ICS 35.240.40
A 11
备案号：

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0025.6—201x
代替JR/T 0025.6—2010

中国金融集成电路（IC）卡规范
第6部分：借记/贷记应用终端规范

China financial integrated circuit card specifications—
Part 6:Debit/credit application terminal specification

（送审稿）

201x-xx-xx 发布　　201x-xx-xx 实施

中国人民银行 发布

目　　次

前　言

JR/T 0025《中国金融集成电路（IC）卡规范》分为17个部分：

——第1部分：电子钱包/电子存折应用卡片规范（废止）；

——第2部分：电子钱包/电子存折应用规范（废止）；

——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9部分：电子钱包扩展应用指南（废止）；

——第10部分：借记/贷记应用个人化指南；

——第11部分：非接触式IC卡通讯规范；

——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17部分：借记/贷记应用安全增强规范。

本部分为JR/T 0025的第6部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分从终端角度根据交易流程描述了芯片卡和终端在借记/贷记交易中相关的技术细节。

本部分代替JR/T 0025.6—2010《中国金融集成电路（IC）卡规范　第6部分：借记/贷记终端规范》。

本部分与JR/T 0025.6-2010相比主要变化如下：

——修订了标准的前言；

——删除了第7.2节中终端构建候选应用列表时对DDF的支持；

——在第7.4节中明确了若卡片返回标签重复，终端应当终止交易；

——在第7.4节中明确了终端不应当应为持卡人姓名和/或持卡人姓名扩展有误而终止交易；

——在第7.12节中明确了发卡行脚本的格式和终端的处理方法；

——对原标准在文字描述上的勘误做出修正。

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/TC180）归口。

本部分主要起草单位：中国人民银行、中国工商银行、中国农业银行、中国银行、中国建设银行、中国邮政储蓄银行、上海浦东发展银行、中国银联股份有限公司、中国印钞造币总公司、中国金融电子化公司、银行卡检测中心、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：

本部分所代替标准的历次版本发布情况为：

——JR/T 0025.6—2005；

——JR/T 0025.6—2010。

引　言

本部分为JR/T 0025的第6部分，与JR/T 0025的第4部分、第5部分和第7部分一起构成借记/贷记规范。

中国金融集成电路（IC）卡规范
第6部分：借记/贷记终端规范

1 范围

JR/T 0025的本部分从终端的角度描述了借记/贷记交易流程，包括终端的硬件需求、终端内部的处理细节、终端所使用的数据元、终端所支持的指令集等。

本部分适用于支持JR/T 0025所规定借记/贷记应用的金融终端、销售点终端以及其他类似的终端设备。使用对象主要是与金融IC卡应用相关的终端设计、制造以及应用系统研制、开发、集成和维护的相关部门（单位）。

2 规范性引用文件

下列文件中的条款通过JR/T 0025的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB/T 2659 世界各国和地区名称代码(GB/T 2659—2000，ISO 3166-1:1997，EQV)

GB/T 12406 表示货币和资金的代码(GB/T 12406—2008，ISO 4217:2001，IDT)

GB/T 15150 产生报文的银行卡 交换报文规范 金融交易内容(GB/T 15150—1994,ISO 8583:1987,IDT)

GB/T 16649.5 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(GB/T 16649.5—2002,ISO/IEC 7816-5:1994,NEQ)

GB/T 21078.1 银行业务 个人识别码的管理与安全 第1部分:ATM和POS系统中联机PIN处理的基本原则和要求(GB/T 21078.1—2007,ISO 9564-1:2002,MOD)

JR/T 0001 银行卡销售点（POS）终端规范

JR/T 0025.3 中国金融集成电路（IC）卡规范 第3部分：与应用无关的IC卡与终端接口规范

JR/T 0025.4 中国金融集成电路（IC）卡规范 第4部分：借记/贷记应用规范

JR/T 0025.5 中国金融集成电路（IC）卡规范 第5部分：借记/贷记应用卡片规范

JR/T 0025.7 中国金融集成电路（IC）卡规范 第7部分：借记/贷记应用安全规范

ISO/IEC 8859（所有部分） 信息处理 八位单字节编码图形字符集

3 术语和定义

下列术语和定义适用于本文件。

3.1

应用 application

卡片和终端之间的应用协议和相关的数据集。

3.2

命令 command

终端向IC卡发出的一条报文，该报文启动一个操作或请求一个响应。

3.3

密文 cryptogram

加密运算的结果。

3.4

金融交易 financial transaction

由于持卡者和商户之间的商品或服务交换行为而在持卡者、发卡机构、商户和收单行之间产生的信息交换、资金清算和结算行为。

3.5

集成电路（IC） integrated circuit (IC)

具有处理和/或存储功能的电子器件。

3.6

集成电路卡（IC卡） integrated circuit(s) card (ICC)

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。

3.7

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。

3.8

发卡行行为代码 issuer action code

发卡行根据TVR的内容选择的动作。

3.9

磁条 magstripe

包括磁编码信息的条状物。

3.10

支付系统环境 payment system environment

当符合JR/T 0025的支付系统应用被选择，IC卡中所确立的逻辑条件集合。

3.11

响应 response

IC卡处理完成收到的命令报文后，返回给终端的报文。

3.12

脚本 script

发卡行向终端发送的命令或命令序列，目的是向IC卡连续输入命令。

3.13

终端 terminal

在交易点安装、用于与IC卡配合共同完成金融交易的设备。它应包括接口设备，也可包括其它的部件和接口（如与主机的通讯）。

3.14

终端行为代码 terminal action code

收单行根据TVR的内容选择的动作。

4 符号和缩略语

下列符号和缩略语适用于本文件。

AAC 应用认证密文(Application Authentication Cryptogram)

AC 应用密文(Application Cryptogram)

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)

AIP	应用交互特征(Application Interchange Profile)
ARPC	授权响应密文(Authorization Response Cryptogram)
ARQC	授权请求密文(Authorization Request Cryptogram)
ATC	应用交易计数器(Application Transaction Counter)
ATM	自动柜员机(Automated Teller Machine)
AUC	应用用途控制(Application Usage Control)
BER	基本编码规则(Basic Encoding Rules)
CA	认证中心(Certificate Authority)
CAM	卡片认证方法(Card Authentication Method)
CDA	复合动态数据认证/应用密文生成(Combined DDA/AC Generation)
CDOL	卡片风险管理数据对象列表（Card Rish Management Data Object List）
CID	密文信息数据(Cryptogram Information Data)
cn	压缩数字型(Compressed Numeric)
CVM	持卡人验证方法（Cardholder Verification Method）
CVR	卡片验证结果(Card Verification Results)
DDA	动态数据认证(Dynamic Data Authentication)
DDF	目录定义文件(Directory Definition File)
DDOL	动态数据认证数据对象列表（Dynamic Data Authentication Data Object List）
DF	专用文件(Dedicated File)
DOL	数据对象列表(Data Object List)
EF	基本文件(Elementary File)
EMV	Europay、MasterCard 和 VISA
FCI	文件控制信息(File Control Information)
GPO	获取处理选项（Get Processing Options）
IAC	发卡行行为代码(Issuer Action Code)
IC	集成电路(Integrated Circuit)
M	必备(Mandatory)
n	数字型(Numeric)
O	可选(Optional)
P1	参数 1(Parameter 1)
P2	参数 2(Parameter 2)
PAN	主账号(Primary Account Number)
PIN	个人识别码(Personal Identification Number)
PIX	扩展的专用应用标识符(Proprietary Application Identifier Extension)
PKI	公钥基础设施(Public Key Infrastructure)
RFU	预留(Reserved for Future Use)
RID	注册的应用提供商标识(Registered Application Provider Identifier)
SAD	签名的静态应用数据(Signed Static Application Data)
SDA	静态数据认证(Static Data Authentication)
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)
TAC	终端行为代码(Terminal Action Code)
TC	交易证书(Transaction Certificate)

TDOL　　交易证书数据对象列表(Transaction Certificate Data Object List)
TLV　　标签、长度、值(Tag Length Value)
TSI　　交易状态信息(Transaction Status Information)
TVR　　终端验证结果(Terminal Verification Results)

5　终端硬件需求

5.1　内存

终端应当具有足够的内存容量来存放应用程序、密钥、交易数据和其它参数等，并确保在掉电后这些数据不会丢失。

5.2　磁条阅读器

磁条阅读器应能够准确阅读在磁性标准正常的磁道信息，并可同时读取磁条卡二、三磁道数据。可选支持读取一、二或一、二、三磁道的卡片，并处理相应的磁卡交易。

5.3　IC 卡读卡器

终端应提供用户卡接口的IC卡读卡器，用来接受用户IC卡插入并与IC卡进行命令数据传递通讯。该读卡器模块包括机械、电气和逻辑协议等部分。

建议终端的用户卡IC卡读卡器插槽附近有一明显标记指示如何插入IC卡。如果终端有锁卡或吞卡功能，则应保证在掉电、设备异常或交易取消时能释放或退出卡。

5.4　显示

有服务员的终端必须配置有显示给服务员的显示屏，可选带有显示给持卡人的显示屏。以供监测交易过程、输入数据、设置选项或确认交易数据。终端应支持ISO 8859的基本字符集。建议显示屏应具备中文显示能力。

5.5　打印机

终端配置有能打印交易单据的打印机，根据支付系统要求可以是针式或热敏打印机。对每笔批准的交易，不论是脱机、联机或语音授权都能打印出交易单据。

打印单据格式由各收单行自定，但应包含如下数据：卡号、应用标识符AID、交易日期时间、签名栏。

5.6　时钟

能处理脱机交易的终端应配有时钟模块，用来提供当地日期和时间。

日期用于应用有效期、失效日期以及脱机数据认证中的证书有效期检查。时间也可用于确保交易唯一性识别以及作为应用密文生成算法中的输入数据。

5.7　与后台通信模块

有联机通讯能力的终端应当配置有与收单行主机后台通信的模块。用于向主机发送交易数据包获取授权，或由主机对终端进行管理的功能。根据收单行的要求可采用PSTN Modem拨号、GSM、GPRS、CDMA和TCP/IP等方式。通信模块与收单行主机的通信速度应能满足实时传送IC卡交易数据的要求。

5.8　键盘

终端应带有用于输入交易金额、选择命令和执行功能的按键键盘。支持EMV规范中描述的数字键、字母键、命令键和功能键。命令键的颜色和布局参考EMV规范。如果采用了带颜色的命令键，推荐使用下面的颜色分配。

命令键颜色：确认－绿色；取消－红色；清除－黄色。

5.9　密码键盘

提供输入个人识别码（PIN）验证的终端应配有密码键盘，允许持卡人输入4－12位的PIN。可以是与终端键盘集成在一起的内置式密码键盘，也可以是与终端通过通讯线连接的外置式密码键盘。密码键盘的设计应当符合EMV的要求。

5.10　终端类型

本部分所覆盖的终端类型包括POS终端、自动柜员机（ATM）和自动售货机等，见附录A.1。

对各种终端类型的硬件要求见表1。

表1　终端类型的硬件要求

项目号	硬件设备	有服务员			无人服务（自助）			
		仅联机	联机/脱机	仅脱机	仅联机	联机/脱机	仅脱机	联机 ATM
1	键盘	必备	必备	必备	推荐	推荐	推荐	必备
2	密码键盘	必备	必备	必备	必备	可选	可选	必备
3	显示屏	必备	必备	必备	推荐	推荐	推荐	必备
4	时钟	推荐	必备	必备	推荐	必备	必备	推荐
5	打印机	必备	必备	必备	推荐	推荐	推荐	推荐
6	磁条阅读器	必备	必备	必备	必备	必备	必备	必备
7	IC 卡读卡器	必备	必备	必备	必备	必备	必备	必备
8	主机通信模块	必备	必备	可选	必备	必备	可选	必备

6　一般需求

6.1　交易类型

JR/T 0025借记/贷记应用支持的交易类型见附录A.3。

6.2　交易输入方式

如果卡片是磁条卡，则终端刷磁条卡进行交易。如果卡片是芯片磁条复合卡，则终端应首先读取芯片卡，如果该设备不能读芯片或卡上无芯片，终端读取磁条数据进行交易。如果设备既不能读芯片也不能读磁条数据，也可通过手工输入账号。终端应按GB/T 15150设置相应的POS输入方式。

终端能识别和支持磁条数据中有效的“服务代码”，发卡行使用服务代码来传递卡的属性。如果磁条卡先读取且服务代码以‘2’或‘6’开头，表示卡片上有芯片模块。如果终端支持芯片卡交易，应提示交易用芯片卡进行。如果终端不能受理IC卡或IC卡无法使用，则允许退转到磁卡交易。

终端能支持卡片中11－19位数字长的账号。

6.3　下载管理

终端应能提供对应用程序、密钥和参数等数据的下载，更新和删除。

下载的通讯端口可以是串行通讯口（RS232、RS485）、Modem通讯口、USB口、红外、GPRS、CDMA和TCI/IP网络端口或其它类型的通讯端口等中的一种或几种。

下载方式也可为本地下载或远程下载等方式。

终端应保证下载控制的安全。只有经过授权或认可的一方才能向终端下载数据，未经授权，不得更改终端中的内容。终端还应能够确认下载数据的安全，能验证终端下载程序的完整性和正确性，确保敏感关键的密钥数据在下载过程中不会泄漏。

7　借记/贷记应用功能

7.1　功能概述

7.1.1　流程简介

JR/T 0025借记/贷记应用遵循如下的交易流程。其中必备功能（标为‘M’）是必须执行的，可选性功能（标为‘O’）由卡片和终端的支持情况决定是否执行。交易流程实例见图1所示。

选择应用（M）

当卡片插入终端时，终端决定哪些应用被卡和终端共同支持，并将这些应用显示出来，供用户选择。如果终端无法显示应用列表，则根据卡片中应用优先指示器自动选择优先权最高的应用执行。

应用初始化/读应用数据（M）

在终端选择应用之后，从卡片读取该应用的数据。由这些数据得知卡片具备的功能以及支持这些功能所需的应用数据。根据交易特征，例如国内或国际的，卡片有可能返回不同的数据或支持功能。终端根据这些数据以及终端能力来决定交易要执行的处理功能。

脱机数据认证（O）

终端根据卡片和终端的支持情况，决定是否使用及使用哪种脱机数据认证方式来认证卡片。如果终端支持脱机数据认证功能，并且检测到卡片支持静态数据认证（SDA）、动态数据认证（DDA）或复合动态数据认证（CDA）中至少一种，则终端需进行脱机数据认证。

静态数据认证（SDA）主要是用于防止非法篡改卡片数据，即验证卡上重要的应用数据自卡片个人化以后未被欺诈性的修改。终端使用储存在卡上公钥证书里的发卡行公钥，对用发卡行私钥加密的数字签名进行恢复运算，恢复数据中包含了对卡片重要应用数据的哈希值，如果还原出的哈希值与终端对实际卡片内应用数据所产生的哈希值一致，则证实了卡片数据未被修改。

脱机动态数据认证（DDA）主要是用于防止卡片数据被非法修改以及验证卡片本身的真伪。动态数据认证有标准动态数据认证（DDA）和复合动态数据认证（CDA）两种。这两种方式在验证卡片静态数据方面都类似SDA。

在标准DDA中，终端要求卡片使用来自卡片和终端的动态数据（交易唯一的）以及IC卡私钥生成加密的数字签名，终端用从卡片数据恢复出的IC卡公钥对该数字签名解密恢复，如果恢复出的数据与原始数据匹配，则证实了该卡不是用合法卡上数据复制生成的伪卡。

在复合动态数据认证（CDA）中，动态签名的产生是与卡片行为分析阶段的应用密文生成结合在一起的，以确保应用密文来自于合法卡片。

处理限制（M）

终端通过处理限制来检查应用交易是否允许继续进行。检查内容包括应用生效日期、应用失效日期、应用版本号以及其他发卡行定义的限制条件，发卡行可以使用应用用途控制（AUC）来限定卡用于国内还是国外，或能否用于取现、商品、服务以及返现等交易。

持卡人验证（M）

持卡人验证用来确认持卡人的合法性，以防止遗失或被盗卡片的使用。终端通过检查卡片上的持卡人验证方法（CVM）列表确定使用哪种验证方法。CVM列表建立了持卡人验证方法的优先处理顺序，根据终端能力和交易特点向持卡人提供某一特定的身份验证方法。例如，脱机PIN验证、联机PIN验证或签名等。

终端风险管理（M）

终端风险管理检查内容包括交易是否超过最低限额，卡片账号是否出现在终端异常文件中，是否超过连续脱机交易限制，卡片是否为一张新卡，是否商户强制交易联机，以及交易是否随机选择进行联机等。这些风险管理过程提高了交易脱机进行的安全性。

终端行为分析（M）

终端行为分析根据脱机数据认证、处理限制、持卡人验证、终端风险管理的结果以及终端和卡片中设置的风险管理参数决定如何继续交易（脱机批准、脱机拒绝或联机授权）。

卡片行为分析（M）

卡片收到终端请求的应用密文类型后，执行卡片行为分析。通过卡片风险管理检查，决定是否返回终端所要求的应用密文，以反映卡片行为分析结果及卡片对交易结果的判断。卡片行为分析包括对上次联机交易未完成，上次发卡行认证失败，上次脱机数据认证失败，是否达到次数或金额频度上限等的检查。卡片可以返回与终端请求类型不一样的密文，如终端请求脱机批准，卡片可以返回联机处理或脱机拒绝；终端请求联机处理，卡片可以返回脱机拒绝；但如果终端请求脱机拒绝，卡片只能返回脱机拒绝。

完成检查后，卡片使用应用数据及卡上的加密DES密钥生成相应的应用密文。并将其返回给终端。对于脱机批准交易，卡片返回交易证书（TC）；对于联机处理交易，卡片返回授权请求密文（ARQC）；

