的应用提供者标识符（RID）和0-11个字节的专有应用标识符扩展（PIX）组成。

应用标识符（AID）唯一标识卡中的应用。由申请机构向金融行业主管部门申请，由管理部门统一组织分配。

应用类型代码的定义见本部分13.4。

13.2 应用提供者标识符（AID）总体编码

依据GB/T16649.5—2002关于AID的规定，应用标识符（AID）编码如表47所示。

表47 应用标识符（AID）编码

应用提供者标识符（RID）	专有应用标识符扩展（PIX）
5个字节	0至11个字节

13.3 专有应用标识符扩展（PIX）编码

具体定义见表48。

应用类型代码应出现，其定义见本部分13.4。

保留位可选出现，若该字段不出现，则其后续字段不应出现。若该字段出现，则该字段取值由发卡机构自行定义。

专有定义标识可选出现，若该字段不出现，则专有定义字节不应出现。若该字段出现，则其定义见表48。

专有定义字节可选出现。

表48　专有应用标识符扩展（PIX）编码

应用类型代码	保留位	专有定义标识	专有定义字节
3 个字节	0-1 个字节 保留给发卡机构	0-1 个字节 00 表示专有定义字节中的内容由本规范保留定义 01-FF 保留	0-6 个字节

13.4　应用类型代码定义

应用类型代码第1字节为00-FE的应用类型代码，保留给本规范使用。其取值的部分定义见表49。

应用类型代码第1字节为FF的应用类型代码，保留给发卡机构使用。

表49　应用类型代码定义

值	定义
01 01 01	借记
01 01 02	贷记
01 01 03	准贷记

附 录 A
（资料性附录）
使用 T=0 协议交换的示例

A.1 情况 1 下的命令

一个形如｛CLA INS P1 P2｝的 C－APDU 从 TAL 传送到 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。

A.2 情况 2 下的命令

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

A.3 情况 3 下的命令

TAL 向 TTL 传递一个形如｛CLA INS P1 P2 Lc [Data（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。

A.4 情况 4 下的命令

TAL 向 TTL 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。

A.5 采用过程字‘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 ≤ xx 时

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

A.6 采用过程字‘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。

A.7 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 ICC

[CLA INS P1 P2 Lc]=>

<=[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一起的返回的数据。

A.8 T=0 协议交换的示例说明

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

——过程字‘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 JR/T 0025—2018 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“61xx”的交换。A7说明了一个情况4的命令的警告条件。

附 录 B
（规范性附录）
数据元表

表B.1定义了可能用于应用选择和他们在数据对象和文件的映射的数据元。

表B.1 数据元字典

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GB/T 16649.4—2010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GB/T 16649.4—2010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（特殊字符仅限于空格）	‘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	‘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
应用选择指示器	对于被终端应用支持的IC卡应用，应用选择指示器指明了终端上相关的AID与卡片上的AID完全相同，包括AID的长度，或者终端上相关的AID与卡上AID的开始部分相同。 终端支持的每个AID仅仅有一个应用选择指示器	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GB/T 16649.4—2010中描述的DF名称	IC卡	b	‘6f’	‘84’	5-16
目录定义文件（DDF）名称	表明与目录相关的DF名称	IC卡	b	‘61’或‘A5’	‘9D’	5-16
目录自定义模板	GB/T 16649. 4的目录的发卡行自定义部分	IC卡	var.	‘61’或‘A5’	‘73’	Var.到252
文件控制信息（FCI）发卡行自定义数据	FCI的发卡行自定义部分	IC卡	var.	‘A5’	‘BF0C’	Var.到222
文件控制信	按照与GB/T 16649.4—2010相关的FCI模板中的	IC卡	var.	‘6f’	‘A5’	Var.