对于脱机拒绝交易，卡片返回应用认证密文（AAC）。TC可以作为脱机批准交易的凭据，以及确保交易数据未被商户或收单行改动。

联机处理（O）

如果卡片或终端决定交易需要进行联机授权，且终端具备联机能力，终端将向发卡行发送联机授权报文。此报文中包含ARQC密文、用来生成ARQC的数据以及表示脱机处理结果的指示符。发卡行在卡片认证方法（CAM）过程中通过验证ARQC来认证卡片。发卡行在它的授权决定中会考虑CAM结果和脱机处理结果。

传送回终端的授权响应报文可以包括发卡行生成的授权响应密文（ARPC）（用卡片的保密DES密钥对ARQC、授权响应码加密生成）。响应报文中也可以包括发卡行脚本，用于发卡行在卡片发行后对卡片中的数据或状态进行更新。

如果授权响应包含ARPC而且卡片支持发卡行认证，则卡片通过验证ARPC进行发卡行认证，确保联机响应来自真正的发卡行（或其代理）。可以要求卡片只有成功地完成发卡行认证，才能重新设置卡片里某些与安全相关的参数。这样可以防止通过模拟联机处理过程来非法获取卡的安全特性，以及通过伪造批准交易来复位卡片的计数器和指示符。如果发卡行认证失败，随后的卡片交易将被要求联机发送请求授权，直到发卡行认证成功。发卡行可以在卡片中设置如果发卡行认证失败则拒绝交易。

发卡行脚本处理（O）

如果发卡行在授权响应报文中包含了脚本，终端则将脚本解析成脚本命令，并发送给IC卡。在执行脚本更新前，卡片要进行安全检查，以确认脚本来自真正的发卡行且在传输过程中未被更改。脚本命令包括应用锁定、应用解锁、卡片锁定、PIN解锁和更改PIN等。这些命令对当前交易并不产生影响，主要会影响卡片的以后的交易功能。

交易结束（M）

除非交易在前几个步骤因处理异常被终止，否则终端必须通过执行此功能来结束交易。

卡和终端执行最后处理来完成交易。发卡行已批准的交易可以根据发卡行认证结果和卡片中发卡行设置的参数而被卡片拒绝。卡片根据交易结果、发卡行认证结果以及发卡行设置的规则来决定是否复位基于卡片的计数器和指示符。卡片生成TC批准交易，生成AAC拒绝交易。

如果终端在授权请求报文后发送一个清算报文，将TC包含在清算报文中上送。如果发卡行联机批准交易，而随后卡片脱机拒绝该交易，则在单信息系统或收单行主机对批准交易数据收集的系统中，终端应发送一个冲正报文。

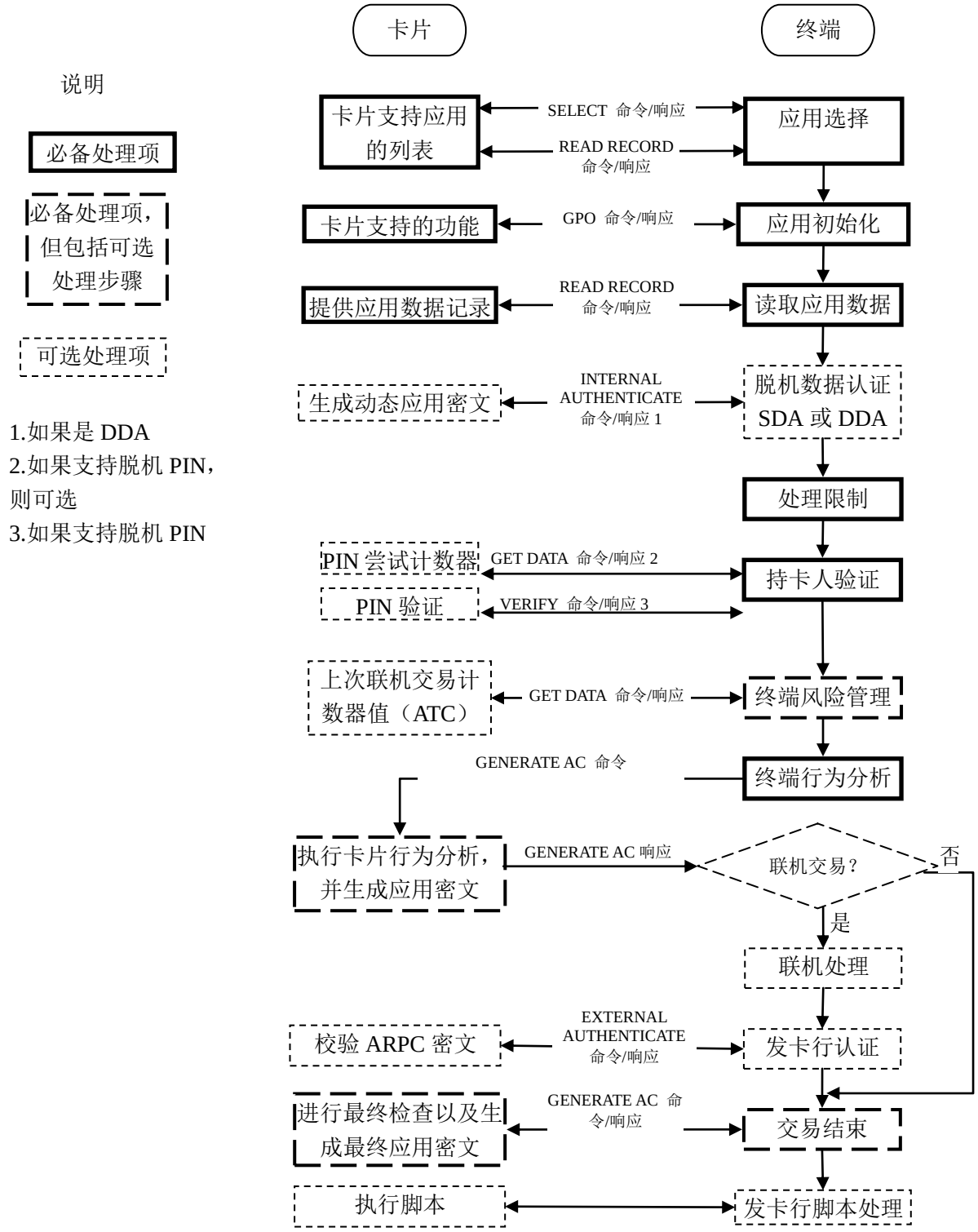

图1　交易流程实例

7.1.2　支持功能

终端支持的功能见表2。

表2　终端功能需求

功能	终端支持
应用选择	必备

功能	终端支持
—— 目录选择方法	必备
—— 应用列表选择方法	必备
启动应用处理	必备
脱机数据认证	有条件的－如果终端有脱机能力则必须支持
—— SDA	有条件的－如果终端有脱机能力，并支持 DDA，则必须支持 SDA
—— DDA	有条件的－如果终端有脱机能力，并支持 CDA，则必须支持 DDA
—— CDA	可选
处理限制	必备
—— 应用版本号	必备
—— 应用用途控制	必备
—— 有效期检查	必备
—— 失效期检查	必备
持卡人验证	必备
—— 无需 CVM	必备
—— CVM 处理失败	必备
—— 脱机明文 PIN	必备
—— 联机 PIN	必备
—— 签名	可选
—— 出示身份证件	可选
终端风险管理	有条件的－如果是商户控制的终端则支持
—— 终端异常文件	对于只联机或只脱机的终端一些功能并不适用
—— 商户强制联机	可选
—— 最低限额	可选
—— 交易日志（与最低限额结合使用）	必备
—— 随机选择	可选
—— 频度检查	有条件的－如果同时有联机和脱机能力则支持
—— 新卡检查	有条件的－如果有联机能力则支持
	必备
终端行为分析	必备
卡片行为分析	（卡功能）
联机处理	
—— 联机能力	必备
—— 通知信息	可选
—— 发卡行认证	有条件的－如果有联机能力则必须支持
交易结束	必备
其它功能	
—— 持卡人金额确认	推荐
—— 发卡行发起的授权参考	推荐
—— 商户强制接受	可选
—— 芯片读取提示	必备

7.2 应用选择

7.2.1 卡片数据

卡片上与应用选择过程相关的数据见表3。

表3 应用选择－卡片数据

数据元	描述
应用定义文件（ADF）	ADF 是一个文件，它是包含应用数据元的应用基本文件（AEF）入口。ADF 包含有关应用的信息例如应用名称、应用首选语言以及应用优先指示器。也可以包含要求终端向卡片传送数据元的处理选项数据对象列表（PDOL）
应用基本文件（AEF）	AEF 包含应用在处理过程中所用到的数据元
应用标识符（AID）	AID 由注册的应用提供商标识（RID）以及扩展的专用应用标识符（PIX）组成
应用标签	按 GB/T 16649.5 标准里与 AID 相关联的名字，用于应用选择。应用标签在 ADF 的 FCI 中可选（推荐要求），在 ADF 目录入口中必须存在
应用首选名称	与 AID 相关联的应用名字。如果应用首选名称存在且终端支持发卡行代码表索引指示的语言，则应用选择过程中显示给持卡人的应用名字应采用应用首选名称，而不是应用标签
应用优先指示器	指示卡片目录里的一个或一组应用的优先权，其格式为一字节长的二进制数，各位含义如下： bit8： 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 bit7-5：保留（000） bit4-1： 0000－未指定优先级 xxxx－应用显示和选择的顺序，取值从 1-15，最高优先级为 1
目录文件	目录文件是列出目录里所包含文件的文件。终端使用 READ RECORD 命令来访问它
文件控制信息（FCI）	FCI 在 SELECT 命令的响应中返回，包含来自卡片的有关应用的信息
发卡行代码表索引	指示卡片所支持的代码表（字符集）按 ISO 8859 定义，用于终端显示应用首选名称
支付系统环境（PSE）	PSE 是名为“1PAY. SYS. DDF01”的 DDF。指示在 PSE 下面的文件结构的目录文件叫做支付系统目录
处理选项数据对象列表（PDOL）	PDOL 是卡片所需终端数据的标签和长度列表。PDOL 包含在 SELECT 命令响应中。终端在 GPO 命令中提供 PDOL 列表所要求的数据给卡片
短文件标识（SFI）	SFI 是基本文件（EF）的指示符

7.2.2 终端数据

终端上与应用选择过程相关的数据如表4。

表4 应用选择－终端数据

数据元	描述
应用标识符（AID）	标签为 ’9F06’，AID 由注册的应用提供商标识（RID）和扩展的专用应用标识符（PIX）组成。它用于唯一识别借记/贷记应用。
应用选择指示器（ASI）	指示应用选择时终端上的 AID 与卡片中的 AID 是完全匹配（长度和内容都必须一样），还是部分匹配（卡片 AID 的前面部分与终端 AID 相同，长度可以更长）。终端支持的应用列表中的每个 AID 仅有一个应用选择指示器，它的格式如

数据元	描述
	表 5 所示
终端支持的应用列表	终端通过一组 AID 来维护所支持的应用列表
PSE 文件名	PSE 的名称“1PAY.SYS.DDF01”，如果终端支持目录选择，PSE 用于应用选择的入口

终端为每个支持的应用设立一个应用选择指示器（ASI）变量，用来表示该应用是全部名称匹配还是部分名称匹配。其定义见表5。

表5　应用选择指示器（ASI）定义

名称	长度	格式	值	含义
应用选择指示器（ASI）	1 字节	二进制	0	部分名称匹配
			1	全部名称匹配

7.2.3　命令

应用选择过程所用到的IC卡金融交易命令：选择（SELECT）命令和读记录（READ RECORD）命令。

SELECT命令

终端发送SELECT命令给卡片，获取卡片支持的应用信息。这些信息由发卡行设定，包括应用优先指示器、应用名称和首选语言等。命令数据中可以包含PSE名（使用目录选择方法）或请求的AID（AID列表选择方法）。

SELECT命令中的P1参数指示应用是否由名称来选择，P2参数指示是否读取具有相同AID前缀的其它应用。

命令返回状态含义如下：

9000 － SELECT命令成功返回；

6A81 － 卡片被锁或命令不支持；

6A82 － 所选的文件未找到；

——情形 1：PSE 未找到，即卡片不支持目录选择方法；

——情形 2：P2 设为读取具有相同 AID 前缀的其它应用时卡片中已没有其它应用。

6283 － 选择文件无效。

READ RECORD命令

在目录选择方法中，终端发READ RECORD命令读取支付系统目录，即与PSE相关联的一个基本文件，该文件列出所有卡片支持的JR/T 0025所定义的支付应用。命令中包括所要读取文件的SFI和文件记录的记录号。卡片返回所要读的记录数据。

7.2.4　建立候选应用列表

终端必须支持下面两种应用选择方法：

——目录选择方法

从卡片上称为支付系统环境（PSE）的主文件－“1PAY.SYS.DDF01”开始，搜索其下的树型卡片文件结构，得到与终端匹配的候选应用列表。卡片对目录选择方法是可选的，但终端必须支持目录选择方法。

——AID 列表方法

终端根据终端应用列表依次发SELECT命令，如果卡片也支持该应用，终端将其加入候选应用列表。如此最终获取卡片和终端共同支持的候选应用列表。终端必须支持AID列表方法。

终端首先尝试用目录选择方法选择应用，用PSE名“1PAY.SYS.DDF01”向卡片发送SELECT命令，如果未找到PSE，或PSE的目录文件中没有与终端匹配的应用，则终端改用AID列表方法选择应用。如果PSE方法成功选出了卡片与终端共同支持的应用（候选应用列表不为空），则终端直接进行下条选择交易应用步骤。

在将卡片应用与终端应用比较时，有两种匹配方式：部分匹配和完全匹配。终端检查应用的应用选择指示器（ASI）确定用哪种匹配方式。

——完全匹配

卡片中的应用AID必须与终端上的应用AID完全相同（包括长度）。对终端支持的每个应用，卡片中最多只有一个应用匹配；

——部分匹配

卡片中的应用AID前面部分完全包括终端上的应用AID，但卡片中的应用AID可以更长一些。即对终端支持的每个应用，卡片中可以有多个应用对应。

7.2.4.1 目录选择方法

步骤1： 终端通过使用选择（SELECT）命令来选择文件名为“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）命令回送状态字“6A82”（文件没有找到）。在这种情况下，终端必须使用12.3.3条所描述的使用应用列表的方式。

如果PSE被锁定，IC卡应该回送状态字“6283”。在这种情况下，终端应该使用12.3.3条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，终端应该使用12.3.3条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12.3.3条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。

步骤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，卡应该回送状态字“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。

步骤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12.3.1条定义），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须要完整匹配（长度和值都相同）还是只须要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。

步骤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12.3.4条所描述的处理过程。

步骤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，终端应该使用12.3.3条所描述的使用应用列表的方式来寻找匹配的应用。

7.2.4.2 AID 列表选择方法

步骤 1：终端使用其列表中的第 1 个 AID 作为文件名发出 SELECT 命令；

步骤 2：如果卡被锁定或者 SELECT 命令不支持导致 SELECT 命令失败（IC 卡回送状态字 SW1 SW2 = “6A81”），终端将中断选择过程；

步骤 3：如果 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，则进入步骤 5；

步骤 4：如果 SELECT 命令返回成功（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；

步骤 5：终端使用其列表中的下一个 AID 向卡片发送 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；

步骤 6：对应于 AID 列表，终端还保存了表明是否允许有多个应用匹配的应用选择指示器（ASI）。终端在选择应用时会检查该指示器，如果指示器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且应用没有锁定（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。

步骤 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”），向卡片发送 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。如果返回其它状态字，终端转到步骤 5。

7.2.5 选择交易应用

终端得到卡片与终端共同支持的候选应用列表后，应从中选择一个应用执行交易。

7.2.5.1 终端自动选择应用

如果终端不支持持卡人选择或持卡人确认，则终端会自动选择具有最高优先级且不要求确认的应用。如果超过一个应用有最高优先级，终端可以选择其中任一应用或按终端所列顺序选择最前面的应用。

7.2.5.2 持卡人选择交易应用

7.2.5.2.1 终端支持持卡人确认

若终端不支持显示供持卡人选择的应用列表，而支持持卡人应用确认，它首先将优先级最高的应用提供给持卡人确认。如果超过一个应用有同样的优先级，终端可以根据遇到的先后次序或自行选择其中一个应用。如果持卡人确认这个选择，终端就选择该应用。

如果持卡人不确认，终端提供下一个优先级最高的应用，直到持卡人确认或不再有更多的可用应用为止。

如果候选应用列表已处理完持卡人仍未确认一个应用，则终止交易。

7.2.5.2.2 终端支持持卡人选择

支持持卡人选择的终端将向持卡人按优先级顺序给出应用列表以供选择。如果超过一个应用有同样的优先级，终端可以按读出的顺序或自行安排顺序。持卡人从列表中选择一个应用。

如果持卡人不选择应用，终端就终止交易。

7.2.5.3 终端处理描述

如候选列表中没有应用，交易终止；

候选列表有一个应用时，终端按JR/T 0025.3的12.3.4所述自动选择应用或由持卡人确认；

候选列表有多个应用时：

如果终端可以同时显示多个应用名，则终端必须支持持卡人选择应用功能。终端将候选列表中的多个应用按卡片中提供的优先权顺序列出，供持卡人选择。一次显示不下全部应用，可以分多次显示。如果有几个应用的优先权相同，则这几个应用按终端列表中出现的顺序显示；

如果终端每次只能显示一个应用名，则终端必须支持持卡人确认功能。终端按优先权顺序逐个显示应用名称供持卡人确认，直至某个应用被确认选择。

如果终端无法显示应用名，则如JR/T 0025.3的12.3.4中描述，终端自动从候选列表中选择优先权最高的应用执行。

选择出一个应用后，终端再向卡片发送SELECT命令，选中该应用，并获取该应用FCI中的数据。如果卡片返回不是“9000”，且候选列表中还有其它应用，则终端将此应用从候选列表删除，在终端上显示“请重试”，重新进行上述的选择过程。如果候选列表里没有其它应用，则交易终止。