名　称	描述	来源	格式	模板	标签	长度
息（FCI）专有模板	规范来标识数据对象专有的					
文件控制信息（FCI）模板	标识与 GB/T 16649.4—2010 相关的 FCI 模板	IC 卡	var.	-	‘6F’	Var. 到 252
发卡行的代码表格检索	指明了与 GB 15273 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 个字母字符按照 GB/T 4880.1 来表示 注意：以‘5F2D’数据元私有化卡片，该数据元以小写字母编码，而无论该数据元是大写还是小写形式，终端都要认可该数据元。	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 GPO 命令或其他应用特殊的命令中	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
应用模板	包含一个或多个 GB/T 166494 中描述的应用目录入口相关的数据对象	IC 卡	b	’70’	’61’	Var. 到 252
银行标识符代码（BIC）	如 GB/T 16711 中的定义，唯一标识一家银行	IC 卡	var.	‘BF0C’ 或 ‘73’	’5F54’	8 or 11
国际银行账号（IBAN）	如 GB/T 20543—2011 中的定义，唯一标识金融机构中的消费者账号	IC 卡	var.	‘BF0C’ 或 ‘73’	’5F53’	Var. 到 34
发卡行国家代码（alpha2 格式）	如 GB/T 2659 中的定义，标识发卡行国家（使用一个 2 字符的字母编码）	IC 卡	a2	‘BF0C’或‘73’	’5F55’	2
发卡行国家代码（alpha3 格式）	如 GB/T 2659 中的定义，标识发卡行国家（使用一个 3 字符的字母编码）	IC 卡	a2	‘BF0C’或‘73’	’5F56’	3
行业识别码（IIN）	识别主要行业和发卡行的号码，该号码组成了主账号（PAN）的第 1 部分	IC 卡	a6	‘BF0C’或‘73’	’42’	3
发卡行 URL	该 URL 提供了网络上发卡行的库服务器的位置	IC 卡	ans	‘BF0C’ 或 ‘73’	’5F50’	Var.
记录入口	提供交易记录的 SFI	IC 卡	b	‘BF0C’ 或 ‘73’	’9F4D’	2

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见表B.2。

表B.2　数据元标签

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’

附 录 C
（资料性附录）
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C.1是仅有单层目录的单应用卡。在这个示例中，主文件（在GB/T 16649.4—2010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。主文件应按照12.2定义的赋予首层DDF的唯一支付系统名。主文件的FCI应包含SFI数据对象。

本例中的“DIR A”不一定是ISO的DIR文件，但他应遵循JR/T 0025—2018，包括他应包含一个范围为1－10的SFI的要求。

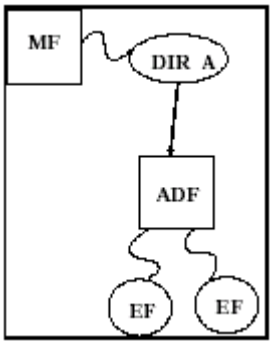

图 C.1 单应用的卡片简单结构

图C.2给出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JR/T 0025—2018的应用，因而对主文件的功能没有限制。根据GB/T 16649.4—2010，可能存在DIR文件，但没有采用第12章中定义的应用选择方法。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JR/T 0025—2018范围之内。

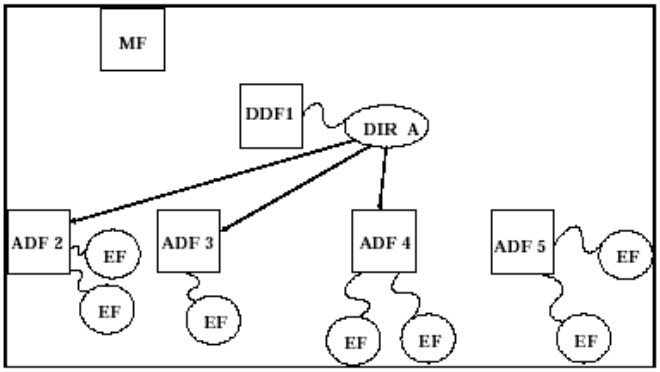

图 C.2 单层目录

参 考 文 献

[1] EMV Integrated Circuit Card Specifications for Payment Systems:
Book 1 Application Independent ICC to Terminal Interface Requirements：Version 4.3
Book 2 Security and Key Management：Version 4.3
Book 3 Application Specification：Version 4.3
Book 4 Cardholder, Attendant, and Acquirer Interface Requirements Version 4.3
[2] Visa Integrated Circuit Card Card Specification：Version 1.4.0
[3] Visa Integrated Circuit Card Application Overview：Version 1.4.0
[4] Visa Integrated Circuit Card Terminal Specification：Version 1.4.0