处理流程

应用选择的处理流程见图2－图4。

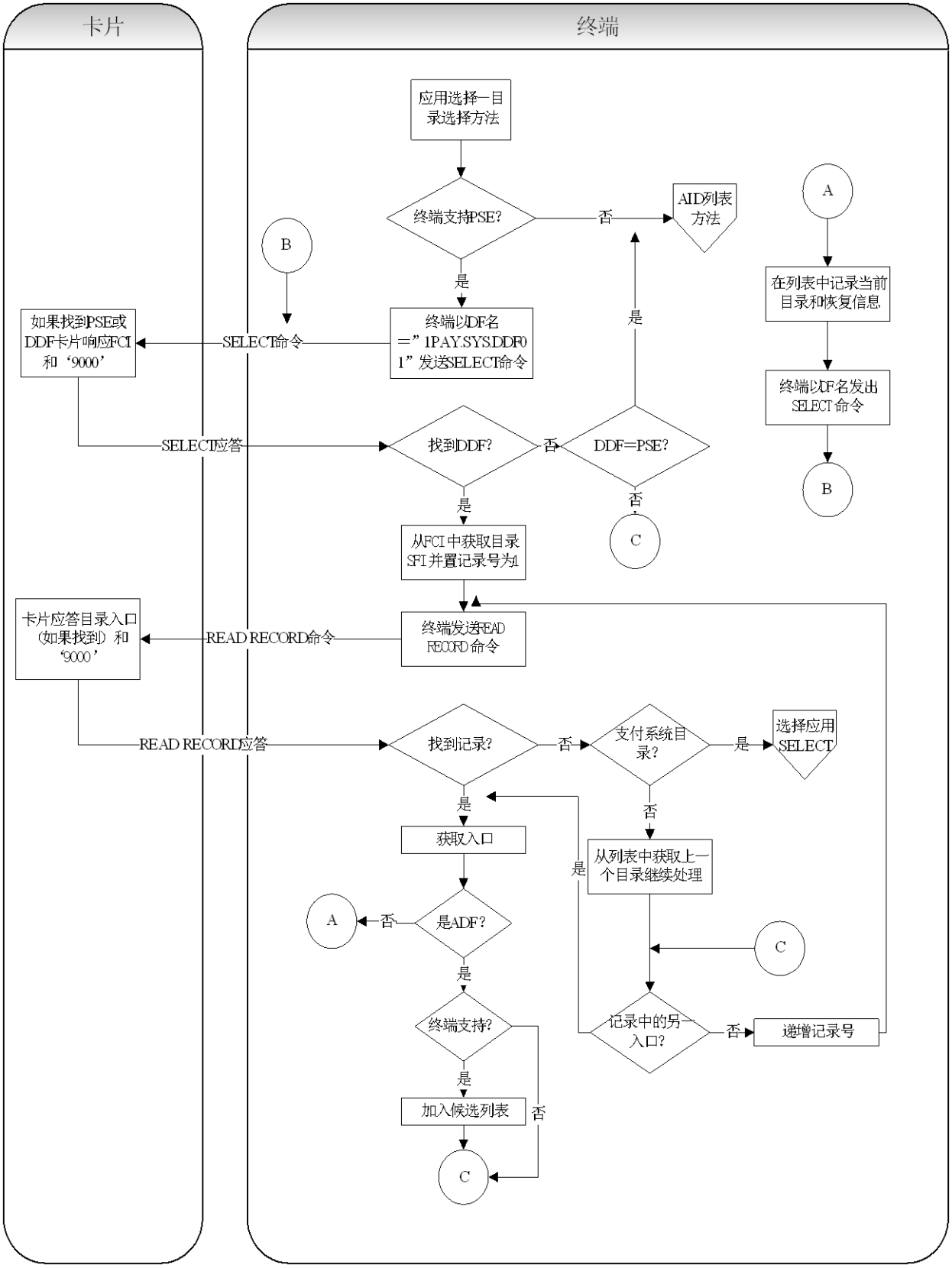
卡片
终端
应用选择—目录选择方法
终端支持PSE?
否
AID列表方法
是
A
在列表中记录当前目录和恢复信息
终端以DF名发出SELECT命令
B
B
如果找到PSE或DDF卡片响应FCI和‘9000’
SELECT命令
终端以DF名=”1PAY.SYS.DDF01”发送SELECT命令
是
SELECT应答
找到DDF?
否
DDF=PSE?
否
是
C
从FCI中获取目录SFI并置记录号为1
卡片应答目录入口（如果找到）和‘9000’
READ RECORD命令
终端发送READ RECORD命令
READ RECORD应答
找到记录?
否
支付系统目录?
是
选择应用SELECT
是
否
获取入口
是
从列表中获取上一个目录继续处理
A
否
是ADF?
C
是
终端支持?
记录中的另一入口?
否
递增记录号
是
加入候选列表
否
C

图2　应用选择流程图(1)

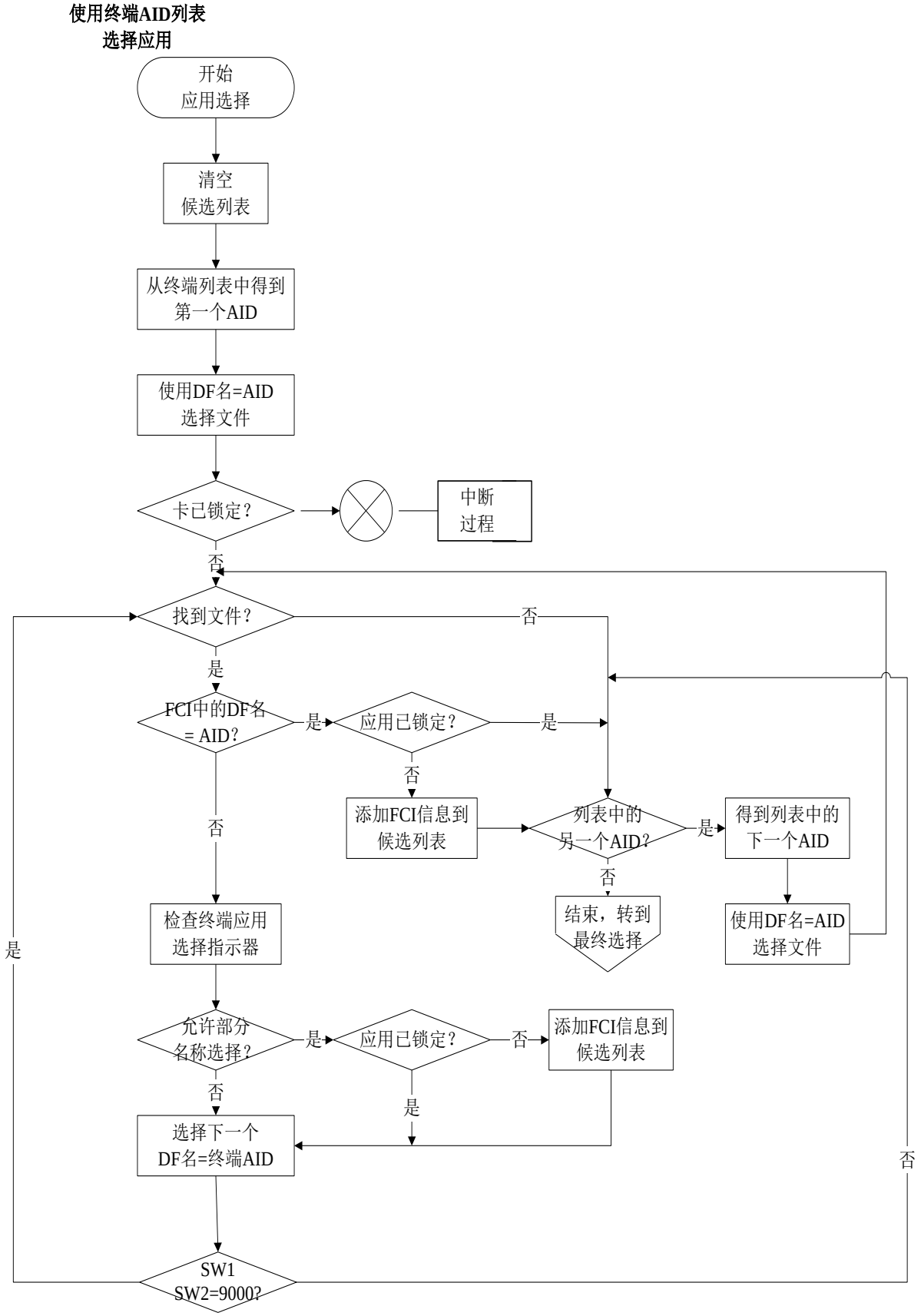
使用终端AID列表
选择应用
开始
应用选择
清空
候选列表
从终端列表中得到
第一个AID
使用DF名=AID
选择文件
卡已锁定?
中断
过程
否
找到文件?
否
是
FCI中的DF名
= AID?
是
应用已锁定?
是
否
添加FCI信息到
候选列表
列表中的
另一个AID?
是
得到列表中的
下一个AID
否
结束，转到
最终选择
使用DF名=AID
选择文件
否
检查终端应用
选择指示器
是
允许部分
名称选择?
是
应用已锁定?
否
添加FCI信息到
候选列表
否
是
选择下一个
DF名=终端AID
SW1
SW2=9000?
否

图3　应用选择流程图(2)

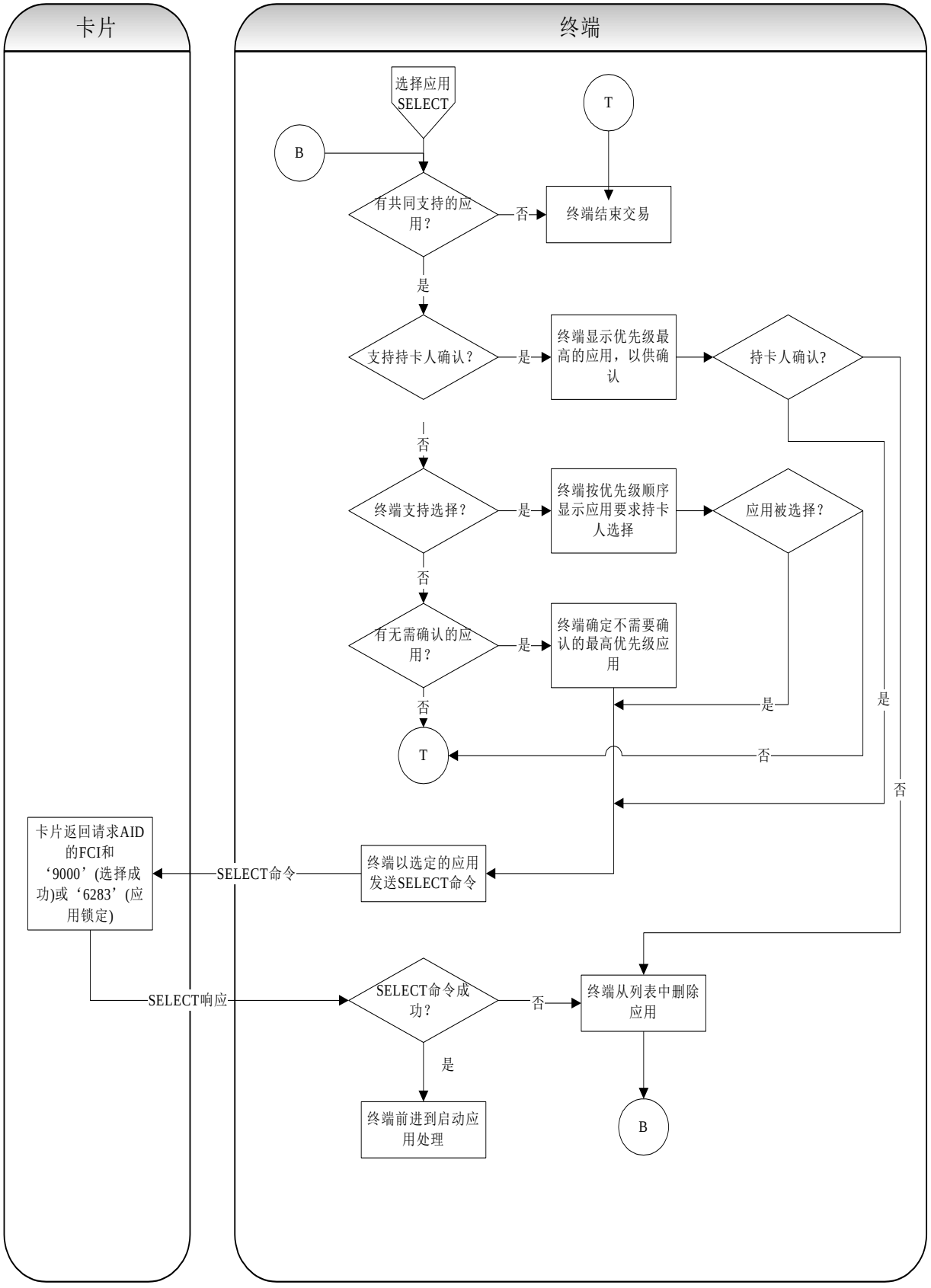
卡片
终端
选择应用SELECT
B
T
有共同支持的应用？
否
终端结束交易
是
支持持卡人确认？
是
终端显示优先级最高的应用，以供确认
持卡人确认？
否
终端支持选择？
是
终端按优先级顺序显示应用要求持卡人选择
应用被选择？
否
有无需确认的应用？
是
终端确定不需要确认的最高优先级应用
否
T
是
否
是
否
卡片返回请求AID的FCI和‘9000’(选择成功)或‘6283’(应用锁定)
SELECT命令
终端以选定的应用发送SELECT命令
SELECT响应
SELECT命令成功？
否
终端从列表中删除应用
是
终端前进到启动应用处理
B

图4　应用选择流程图(3)

7.2.6 后续相关处理

应用初始化

终端发送到卡的GPO命令包括PDOL指定的所有终端数据元。如果卡片支持PDOL，则应用选择时PDOL会被包含在SELECT响应里。如果卡片不允许执行所选择的应用，终端就退出当前应用处理，并返回应用选择过程再选择另一个应用。

7.3 应用初始化

7.3.1 卡片数据

卡片上与应用初始化相关的数据见表6。

表6 应用初始化－卡片数据

数据元	描述
应用文件定位器（AFL）	包含终端将要读取用来交易处理的卡片数据文件的 SFI 和记录范围。每个要读取的文件在 AFL 中对应四个字节，含义如下： 字节 1：短文件标识符 字节 2：文件中要读取的第 1 个记录的记录号 字节 3：文件中要读取的最后一个记录的记录号 字节 4：从第 1 个记录开始的用于脱机数据认证的连续记录数
应用交互特征（AIP）	指示卡片对借贷记功能的支持能力，包括静态数据认证（SDA）、动态数据认证（DDA）、复合动态数据认证（CDA）、持卡人验证、终端风险管理和发卡行认证等
文件控制信息（FCI）	FCI 是卡片有关应用的信息，包含在 SELECT 命令的响应中
处理选项数据对象列表（PDOL）	PDOL 是卡片向终端请求的终端数据的标签和长度列表。它包含在终端使用 SELECT 命令得到的 FCI 中。终端通过获取处理选项（GPO）命令提供 PDOL 所列的数据

7.3.2 终端数据

终端上根据PDOL所定义的内容提供相应的终端数据给卡片。

7.3.3 命令

终端通过获取处理选项（GPO）命令通知卡片交易开始。命令数据为PDOL指定的终端数据。卡片在命令响应中按格式1返回AIP和AFL，见JR/T 0025.5的附录B.8对GPO命令响应数据格式的描述。

7.3.4 处理流程

终端读取所选应用的SELECT命令返回的包含在FCI中的PDOL。

终端处理PDOL，根据DOL的处理规则填入终端数据。

终端向卡片发送GPO（获取处理选项）命令，将处理PDOL得到的终端数据作为命令数据以TLV格式（标签‘83’）送给卡片。如果PDOL不存在，则命令数据域为“83 00”。

如果卡片返回成功（SW1 SW2＝“9000”），终端读取AIP和AFL，然后进行后面的读应用数据处理。

如果卡片返回“69 85”，表明卡片不支持该应用，终端应从本次交易的应用候选列表中删除该应用，返回到应用选择过程重新选择应用。

应用初始化流程见图5。

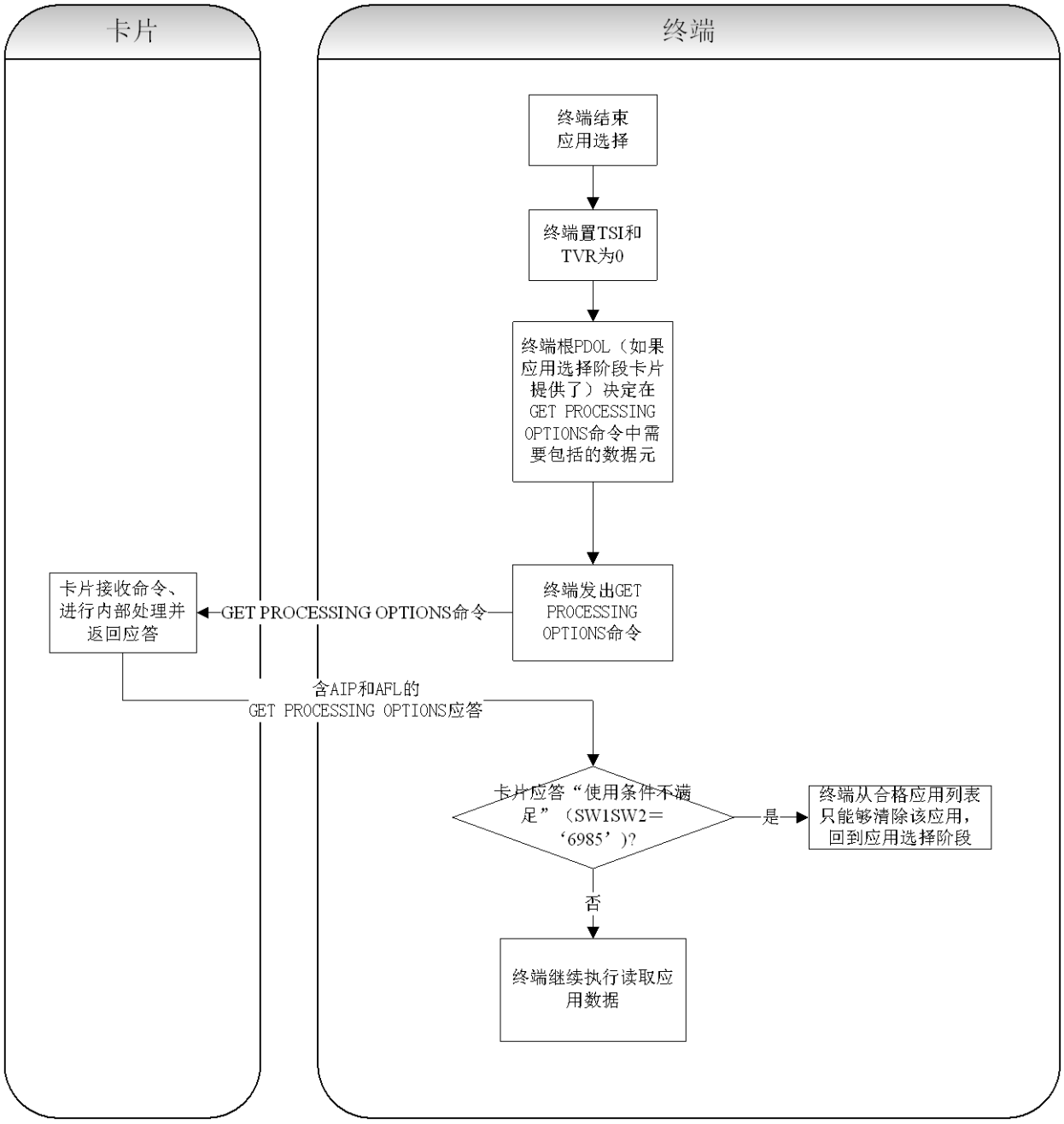

图5　应用初始化流程

7.3.5　前期相关处理

应用选择

卡片在SELECT命令的响应中将PDOL（若存在）作为FCI的一部分提供给终端。

7.3.6　后续相关处理

读应用数据

终端使用由卡片提供的包含在GPO命令响应中的AFL，来确定从卡读取哪些应用数据以及哪些应用数据将要用到脱机数据认证中。

脱机数据认证

终端使用由卡片提供的包含在GPO命令响应中的AIP，来确定卡片是否支持脱机数据认证。

持卡人验证

终端使用由卡片提供的包含在获取处理选项（GPO）命令响应中的AIP，来确定卡片是否支持持卡人验证。

联机处理

终端使用由卡片提供的包含在获取处理选项（GPO）命令响应中的AIP，来确定卡片是否支持发卡行认证。

7.4 读应用数据

7.4.1 卡片数据

卡片上与读应用数据相关的数据见表7。

表7 读应用数据－卡片数据

数据元	描述
应用文件定位器（AFL）	包含终端将要读取的用来交易处理的卡片数据文件的 SFI 和记录范围。每个条目指定了要从文件读取的第 1 条记录和最后一条记录号以及哪些记录要用在脱机数据认证中
应用基本文件（AEF）	包含应用交易处理使用到的数据的卡片数据文件。AEF 由一组按记录号寻址的记录组成，终端用读记录（READ RECORD）命令读取这些记录，命令参数包含要读取的文件 SFI 和记录号
短文件标识符（SFI）	SFI 是用来唯一标识应用数据文件的符号。在 AFL 里列出，终端用它来标识要读取的文件

7.4.2 终端数据

无。

7.4.3 命令

终端向卡片发送读记录（READ RECORD）命令读取记录数据。命令参数P2包含所要读取文件的SFI，P1为所读取记录的记录号。如果返回状态SW1 SW2为“9000”，则响应数据域中包含请求的记录数据。

7.4.4 处理流程

终端通过AFL决定要从卡片中读取哪些交易数据记录，每个AFL项（四个字节）代表了卡片一个文件中的连续记录。对每个AFL项（四个字节），从第1条记录开始，终端依次对每条记录向卡片发送一个读记录（READ RECORD）命令读取记录数据，一直到最后一条记录。如此将所有AFL项处理完。读到的交易数据中可以识别的应存储在终端上供交易使用。如果读取到TLV格式正确但规范未定义的标签，终端应将其保存以备后用，终端不应因此而终止交易。对于AFL指明要用于脱机数据认证的记录，则将其数据加到脱机认证的数据列表中供脱机数据认证使用。

读数据处理中如果出现如下情况之一，终端应当终止交易：

——卡片在一条或多条记录中返回同一个标签两次及两次以上；

——卡片在某条记录中返回了卡片已经在 GPO 响应中返回的标签；

——卡片中缺少必须有的数据；

——数据格式错；

——READ RECORD 命令返回状态字不是“9000”。

不应当因为下列情况中的一条或多条的存在而终止交易：

——卡片返回了持卡人姓名（5F20）但该标签的长度不符合 JR/T 0025.5 的规定；

——卡片返回了持卡人姓名扩展（9F0B）但该标签的长度不符合 JR/T 0025.5 的规定；

——卡片既返回了持卡人姓名（5F20）也返回了持卡人姓名扩展（9F0B）。

终端的处理流程图见图6。

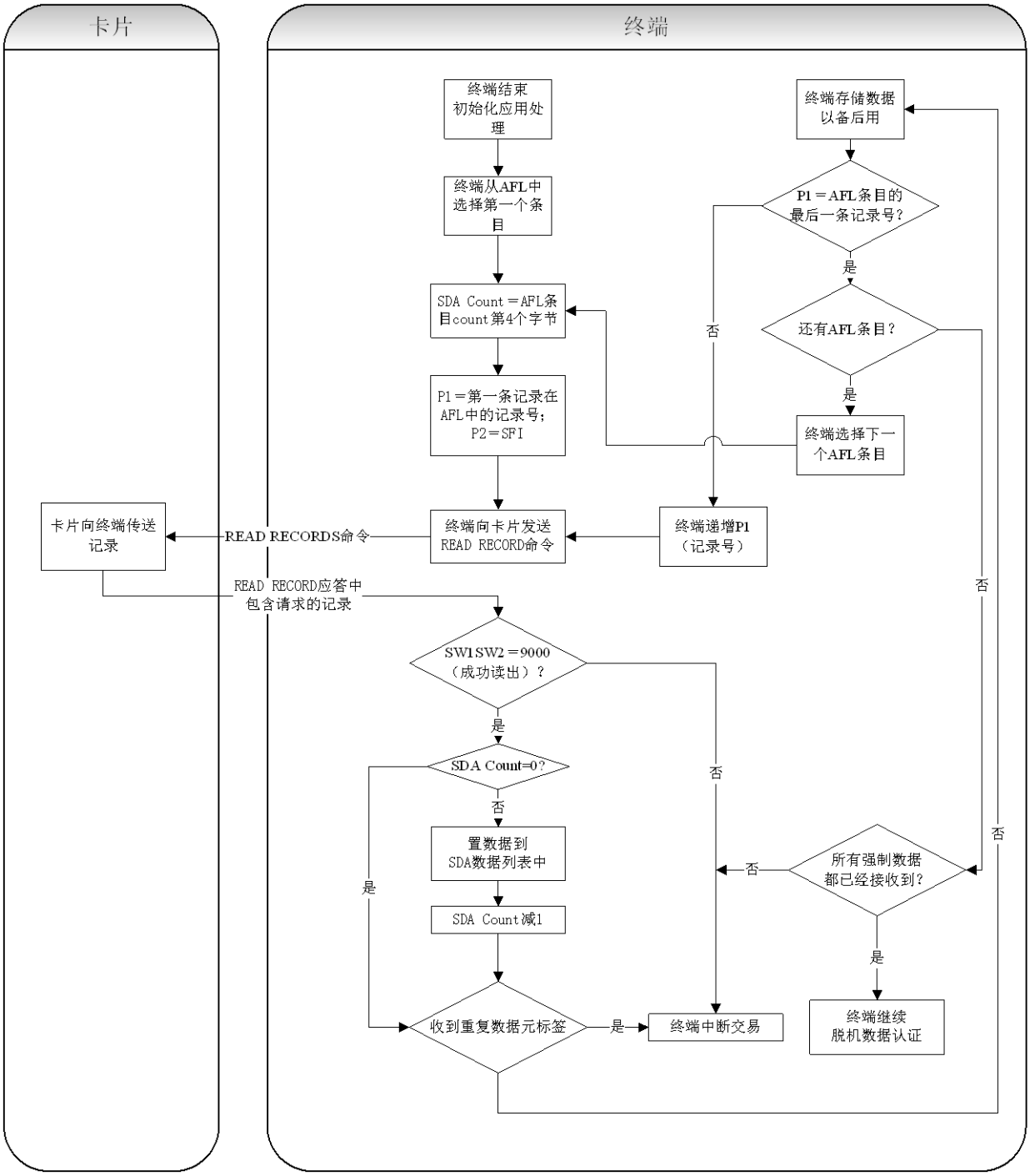

图6　读应用数据处理流程图

7.4.5　前期相关处理

应用初始化

终端从获取处理选项（GPO）命令的响应中得到应用的AFL用于读取应用数据。

7.4.6　后续相关处理

脱机数据认证

SDA、DDA和CDA用读应用数据时建立的静态认证数据列表来验证带签名的静态数据。

其他功能

其它交易功能用读应用数据时读取的数据进行处理。

7.5 脱机数据认证

7.5.1 终端要求

7.5.1.1 加密算法

为支持脱机数据认证，终端应支持JR/T 0025.7中所描述的非对称加密算法和哈希算法。关于算法描述请见JR/T 0025.7。

7.5.1.2 公钥管理

终端应至少支持六组认证中心公钥。所支持的公钥长度最大可至1984位（248字节）。应能确保公钥下载和存储的安全、正确性，并按JR/T 0025.7的要求支持公钥的回收和更新。

7.5.2 支持条件

JR/T 0025规定了三种脱机数据认证方法：静态数据认证(SDA)，动态数据认证(DDA)和复合动态数据认证(CDA)。SDA验证了卡内数据的正确性，DDA验证了卡内数据的正确性及卡的合法性。CDA则将动态数据认证(DDA)和应用密文生成结合起来，提供对卡内数据、卡片本身和交易安全的认证。各种类型的终端对脱机数据认证方法的支持见表8。

表8 终端对脱机数据认证的支持

终端类型	支持		
	SDA	DDA	CDA
有服务员的仅联机终端	可选	可选	可选
有服务员的具备联机能力的脱机终端	必备	必备	可选
有服务员的仅脱机终端	必备	必备	可选
自助式仅联机终端	可选	可选	可选
自助式具备联机能力的脱机终端	必备	必备	可选
自助式仅脱机终端	必备	必备	可选
仅联机的 ATM	可选	可选	可选

7.5.3 脱机数据认证方法的确定

7.5.3.1 卡片数据

表9 脱机数据认证方式判断－卡片数据

数据元	描述
应用交互特征（AIP）	包含卡片对脱机数据认证支持能力的标志位： ● 卡片支持 SDA ● 卡片支持 DDA ● 卡片支持 CDA

7.5.3.2 终端数据

表10 脱机数据认证方式判断－终端数据

数据元	描述
终端性能	包含终端对脱机数据认证支持能力的标志位： ● 终端支持 SDA ● 终端支持 DDA ● 终端支持 CDA
交易状态信息（TSI）	包含指示执行了某种脱机数据认证方法的标志位
终端验证结果（TVR）	包含指示没有任何一种脱机数据认证方法被执行的标志位

7.5.3.3 处理

在一个交易中，最多只执行一种脱机数据认证方法。卡片对脱机数据认证的支持情况在AIP中指示；终端对脱机数据认证方法的支持在终端性能中指示。终端根据卡片和终端对脱机数据认证的共同支持情况决定本次交易采用哪种脱机数据认证。三种认证方式的处理优先权顺序依次为：CDA、DDA和SDA。终端判断处理规则如下：

——如果卡片和终端都支持 CDA，则执行 CDA；

——否则，如果卡片和终端都支持 DDA，则执行 DDA；

——否则，如果卡片和终端都支持 SDA，则执行 SDA；

——如果上述条件都不满足，则终端不执行脱机数据认证，并在 TVR 中设置“脱机数据认证未执行”位为‘1’。

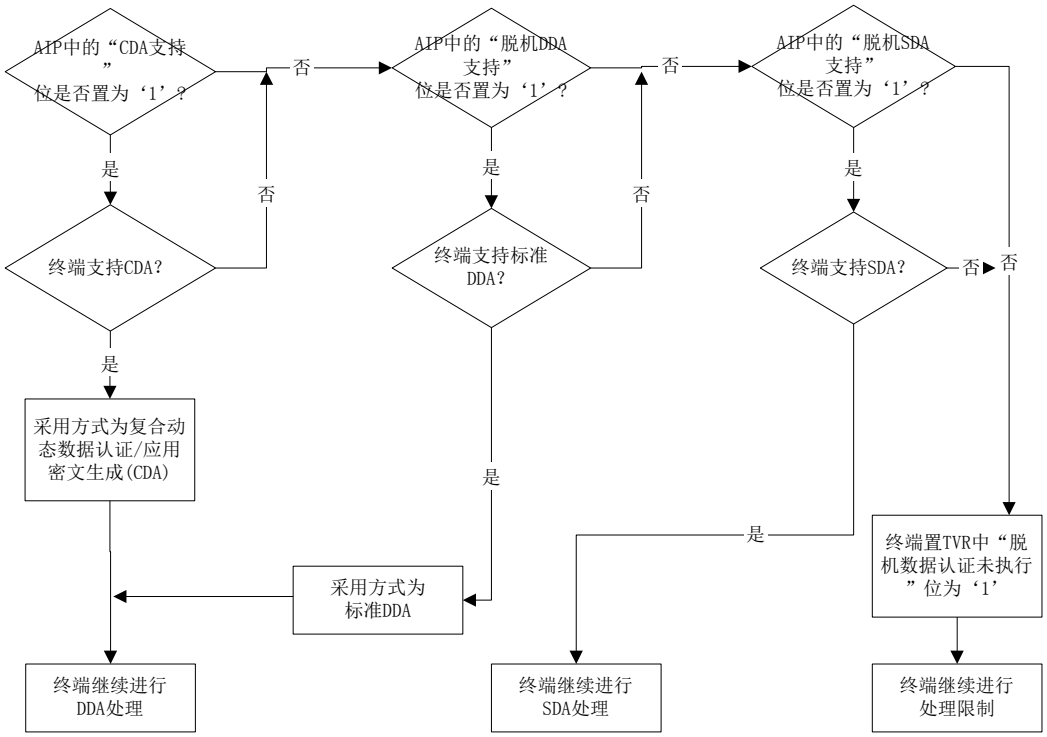

图7 脱机数据认证执行方式判断

7.5.4 静态数据认证

7.5.4.1 卡片数据

卡片上与SDA相关的数据见表11。

表11 SDA－卡片数据

数据元	描述
认证中心公钥索引（PKI）	静态数据认证中用于脱机数据认证的每个公钥都由认证中心公钥索引（PKI）与注册的应用提供商标识一起唯一标识
发卡行公钥证书	发卡行公钥证书包含用认证中心私钥签名的发卡行公钥
发卡行公钥指数	用于恢复签名静态应用数据和 IC 卡公钥证书
发卡行公钥余项	包含发卡行公钥中未列入发卡行公钥证书的部分
注册的应用提	AID 的一部分（前 5 个字节），用于标识支付机构。RID 与公钥索引一起用来确定交易所要用的公钥

数据元	描述
供商标识（RID）	
签名静态应用数据（SAD）	用发卡行私钥加密的签名，包含卡内重要数据的哈希值
静态数据认证标签列表	包含用于脱机数据认证的数据的标签列表，该数据元可选，但如果出现，只允许包含 AIP（标签‘82’），如果包含了其它数据，则 SDA 失败
需认证的静态数据	用于验证签名静态应用数据（SAD）的卡片数据，包括在 AFL 指定的用于脱机数据认证的记录数据，以及 SDA 标签列表中的指定的数据。如果 SDA 标签列表存在，应当只包含 AIP 的标签（‘82’），终端检查 SDA 标签列表中是否只有 AIP 的标签

7.5.4.2 终端数据

终端上与SDA相关的数据见表12。

表12 SDA－终端数据

数据元	描述
公钥索引（PKI）	用于脱机数据认证中的每个 CA 公钥由 PKI 和应用标识符（AID）中的注册的应用提供商标识（RID）一起唯一标识
CA 公钥	存储在终端中用于恢复发卡行公钥证书的公钥
终端验证结果（TVR）	包含一个用于指示 SDA 失败的标志
注册的应用提供商标识（RID）	指示终端中特定支付机构的公钥列表和 PKI 一起标识认证中心公钥

7.5.4.3 处理流程

SDA的执行步骤如下，见JR/T 0025.7的5.2。

步骤 1：取得 CA 公钥

终端使用卡片中的公钥索引和RID来唯一确定并取得存储在终端中的公钥和相关信息。

步骤 2：发卡行公钥的恢复

a)终端检查发卡行公钥证书与认证中心公钥模长度是否相同；

b)终端利用认证中心公钥对发卡行公钥证书恢复，取出证书里的数据；

c)检查恢复数据中的各项是否正确：恢复的数据尾、恢复的数据头、证书格式、发卡行标识、证书有效期和发卡行算法标识；

d)计算静态认证数据的哈希结果，并与从证书里恢复的哈希结果比较是否一致；

e)将恢复数据中的发卡行公钥模部分与余项部分（如果有）组合成发卡行公钥。

步骤 3：签名静态应用数据(SAD)的认证

终端利用发卡行公钥对签名的静态应用数据恢复,并进行哈希值比较,验证签名是否正确。

a)终端检查签名静态应用数据与发卡行公钥模长度是否相同；

b)终端利用发卡行公钥对签名的静态应用数据进行恢复；

c)检查恢复数据中的各项是否正确：恢复的数据尾、恢复的数据头和数据格式；

d)终端依次连接从签名静态应用数据恢复出的数据、由 AFL 指定的用于脱机数据认证的记录数据、以及由静态数据认证标签列表表示的数据，并计算其哈希结果；

e)将计算出的哈希结果与从签名静态应用数据恢复出的哈希结果比较，如果不一致，则 SDA 失败。

步骤 4：SDA 结果

——如果以上所有步骤执行成功，则 SDA 成功；

——如果 SDA 失败，TVR 中的“脱机静态数据认证失败”位应设为“1”；

——如果执行了 SDA，则交易状态信息（TSI）中的“脱机数据认证被执行”位设为“1”。

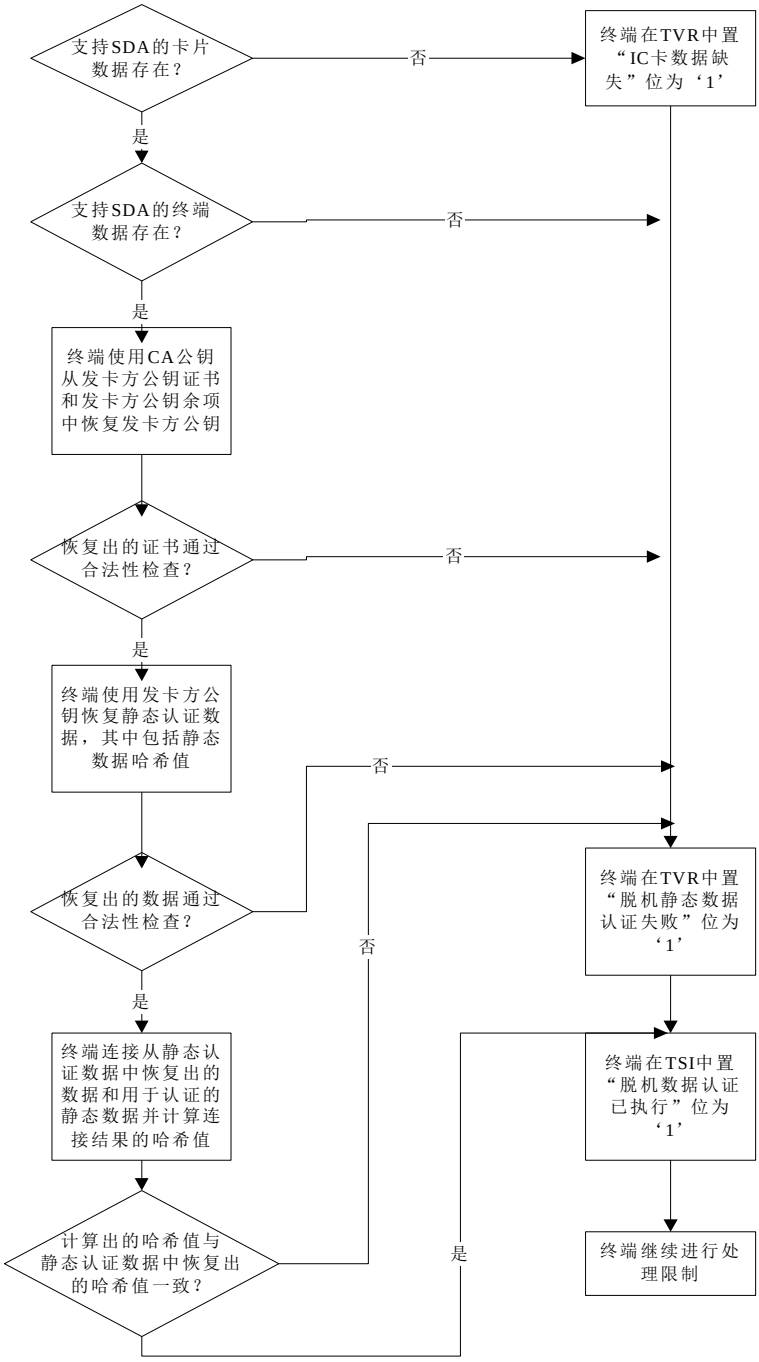

图8　SDA 流程图

7.5.5　动态数据认证

如果要求执行DDA，终端使用公钥算法验证卡片里的静态应用数据，这一步与静态数据认证相似，但不完全一样。验证了静态数据后，终端要求卡片用交易动态数据生成一个动态签名，终端验证此签名。从而验证了卡片中的数据未被更改，以及卡片本身是一张真正的卡，而不是用复制真卡数据而伪造的假卡。

7.5.5.1　卡片数据

DDA使用SDA中用到的除了签名静态应用数据外的其它卡片数据，除此之外DDA用到的卡片数据见表13。

表13 DDA－卡片数据

数据元	描述
动态数据认证数据对象列表（DDOL）	动态数据认证处理中要传递到卡片的终端数据对象的标签列表
IC 卡公钥证书	IC 卡公钥证书包含用发卡行私钥签名的 IC 卡公钥
IC 卡公钥指数	用于恢复签名动态应用数据
IC 卡公钥余项	包含 IC 卡公钥未列入 IC 卡公钥证书的部分
签名动态应用数据	卡片用 IC 卡私钥对来自卡片和终端的动态交易数据进行加密后的签名数据

7.5.5.2 终端数据

终端上与DDA相关的数据说明。

表14 DDA－终端数据

数据元	描述
缺省动态数据认证数据对象列表（缺省 DDOL）	如果未从卡片中得到 DDOL，指明要求终端在动态签名生成中传送给卡片的数据。缺省 DDOL 仅包含不可预知数的标记和长度（“9F 37 04”），不应包含其它的数据对象
终端验证结果（TVR）	包含 DDA 失败的指示位
不可预知数	由终端产生的四字节长的不可预知的交易唯一数字，用于包含在内部认证（INTERNAL AUTHENTICATE）命令中

7.5.5.3 命令

内部认证（INTERNAL AUTHENTICATE）命令

在DDA中终端给卡片发送内部认证（INTERNAL AUTHENTICATE）命令请求动态签名。命令数据域中包含由DDOL指明的数据。在响应中卡片返回签名动态应用数据。

7.5.5.4 处理流程

标准DDA的执行步骤如下，详细描述见JR/T 0025.7的5.3。

步骤 1：取得 CA 公钥

终端使用卡片中的公钥索引和RID来唯一确定并取得存储在终端中的公钥和相关信息。

步骤 2：恢复发卡行公钥

a)终端检查发卡行公钥证书与认证中心公钥模长度是否相同；

b)终端利用认证中心公钥对发卡行公钥证书恢复，得到发卡行公钥；

c)检查恢复数据中的各项是否正确：恢复的数据尾、恢复的数据头、证书格式、发卡行标识、证书有效期和发卡行算法标识；

d)计算静态认证数据的哈希结果，并与从证书里恢复的哈希结果比较是否一致；

e)将恢复数据中的发卡行公钥模部分与余项部分（如果有）组合成发卡行公钥。

步骤 3：恢复 IC 卡公钥

a)终端检查 IC 卡公钥证书与发卡行公钥模长度是否相同；

b)终端利用发卡行公钥对 IC 卡公钥证书进行恢复，取出证书里的数据；

c)检查恢复数据中的各项是否正确：恢复的数据尾、恢复的数据头、证书格式、证书有效期、IC 卡密钥算法标识和 PAN；

d)终端依次连接从 IC 公钥证书恢复出的数据、由 AFL 指定的用于脱机数据认证的记录数据、以及由静态数据认证标签列表表示的数据，并计算其哈希结果；

e)将计算出的哈希结果与从 IC 公钥证书恢复出的哈希结果比较，如果不一致，则 DDA 失败；

f)将恢复数据中的 IC 卡公钥模部分与余项部分（如果有）组合成 IC 卡公钥。

步骤 4：动态签名生成

终端向卡片发送内部认证（INTERNAL AUTHENTICATE）命令，该命令包含一串DDOL指定的数据元。如果未从卡片上读到DDOL，则使用来自终端的缺省DDOL。如果所用的DDOL中不包含不可预知数的标签（“9F 37”），则DDA失败。

IC卡通过使用卡片上的IC卡私钥对来自内部认证（INTERNAL AUTHENTICATE）命令的终端动态数据和来自卡片的动态数据进行签名加密产生签名动态应用数据。签名动态应用数据在内部认证（INTERNAL AUTHENTICATE）命令的响应里返回给终端。

步骤 5：动态签名认证

终端利用IC卡公钥对签名的动态应用数据恢复，并进行哈希值比较，验证签名是否正确。

a)终端检查签名动态应用数据与 IC 卡公钥模长度是否相同；

b)终端利用 IC 卡公钥对签名动态应用数据进行恢复，取出签名里的数据；

c)检查恢复数据中的各项是否正确：恢复的数据尾、恢复的数据头和数据格式；

d)终端依次连接从签名动态应用数据恢复出的数据、DDOL 所表示的数据，并计算其哈希结果；

e)将计算出的哈希结果与从签名动态应用数据恢复出的哈希结果比较，如果不一致，则 DDA 失败。

步骤 6：DDA 结果

——如果以上步骤全部执行成功，则 DDA 执行成功；

——如果 DDA 失败，TVR 中的“脱机动态数据认证失败”位须设为“1”；

——如果执行了 DDA，则交易状态信息（TSI）中的“脱机数据认证被执行”位设为“1”。

DDA流程图见图9-图11。

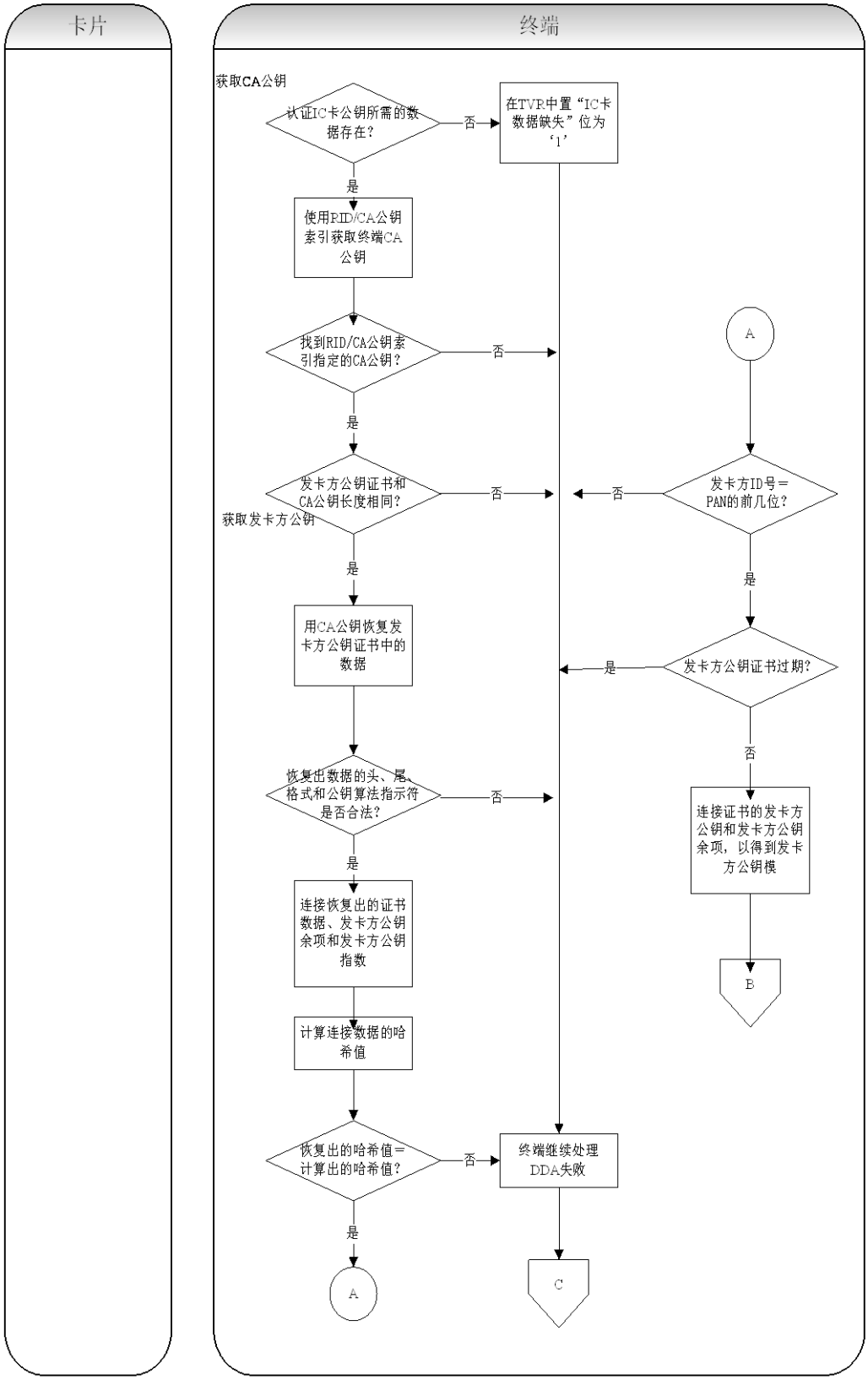
卡片
终端
获取CA公钥
认证IC卡公钥所需的数据存在?
否
在TVR中置“IC卡数据缺失”位为‘1’
是
使用RID/CA公钥索引获取终端CA公钥
找到RID/CA公钥索引指定的CA公钥?
否
是
A
发卡方公钥证书和CA公钥长度相同?
否
否
发卡方ID号＝PAN的前几位?
获取发卡方公钥
是
是
用CA公钥恢复发卡方公钥证书中的数据
是
发卡方公钥证书过期?
否
恢复出数据的头、尾、格式和公钥算法指示符是否合法?
否
连接证书的发卡方公钥和发卡方公钥余项，以得到发卡方公钥模
是
B
连接恢复出的证书数据、发卡方公钥余项和发卡方公钥指数
计算连接数据的哈希值
恢复出的哈希值＝计算出的哈希值?
否
终端继续处理DDA失败
是
A
C

图9　DDA 流程图（1）

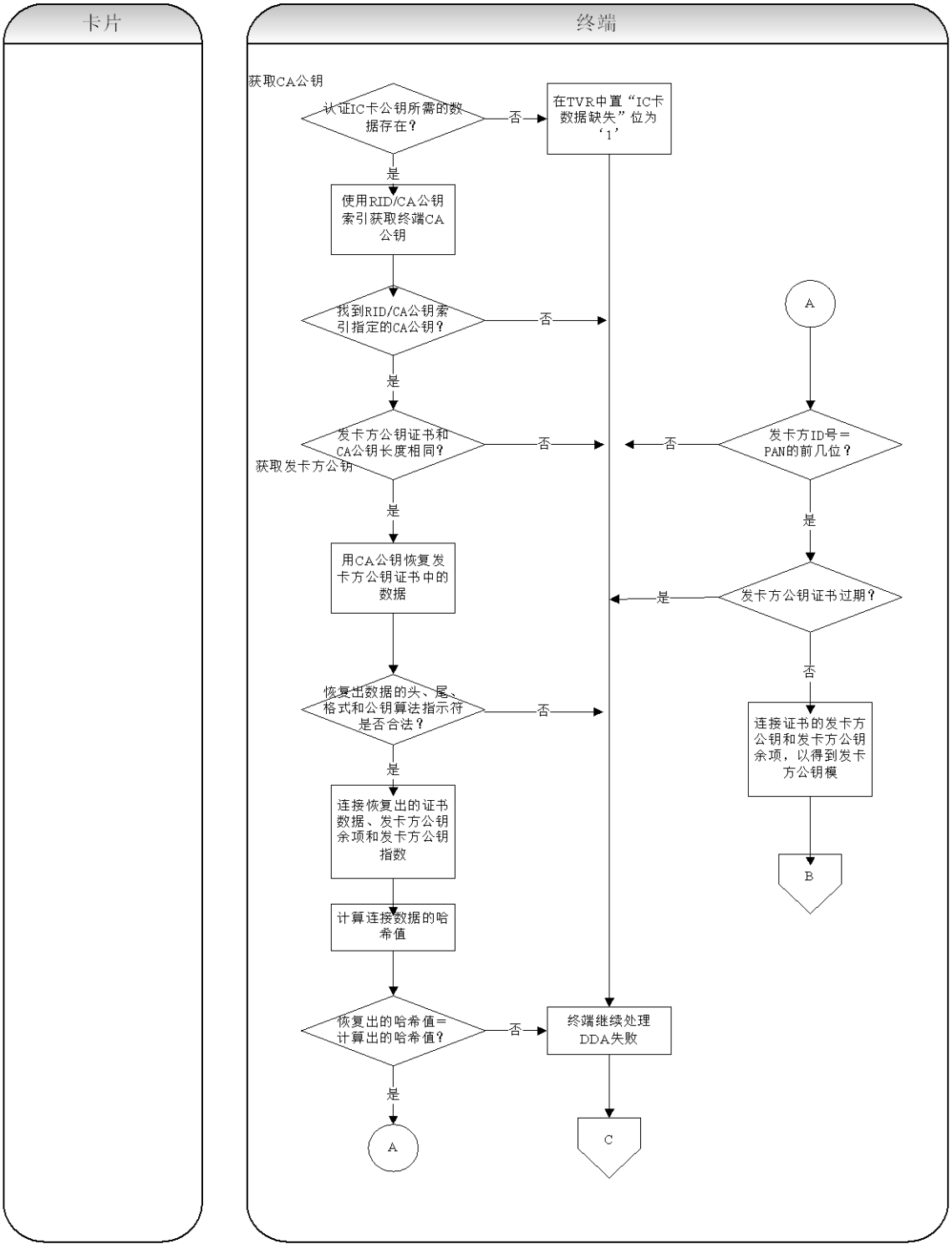
卡片
终端
获取CA公钥
认证IC卡公钥所需的数据存在？
否
在TVR中置“IC卡数据缺失”位为‘1’
是
使用RID/CA公钥索引获取终端CA公钥
找到RID/CA公钥索引指定的CA公钥？
否
是
发卡方公钥证书和CA公钥长度相同？
否
获取发卡方公钥
是
用CA公钥恢复发卡方公钥证书中的数据
恢复出数据的头、尾、格式和公钥算法指示符是否合法？
否
是
连接恢复出的证书数据、发卡方公钥余项和发卡方公钥指数
计算连接数据的哈希值
恢复出的哈希值＝计算出的哈希值？
否
是
A
终端继续处理DDA失败
C
A
发卡方ID号＝PAN的前几位？
否
是
发卡方公钥证书过期？
是
否
连接证书的发卡方公钥和发卡方公钥余项，以得到发卡方公钥模
B

图10　DDA 流程图（2）

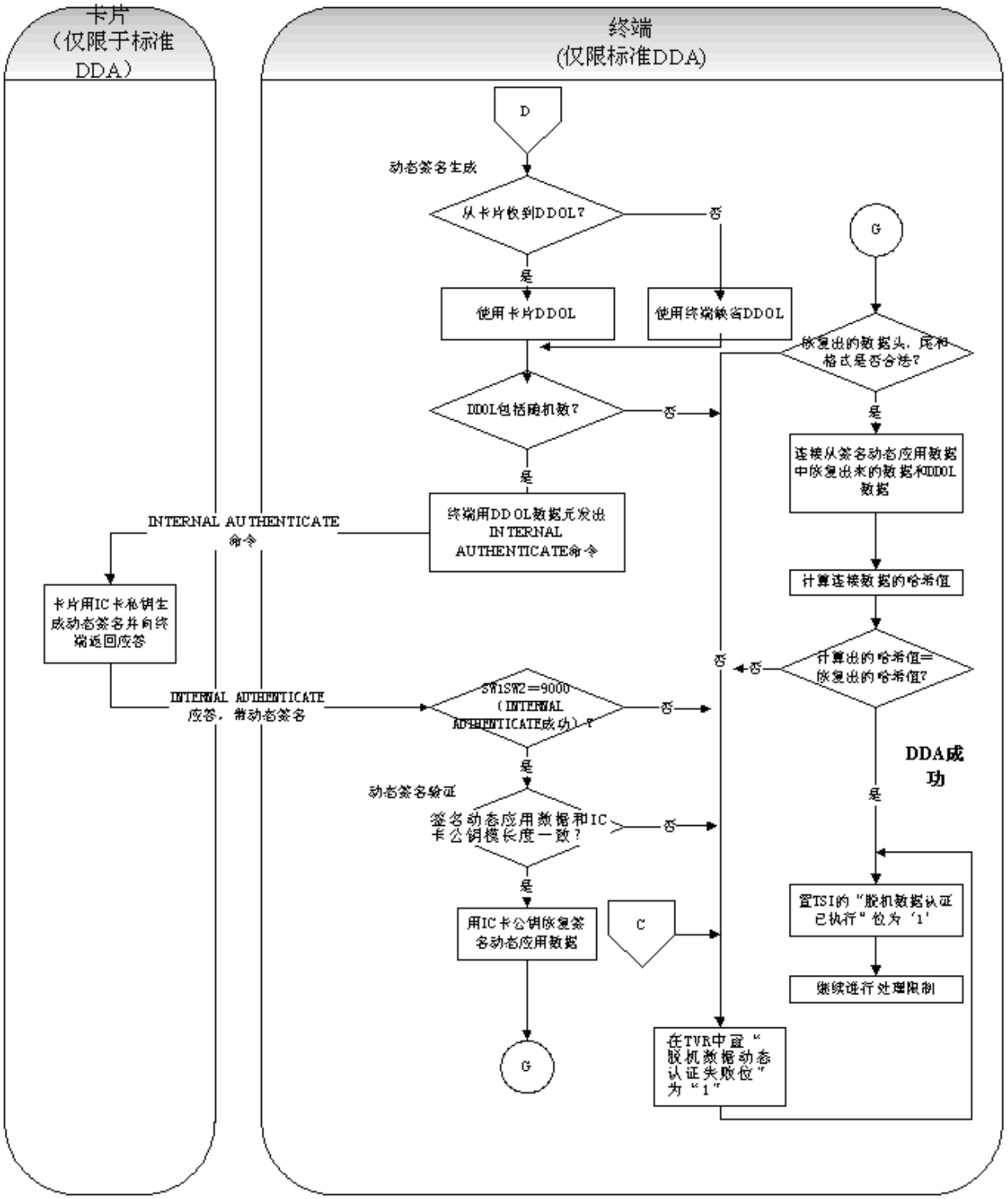

图11　DDA 流程图（3）

7.5.6　复合动态数据认证

CDA的前三个步骤与DDA相同，区别是签名动态应用数据不是通过内部认证（INTERNAL AUTHENTICATE）命令进行，而是通过生成应用密文(GENERATE AC)命令产生，恢复验证时也应比较应用密文。

终端如果判断须执行CDA，则终端作一标记，表明需要执行CDA，在执行完DDA前三个步骤恢复出IC卡公钥后，进行后续交易处理，而CDA的剩下执行过程在对GENERATE AC命令的处理中进行。

终端在收到了GENERATE AC响应之后，如果CDA认证失败，则见JR/T 0025.7中5.3.6的相关规定，终端必须将TVR的“复合动态数据认证/应用密文生成失败”位置“1”。

如果CDA验证失败是发生在第1次GENERATE AC后：

——如果卡片返回 TC，终端应拒绝该交易；

——如果卡片返回 ARQC，终端应立即执行第 2 次 GENERATE AC（AAC）并结束交易。

如果是发生在第2次GENERATE AC后，则终端必须拒绝该交易。

7.5.7 前期相关处理

应用初始化

从卡片中读取AIP，AIP表明卡片是否支持SDA、DDA或CDA。

读应用数据

终端从卡片读取应用数据,其中包括为支持脱机数据认证方法所要求的数据。应用文件定位器(AFL)和静态数据认证标签列表指明了脱机数据认证中用于签名加密并进行哈希值验证的静态数据。

7.5.8 后续相关处理

终端行为分析

在后续的终端行为分析中用到TVR里的“脱机数据认证未执行”、“SDA失败”、“DDA失败”位来决定交易被脱机拒绝还是联机处理。当要求执行CDA时，终端在GENERATE AC命令里设置要求执行CDA指示位。

联机处理

如果要求执行CDA且卡片在第1个GENERATE AC命令中返回ARQC或TC，则终端执行剩下的CDA操作。如果动态签名验证成功，终端继续处理。如果动态签名验证失败且卡片返回的是TC，则终端拒绝交易，并设授权响应码为‘Z1’。

交易结束

如果执行了CDA并且失败，终端作如下处理：

——如果在第 1 个 GENERATE AC 命令中返回 TC，终端脱机拒绝交易；

——如果在第 1 个 GENERATE AC 命令中返回 ARQC，终端发第 2 个 GENERATE AC 命令请求 AAC（表明脱机拒绝交易）。

7.6 处理限制

7.6.1 卡片数据

卡片上与处理限制相关的数据见表15。

表15 处理限制－卡片数据

数据元	描述
应用版本号	该数据元（标签“9F08”）表示卡片中的应用版本，用于终端进行应用版本号的检查
应用用途控制（AUC）	AUC 是可选数据元，表明发卡行设置的有关卡片应用地域以及所允许的交易类型方面的限制。由终端用于应用用途控制检查
发卡行国家代码	发卡行国家代码表示发行卡片的国家，由终端用于应用用途控制检查。见 GB/T 2659，中国的国家代码为“0156”
应用生效日期	应用生效日期是应用被激活使用的日期
应用失效日期	应用失效日期过后，应用即被禁止

7.6.2 终端数据

终端上与处理限制相关的数据说明见表16。

表16 处理限制－终端数据

数据元	描述
应用版本号	该数据元（标签“9F09”）指明终端上的应用版本

数据元	描述
终端国家代码	指明终端所处的国家，用于应用用途控制中对终端进行检查。见 GB/T 2659，中国的国家代码为“0156”
终端验证结果（TVR）	包含根据处理限制结果被设为“1”的位
交易日期	指交易处理所发生的当地（终端中）日期，用于终端进行有效日期和失效日期检查
交易类型	该数据元指明金融交易的类型，按 GB/T 15150 中处理代码的前两位表示，用于终端上应用用途控制检查

7.6.3 应用版本号检查

终端检查终端上的借记/贷记应用版本号与卡片上的应用版本号是否一致。应用版本号由支付系统制定区分遵循不同版本规范的应用。应用版本号为两字节二进制变量。如果终端与卡片上的应用版本号不一样，则终端设置TVR中的“IC卡和终端应用版本不一致”位为‘1’。

7.6.4 应用用途控制检查

AUC为两字节的二进制变量，定义了卡片上应用的交易能够进行的条件。可以限定卡片在哪些区域（国内、国际）、哪些类型终端（ATM、非ATM）、进行哪些类型（取现、返现、商品、服务）的交易。如果卡片中的AUC存在，则终端应进行如下检查：

——如果终端为 ATM，则 AUC 中的“ATM 有效”位必须为‘1’；

——如果终端不是 ATM，则 AUC 中的“在非 ATM 终端上有效”位必须为‘1’；

——如果卡中 AUC 和发卡行国家代码同时存在，则终端须进行表 17 中描述的检查。

表17 应用用途检查时的终端行为

如果交易类型	如果发卡行国家代码	那么应用用途中的位必须有如下设置
交易类型是现金交易	匹配终端国家代码	国内现金交易有效
	不匹配终端国家代码	国际现金交易有效
交易类型是消费(商品或服务)	匹配终端国家代码	国内商品有效和/或国内服务有效
	不匹配终端国家代码	国际商品有效和/或国际服务有效
交易中有返现金额	匹配终端国家代码	允许国内返现
	不匹配终端国家代码	允许国际返现

如果上面的检查有一个失败，终端将TVR中的“卡片不允许所请求的服务”位设为‘1’。

表18 应用用途控制

字节	b8	b7	b6	b5	b4	b3	b2	b1	意义
字节 1	1	x	x	x	x	x	x	x	国内现金交易有效
	x	1	x	x	x	x	x	x	国际现金交易有效
	x	x	1	x	x	x	x	x	国内商品有效
	x	x	x	1	x	x	x	x	国际商品有效
	x	x	x	x	1	x	x	x	国内服务有效
	x	x	x	x	x	1	x	x	国际服务有效
	x	x	x	x	x	x	1	x	ATM 有效
	x	x	x	x	x	x	x	1	在非 ATM 终端上有效
字节 2	1	x	x	x	x	x	x	x	允许国内返现
	x	1	x	x	x	x	x	x	允许国际返现
	x	x	0	x	x	x	x	x	RFU
	x	x	x	0	x	x	x	x	RFU
	x	x	x	x	0	x	x	x	RFU

字节	b8	b7	b6	b5	b4	b3	b2	b1	意义
	x	x	x	x	x	0	x	x	RFU
	x	x	x	x	x	X	0	x	RFU
	x	x	x	x	x	X	x	0	RFU

7.6.5 应用生效日期检查

如果卡片上应用生效日期（标签5F25）存在，则终端应进行应用生效日期检查，通过比较应用生效日期（标签5F25）与当前日期，判断卡片上的应用是否已开始生效。如果卡片上的应用生效日期（标签5F25）晚于终端当前日期，则终端将TVR中的“应用尚未生效”位设为‘1’。

7.6.6 应用失效日期检查

应用失效日期（标签5F24）是卡片上必须存在的数据，因此终端必须进行应用失效日期检查，比较应用失效日期（标签5F24）与当前日期，判断卡片上的应用是否已过期。如果卡片上的应用失效日期（标签5F24）早于终端当前日期，则终端将TVR中的“应用已经失效”位设为‘1’。

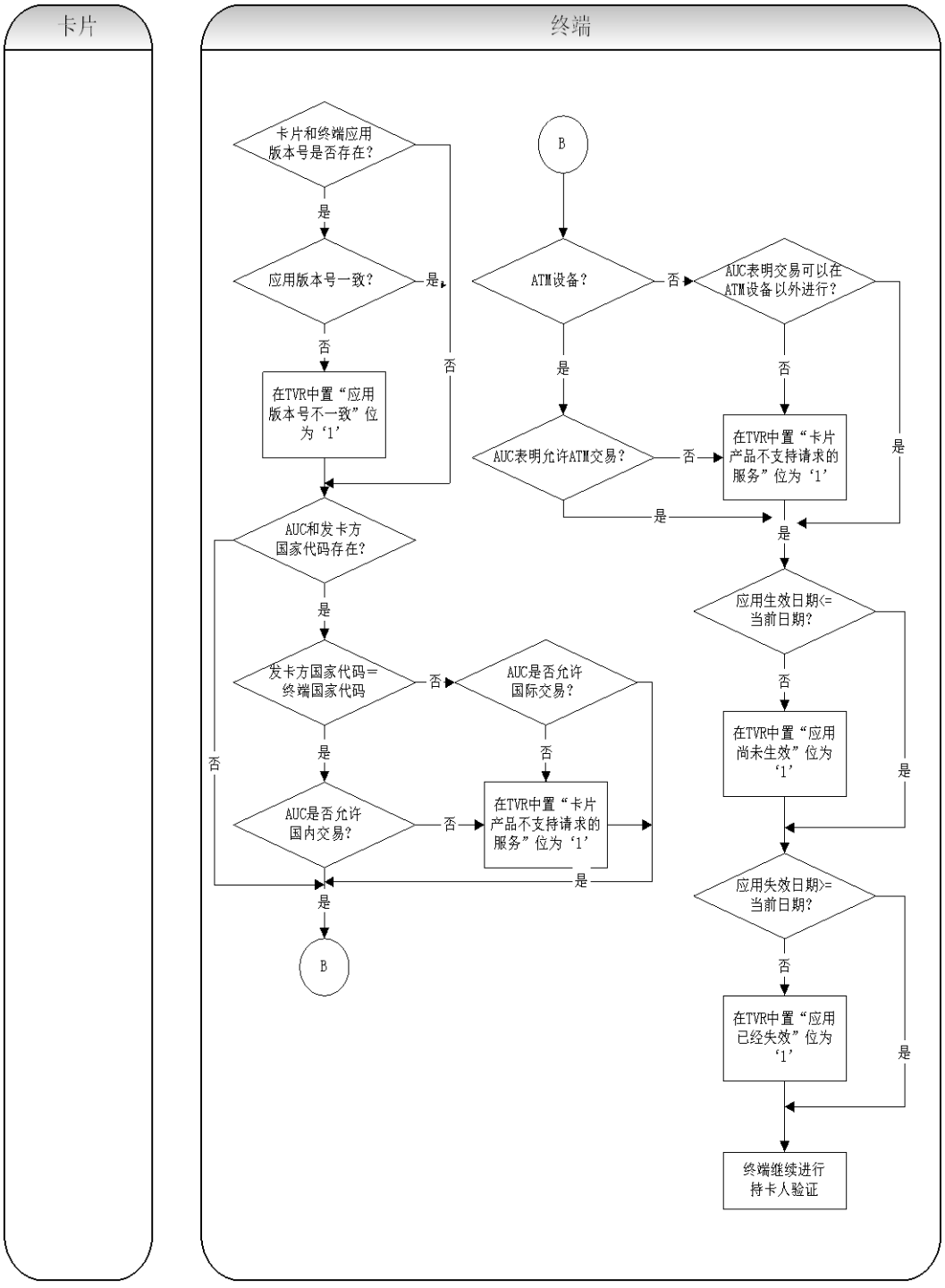

图12　处理限制流程图

7.6.7　前期相关处理

读应用数据

终端使用READ RECORD命令获得应用版本号以及应用失效日期。如果存在应用用途控制、发卡行国家代码和应用生效日期，则它们也从卡片中被读出。

7.6.8 后续相关处理

终端行为分析

终端行为分析中,终端检查发卡行行为代码和终端行为代码以决定如果应用版本不一致、卡未生效、卡已失效、或卡不支持所请求的服务时，必须采取怎样的处理。

7.7 持卡人验证

持卡人验证用来确保持卡人是卡片合法的所有人，卡片不是遗失的或被盗用的。终端通过处理卡片提供的持卡人验证方法（CVM）列表，根据卡片和终端对持卡人验证方法的支持能力，执行相应的持卡人验证方法。

本部分目前支持的持卡人验证方法有：

——脱机明文 PIN 验证；

——联机 PIN 验证；

——签名；

——CVM 失败；

——无需 CVM；

——签名与脱机明文 PIN 验证组合；

——持卡人证件出示。

持卡人验证方法列表中的选择准则可包括交易类型（取现或消费）、交易金额以及终端性能。如果某一CVM失败，持卡人验证方法列表会指示终端下一步的行为。

7.7.1 终端要求

终端为支持持卡人验证必须满足下面的需求：

——密码键盘

如果终端支持联机或脱机PIN验证，则终端应带有内置或外置的密码键盘，以便在交易需要时输入用户识别码(PIN)，并确保密码键盘到加密或验证设备之间密码传输和存储的安全。具体要求见JR/T 0025.7。

——CVM 列表处理

如果卡片支持持卡人验证方法的处理，POS终端应使用CVM列表决定交易所采用的持卡人验证方法。对于ATM，不管在CVM列表里是否支持，ATM应总是能支持联机PIN输入。

——终端显示消息

当PIN输入次数只剩下一次时，终端应显示“最后一次PIN输入”消息，提示持卡人只剩最后一次PIN输入机会，以便持卡人选择退出交易或确认密码正确后再输，避免因误输密码导致锁卡或吞卡。

7.7.2 卡片数据

卡片上与持卡人验证相关的数据见表19。

表19 持卡人验证－卡片数据

<table>
<tr><th>数据元</th><th colspan="2">描述</th></tr>
<tr><td>应用货币代码</td><td colspan="2">用于决定带有金额的 CVM 条件是否满足</td></tr>
<tr><td>应用交互特征（AIP）</td><td colspan="2">包含一个指示位表明卡片是否支持持卡人验证。</td></tr>
<tr><td rowspan="3">持卡人验证方法（CVM）列表</td><td colspan="2">定义了一组有先后处理顺序的持卡人验证方法列表。持卡人验证方法列表包含以下部分：
金额 X—可能在持卡人验证方法使用条件中用到的金额
金额 Y—可能在持卡人验证方法用法条件中用到的第 2 个金额
持卡人验证方法条目—持卡人验证方法列表可能包括不止一个条目，每个条目包含以下子域：</td></tr>
<tr><td>子域</td><td>说明</td></tr>
<tr><td>持卡人验证方法代码</td><td>指定如果 CVM 失败，要采取的行动。可以选择处理下一个持卡人验证方法或持卡人验证处理失败</td></tr>
</table>

数据元	描述	
	持卡人验证方法类型	持卡人验证方法要执行的类型，有： ● 脱机明文 PIN 验证 ● 联机 PIN 验证 ● 签名 ● CVM 失败 ● 无需 CVM ● 签名与脱机明文 PIN 验证组合 ● 持卡人证件出示
	持卡人验证方法条件	执行持卡人验证方法的条件，有： 总是执行 ● 如果交易类型是现金或返现 ● 如果终端支持该 CVM ● 如果交易金额小于 X ● 如果交易金额大于 X ● 如果交易金额小于 Y ● 如果交易金额大于 Y 注： 最后四个条件要求交易货币与卡片中的应用货币相同。

7.7.3 终端数据

终端上与持卡人验证相关的数据说明。

表20 持卡人验证－终端数据

数据元	描述
授权金额	以交易币种为单位的交易金额
持卡人验证方法（CVM）结果	指出最后一个 CVM 执行的结果
加密的 PIN 数据	在联机 PIN 验证时由密码键盘加密的交易 PIN；或在脱机 PIN 验证且密码键盘和读卡器不在同一个防篡改设备中时加密传送的 PIN
密码键盘密钥	用于在脱机明文 PIN 处理过程中通过密码键盘加密键入的 PIN，和用于通过终端解密加密的 PIN。如果终端和密码键盘不在同一个防篡改设备中，该密钥是必须的
终端性能	包含终端对持卡人验证方法支持的指示位
终端验证结果（TVR）	在下面条件下设置在 TVR 中的指示位： ● 持卡人验证不成功 ● 无法识别的 CVM ● PIN 尝试限制超过（在当前和以前的交易） ● PIN 要求输入，但密码键盘没有提供或损坏 ● PIN 要求输入，且提供了密码键盘，但是没有输入 PIN ● 联机 PIN 输入
交易货币代码	交易使用的货币
交易 PIN	由持卡人键入用于 PIN 验证的数字密码
交易状态信息（TSI）	包含一个指示位，当持卡人验证执行后该指示位被置为‘1’

7.7.4 命令

以下命令用于脱机PIN处理：

取数据（GET DATA）

在脱机PIN验证时终端用这条命令从卡片获取“PIN重试计数器”以便决定在先前的交易中“PIN重试上限”是否超过或即将超过。

在取数据（GET DATA）命令的P1、P2参数包含“PIN重试计数器”的标签（“9F17”）。如果卡片返回“9000”，则在响应数据域里包含TLV格式的“PIN重试计数器”值（1字节长）。例如‘9F 17 01 03’，表明还有三次PIN重试机会。如果“PIN重试计数器”不可读，例如在一个私有数据文件内，卡片就返回非“9000”的状态字。这种情况下，终端跳过“PIN重试计数器”检查，继续脱机PIN验证处理。

验证（VERIFY）

该命令用于脱机明文PIN验证。卡片比较交易输入PIN与卡片内部存储的参考PIN是否一致。支持持卡人验证的终端应当支持该命令。

命令中的P2参数应设为‘80’，表明是脱机明文PIN验证。

有效的卡片返回状态有：

——“9000”，交易输入 PIN 与参考 PIN 一致；

——“63Cx”，交易输入 PIN 与参考 PIN 不一致。其中‘x’表示还剩下的 PIN 输入允许次数。“63C0”表明在 VERIFY 命令的处理中超过了“PIN 重试上限”；

——“6983”或“6984”，前一次交易或前一次 VERIFY 命令中超过了“PIN 重试上限”。

7.7.5 处理流程

7.7.5.1 CVM 列表处理

CVM列表处理的目的是终端基于发卡行制定的持卡人验证规则（CVM列表）、终端性能和交易特点来决定交易中使用的CVM。

如果AIP指示卡片支持CVM处理，但卡片中没有CVM列表数据元，终端设置TVR中的“IC卡数据缺少”位为‘1’，不设置TSI中的“持卡人验证已执行”位，并终止持卡人验证过程。

如果卡片应用数据文件中包含CVM列表并且AIP显示卡片支持CVM处理，则终端将执行CVM列表处理。终端按显示在CVM列表中的顺序来处理每个CVM列表入口。

步骤 1：选择 CVM

从CVM列表中的第1个CVM开始，逐个判断CVM执行条件是否成立。如果下面这些条件都成立，则执行该CVM：

——“CVM 条件代码”是终端可理解的；

——条件要求的卡片数据存在。例如 CVM 条件中包含金额检查时“应用货币代码”存在；

——“CVM 条件代码”规定的条件满足。例如如果“CVM 条件代码”为“终端支持该 CVM”，则“终端性能”中应指示支持 CVM 处理。如果条件包括金额判断则“交易货币代码”应与“应用货币代码”相同。

如果上面有一个条件不满足，终端根据“持卡人验证方法代码”决定是否继续下一个CVM处理。

步骤 2：处理 CVM

如果CVM执行的条件满足，终端就处理该CVM。每种CVM的详细处理过程见后面几条的描述。如果终端无法识别该CVM，则在TVR中将“无法识别的CVM”位设为‘1’，并根据“CVM代码”描述的动作进行下一步处理。

步骤 3：CVM 成功

如果CVM执行成功，则持卡人验证完成并成功。

步骤 4：CVM 失败

如果CVM失败，则终端将检查“CVM代码”来确认终端是认为持卡人验证失败或继续下一个CVM处理。

——如果“CVM 代码”指示“CVM 失败”，终端设置 TVR 中的“持卡人验证失败”位为‘1’，完成

持卡人验证处理；

——如果“CVM 代码”指示“应用下一个 CVM”，终端处理下一个 CVM。

步骤 5：CVM 列表处理完毕

如果终端处理到达CVM列表的结尾，则持卡人验证已经失败并且终端设置TVR中“持卡人验证失败”位为‘1’。

步骤 6：持卡人验证完成

下面的条件有一个满足，则认为持卡人验证完成：

——有一个 CVM 处理成功；

——某一 CVM 处理失败且“CVM 代码”指示“CVM 失败”；

——CVM 列表处理完毕。

当CVM列表处理完成时，终端将在交易状态信息（TSI）中设置“持卡人验证已经执行”位为‘1’。CVM列表处理流程图见图13。

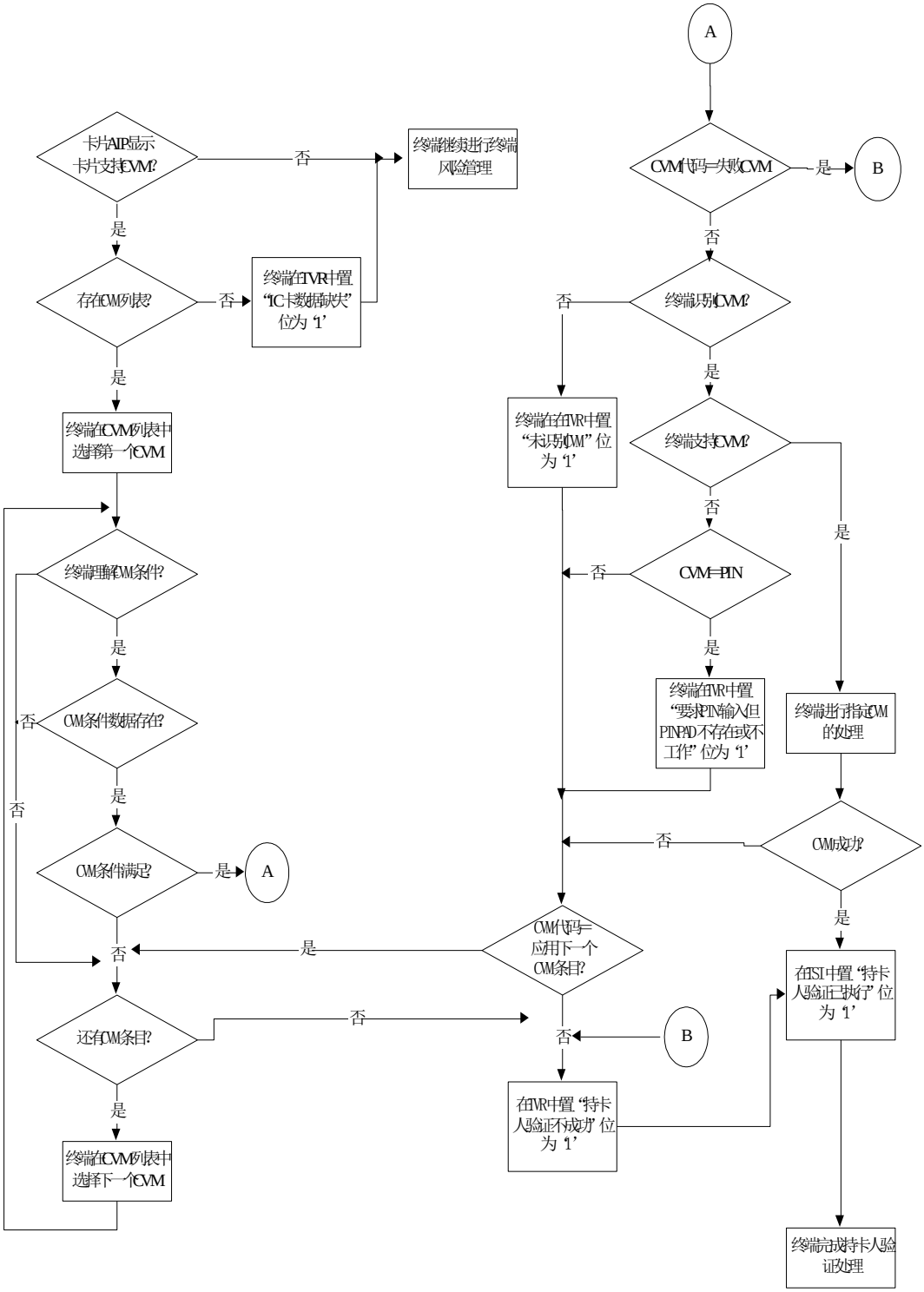

图13　CVM 列表处理流程图

7.7.5.2　脱机明文 PIN 验证

当CVM是脱机明文PIN时，交易PIN用脱机明文PIN直接发送给卡片。当IC卡读卡器和密码键盘分离时，为了PIN安全，终端应该在密码键盘上加密PIN，并且在将PIN发送IC卡读卡器时将PIN解密，然后通过验证（VERIFY）命令送给卡片进行核对比较。

如果终端不支持脱机PIN验证或密码键盘无法正常工作，终端应当：

——设置 TVR 中的“要求输入 PIN，密码键盘没有提供或工作不正常”位为‘1’；

——该 CVM 失败，按“CVM 代码”定义的行为继续处理。

带密码键盘的有服务员终端可以允许在几次不成功的PIN输入验证之前或之后跳过PIN输入，以免一个合法的持卡人在忘记密码的情况下不得不重复输入错误的PIN密码而导致卡片PIN锁住。如果商户或持卡人指示跳过PIN输入，终端应当：

——设置 TVR 中的“要求输入 PIN，有密码键盘，但 PIN 未输入”位为‘1’；

——该 CVM 失败，按“CVM 代码”定义的行为继续处理；

——不设置 TVR 中的“PIN 重试上限超过”位。

当终端决定要求输入脱机PIN，终端应当提示PIN输入，或检查卡片上的“PIN重试计数器”。

步骤 1：检查“PIN 重试计数器”

终端向卡片发送取数据（GET DATA）命令读取“PIN 重试计数器”。卡片返回“PIN 重试计数器”的值或错误响应码。

a)返回错误响应码

如果返回码不是“9000”，表明“PIN重试计数器”是卡片私有数据，终端无法读取。终端应跳过“PIN重试计数器”检查，提示PIN输入。

b)“PIN 重试计数器”为‘0’

如果“PIN 重试计数器”为 0，表明没有剩余的 PIN 输入次数，终端应当：

——不允许脱机 PIN 输入；

——设置 TVR 中的“PIN 重试上限超过”位为‘1’；

——不显示任何有关 PIN 的消息；

——按 CVM 代码中定义的行为继续处理。

c)“PIN 重试计数器”不为‘0’

如果“PIN重试计数器”不为0，表明允许PIN输入，终端提示持卡人输入PIN。如果该值为‘1’，终端还应显示“最后一次机会”。

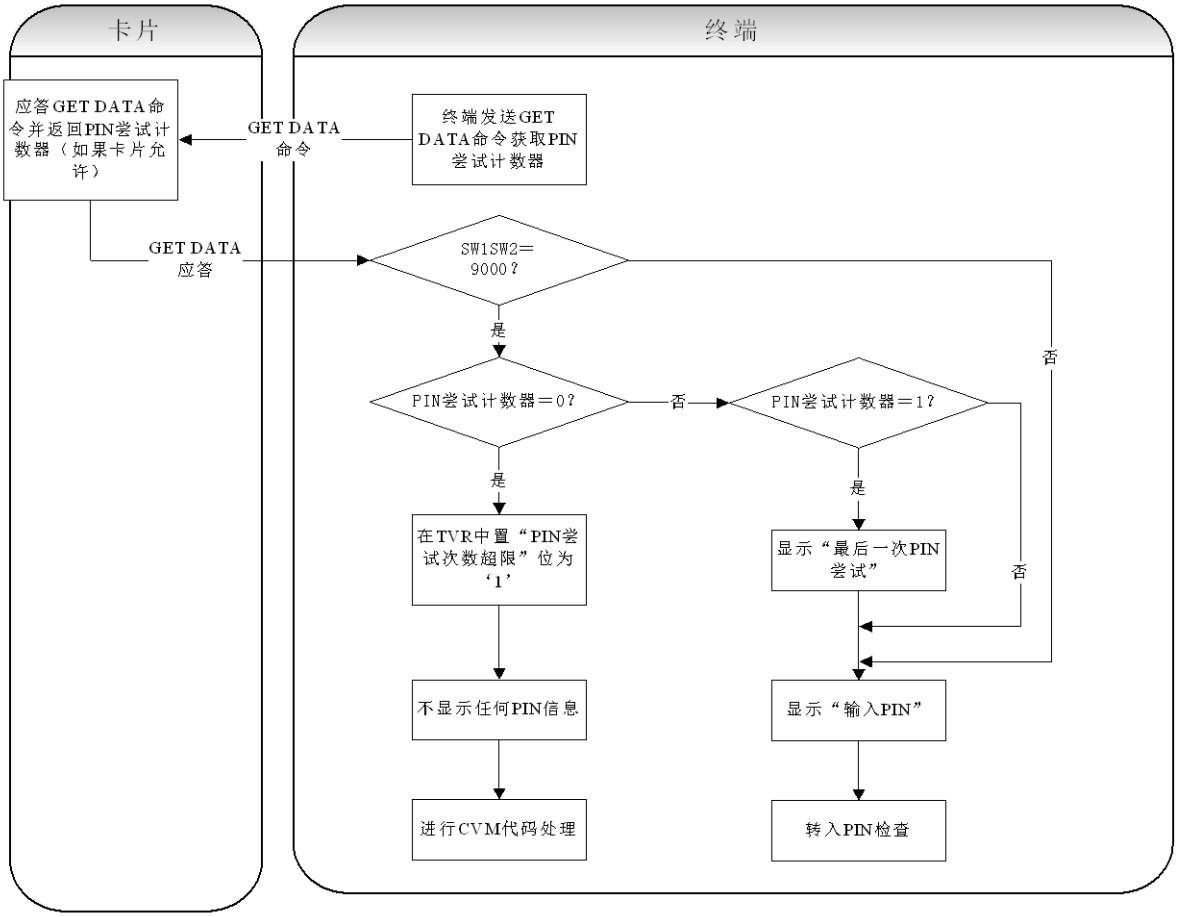

图14 “PIN 重试计数器”检查

步骤 2：加密 PIN

如果读卡器和密码键盘集成在一个安全的防篡改设备中，且脱机明文PIN是被直接从密码键盘传到读卡器。则当CVM是脱机明文PIN验证方法时，不要求对交易PIN加密，明文PIN可直接从密码键盘传送给读卡器。

如果读卡器和密码键盘是分离的两个设备（例如通过RS232串行通讯线连接），或者明文PIN不是直接从密码键盘传到读卡器，则密码键盘应按GB/T 21078.1（或相当的被支付系统批准的其它方式）中要求用保密密钥对交易PIN加密，然后传给读卡器，在读卡器端再用同样的密钥解密，再以明文形式将PIN传给卡片。

步骤 3：用金融 PIN 验证（VERIFY）命令验证 PIN

输入了脱机PIN后，终端通过金融PIN验证（VERIFY）命令将交易PIN送给卡片验证。命令中的P2应设为‘80’，表明是脱机明文PIN验证。

a)PIN 验证（卡片执行）

—— 如果卡片的“PIN 重试计数器”为 0，卡片不进行 PIN 核对，在 VERIFY 命令响应中返回 SW1 SW2 为“6983”或“6984”；

—— 如果交易 PIN 和卡片中的参考 PIN 不一致，卡片将“PIN 重试计数器”减 1，并返回 SW1 SW2 为“63Cx”，其中 x 为剩余的 PIN 重试次数；

—— 如果两个 PIN 一致，卡片复位“PIN 重试计数器”为“PIN 重试上限”，并返回 SW1 SW2 为“9000”。

b)PIN 匹配

如果交易PIN与参考PIN一致（SW1 SW2为“9000”），终端可以显示“密码正确”。

c)上次交易“PIN 重试上限”超过

如果上次交易中“PIN重试上限”超过（SW1 SW2为“6983”或“6984”），终端应：

—— 设置 TVR 中的“PIN 重试上限超过”位为‘1’；

—— 按 CVM 代码定义的行为继续处理。

d)PIN 不匹配

如果PIN不匹配（SW1 SW2为“63Cx”），终端应根据‘x’的值分别处理：

—— 如果 PIN 重试次数为 0，终端应：

- 显示“密码不对”消息；
- 设置 TVR 中的“PIN 重试上限超过”位为‘1’；
- 不再发送 VERIFY 命令给卡片。

—— 如果 PIN 重试次数为不为 0，终端应：

- 显示“密码不对”消息后再显示“输入密码”消息提示输入 PIN；
- 如 PIN 重试剩余次数为 1，终端应在上面的两个消息中间显示“最后一次机会”；
- 输入 PIN 后，应向卡片再次发 VERIFY 命令，重复脱机 PIN 处理。

终端可以允许持卡人或服务员通过按键退出PIN输入，并在终端上显示未输入PIN消息，且脱机明文PIN验证失败。

如果在“PIN重试计数器”减为‘0’之前PIN验证成功，终端应显示“密码正确”消息。

脱机PIN验证处理流程见图15。

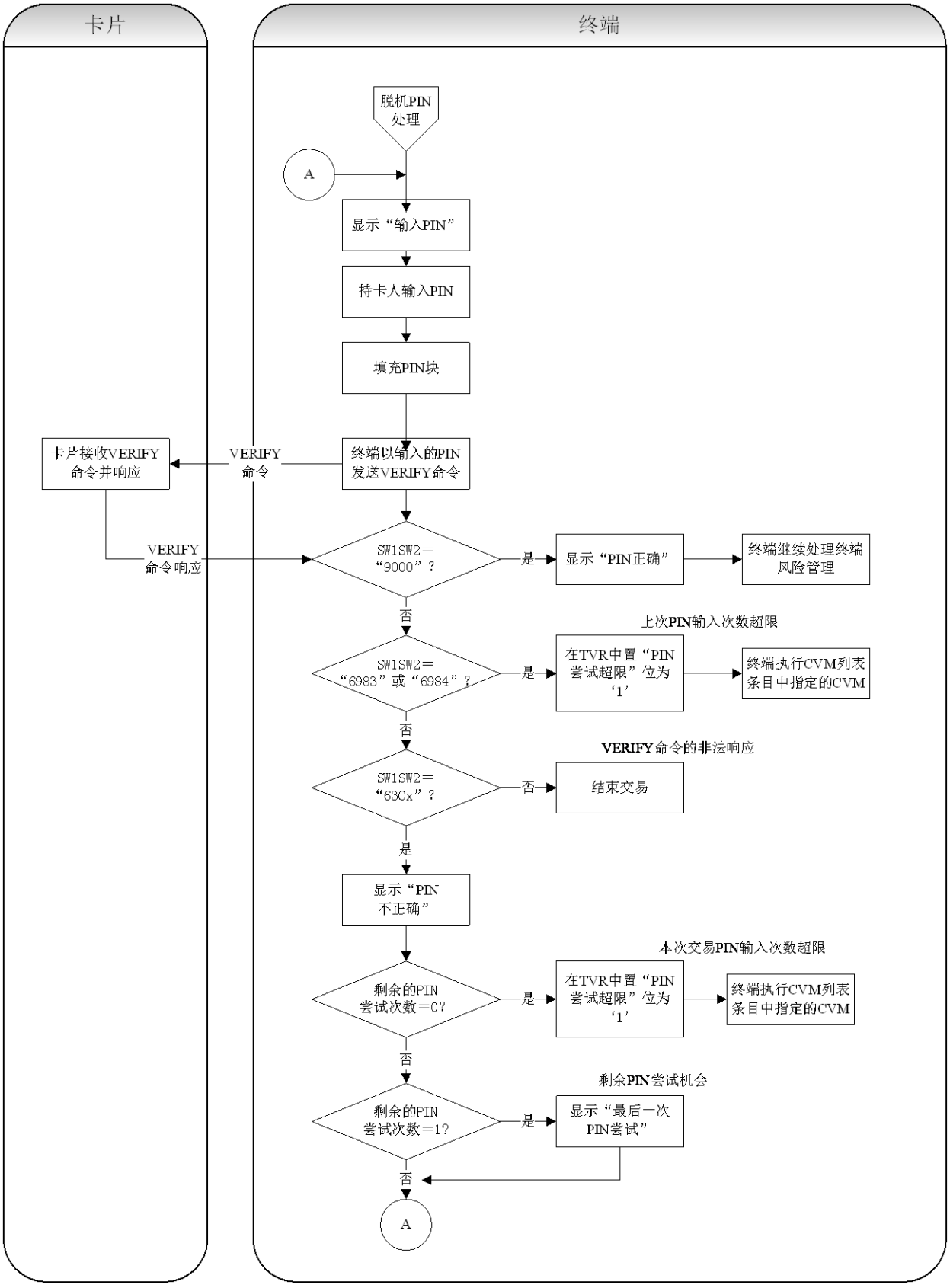

图15　脱机 PIN 验证处理流程图

7.7.5.3　联机 PIN 验证

联机PIN验证按如下过程处理：

——如果终端不支持联机 PIN 验证或密码键盘无法正常工作，终端应当：

- 设置 TVR 中的“要求输入 PIN，密码键盘不存在或无法正常工作”位为‘1’；
- 按“CVM 代码”定义的行为继续处理。

——如果商户或持卡人指示终端跳过 PIN 输入，终端应当：

- 设置 TVR 中的“要求输入 PIN，密码键盘存在，但未输入 PIN”位为‘1’；
- 按“CVM 代码”定义的行为继续处理。

——即使卡片的“PIN 重试上限”超过，终端也应允许输入 PIN 进行联机 PIN 验证；

——如果联机 PIN 成功输入，终端应设置 TVR 中的“输入了联机 PIN”位为‘1’。并认为该 CVM 执行成功。

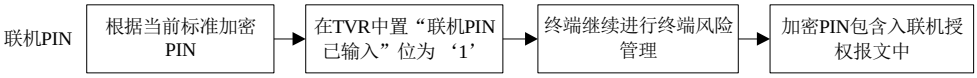

图16　联机 PIN 验证处理

7.7.5.4　签名

当CVM是签名并且终端支持签名操作时，CVM被认为已经执行成功并且持卡人验证完成。在交易结束时，终端将打印带有签名行的凭单，用于给持卡人签名。

如果终端不支持签名处理，应按照“CVM代码”定义的行为继续CVM处理。

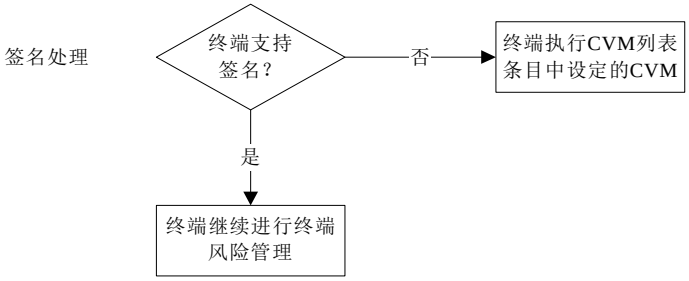

图17　签名处理

7.7.5.5　签名与脱机 PIN 结合验证

如果持卡人验证方法（CVM）由签名和脱机PIN两种方式相结合，则只有这两种方式都成功时该CVM才被认为成功。

7.7.5.6　CVM 失败

当持卡人验证方法（CVM）是“持卡人验证方法（CVM）失败处理”时，持卡人验证方法（CVM）可以被确认为已经失败。

7.7.5.7　无需 CVM

如果持卡人验证方法（CVM）是“无需CVM”，则认为CVM已经执行成功，且CVM完成。

7.7.5.8　持卡人证件出示

终端可通过要求由服务员核对身份证件的方式进行持卡人身份验证。

终端在读应用数据时从卡片中读取持卡人证件类型及号码，然后将证件类型及号码显示在屏幕上，并提示服务员要求持卡人出示相应证件，并比较证件号码与终端显示的号码是否一致，以及证件与持卡人本人是否一致。如果都符合，则持卡人证件验证成功。

7.7.6　前期相关处理

应用初始化

从卡中获取应用交互特征（AIP），表明卡片是否支持持卡人验证。

读取应用数据

终端从卡中读取持卡人验证方法（CVM）列表以及其它持卡人验证处理中使用的数据。

7.7.7 后续相关处理

终端行为分析

终端使用持卡人验证结果，以及发卡行行为代码和终端行为代码来决定交易是被脱机拒绝、联机发送授权请求、还是脱机批准。

卡行为分析

当PIN尝试次数超限时，卡片使用持卡人验证结果与应用缺省行为中的参数来决定是拒绝交易，还是进行请求联机授权。

联机处理

授权请求报文中含有包括脱机PIN验证结果在内的持卡人验证结果，发卡行的授权决定里应该考虑这些结果。联机授权报文里不包括脱机PIN。如果所执行的CVM是联机PIN，则授权请求报文中会包含加密的联机PIN。

发卡行脚本命令处理

PIN更改/解锁（PIN CHANGE/UNBLOCK）命令可以用于重新设置PIN重试次数计数器，使其与PIN重试限制数相等，并改变参考PIN。

应用解锁（APPLICATION UNBLOCK）命令可用来解锁在持卡人验证处理中锁定的应用。

交易结束

联机获取授权的尝试失败后，卡片使用持卡人验证结果和应用缺省行为中的参数来决定是否拒绝交易。

7.8 终端风险管理

7.8.1 卡片数据

卡片上与终端风险管理相关的数据说明见表21。

表21 终端风险管理－卡片数据

数据元	描述
应用主账号（PAN）	终端异常文件检查时使用的有效的持卡人账号
应用交易计数器（ATC）	自应用被放到卡片后卡片对该应用交易的计数，在终端频度检查中用到
上次联机 ATC 寄存器	上次联机交易的交易序号值。如果卡要求终端进行终端频度检查或新卡检查，则该数据元必须提供
连续脱机交易下限	如果终端可以联机，该数据元（标签“9F14”）是发卡行定义的在（有联机能力的终端上）进行交易必须联机之前所允许的最大连续脱机交易笔数。它用于终端频度检查
连续脱机交易上限	该数据元（标签“9F23”）是发卡行定义的在交易必须被拒绝脱机之前所允许的最大连续脱机交易笔数。它用于终端频度检查

7.8.2 终端数据

终端上与终端风险管理相关的数据见表22。

表22 终端风险管理－终端数据

数据元	描述
授权金额	数值型数据元（标签“9F02”），用来存储当前交易的金额（不包括调整）；在最低限额检查中用到
用于偏置随机选择的最大目标百分比	在终端风险管理的随机交易选择联机处理过程中使用到
随机选择的目标百分比	在终端风险管理的随机交易选择联机处理过程中使用到
终端最低限额	该数据元（标签“9F1B”）描述了终端中对应于应用 AID 的最低限额。这个值在最低限额检查和随机交易选择过程中都将使用到
终端验证结果（TVR）	包含用来记录所有终端风险管理的处理结果的一组指示位

数据元	描述
偏置随机选择的阈值	在终端风险管理的随机交易选择联机处理过程中使用到
交易日志	终端上保存已被批准的交易的日志文件，用来防止使用分次消费的方法企图躲过最低限额检查。这个日志至少包含了应用的主账号和交易金额，并可选包含应用主账号序列号和交易日期。而交易数量的储存和日志的维护由具体应用定义。如果该日志存在，则终端最低限额检查将使用到这个日志
交易状态信息（TSI）	概述了交易过程中终端执行的功能。在联机授权和清算报文中，这个数据元不被提供，但是终端用这个数据元说明终端风险管理已被执行

7.8.3 命令

终端用取数据（GET DATA）命令从卡片中获取上次联机应用交易序号寄存器(标签“9F13”)和应用交易计数器（ATC）(标签“9F36”)。

命令的P1和P2参数设置为所要读取的数据的标签。如果成功得到所要读取的数据，卡片返回“9000”。响应数据中包含TLV格式的所要读取的数据。

7.8.4 异常文件检查

如果终端异常文件存在，则终端检查应用主账号是否在异常文件列表中。如果卡片出现在异常文件中，终端将TVR中的“卡片出现在终端异常文件中”位置为‘1’。

7.8.5 商户强制交易联机

对可以联机的终端，商户可以将当前交易强制为联机处理。如果商户强制交易联机，终端将TVR中“商户强制交易联机”位设置成“1”。

7.8.6 最低限额

最低限额用于控制交易当前交易金额或同一张卡片连续几笔交易累积金额超过某个数值时则要求联机授权。

如果终端不支持交易日志，则终端直接比较授权金额和最低限额。如果交易授权金额大于或等于最低限额，终端将TVR中的“交易超过最低限额”位设为‘1’。即使最低限额为0，终端也进行同样检查，这种情况会导致所有交易的TVR中的“交易超过最低限额”位都设为‘1’。

如果终端支持交易日志，则终端在交易日志中寻找与当前交易的PAN和PAN序列号（如果终端交易日志和卡片中都存在）相同的一个交易记录，将其对应的累计交易金额与当前交易的授权金额相加，如果和大于或等于最低限额，则TVR中的“交易超过最低限额”位设为‘1’。

7.8.7 随机交易选择

控制交易基于当前交易的金额随机决定交易是否联机授权，终端可选支持该功能。如果终端支持随机交易选择，则终端必须具有如下数据：最低限额、偏置随机选择阈值、随机选择目标百分数和偏置随机选择的最大目标百分数。此外，终端还应产生位于1－99之间的一个随机数。

任何交易金额小于偏置随机选择阈值的交易需要进行随机选择，而不管交易的金额具体为多少。终端会产生一个1－99之间的随机数，如果此随机数小于或等于随机选择的目标百分数，该交易就会被选中。

任何交易金额大于偏置随机选择阈值而小于最低限额的交易需要进行偏置随机选择，有倾向性地使高额交易有更高的几率通过联机处理完成。对于这些交易，终端需要把它产生的随机数字与支付系统的交易目标百分数进行比较，如果随机数小于或等于交易目标百分数，交易就被选中。交易目标百分数是支付系统的目标百分数的线性插值(即随机选择的目标百分数与偏置随机选择使用的最大目标百分数的线性插值)，其计算方法如下：

插值因子=(授权金额-阈值)/(最低限额-阈值)

交易目标百分比=((最大目标百分比-目标百分比)×插值因子)+目标百分比

如果交易在上述的过程中被选中，则将TVR中的“交易被随机选中进行联机处理”位设为‘1’。

表23　终端风险管理参数示例

参数	值
终端最低限额	100
终端随机数	25
偏置随机选择的阈值	40
随机选择目标百分比	20%
偏置随机选择的最大目标百分比	50%

情形1：

交易金额是20。因为交易金额小于偏置随机选择阈值，因此执行随机选择。

比较终端随机数与目标百分数。因为随机数（25）大于目标百分数（20），所以交易不被选中作联机处理。

情形2：

交易金额是60。这个金额大于偏置随机选择的阈值，但小于终端最低限额。因此应用偏置随机选择。

交易金额比阈值高20，该差值是终端最低限额与阈值差值（100－40＝60）的1/3。因此将最大目标百分数与目标百分数的差值的1/3（50%－20%＝30%×1/3＝10%）加到目标百分数上，得到交易目标百分数为30%（20%＋10%＝30%）。

终端随机数为25，小于交易目标百分数（30），所以交易被选中进行联机处理。

情形3：

交易金额为150。因该金额大于终端最低限额，因此交易不进行随机选择。而是进行最低限额检查而联机处理。

7.8.8　频度检查

支持脱机交易的联机终端必须支持频度检查，要求卡片在连续脱机交易一定次数后要求进行一次联机交易。处理过程如下：

如果连续脱机交易次数下限（LCOL，标签“9F14”）和连续脱机交易次数上限（UCOL，标签“9F23”）都存在（在读应用数据阶段从卡片读到），终端应执行频度检查。如果LCOL、UCOL不存在，则终端跳过频度检查。

终端向卡片分别发送取数据（GET DATA）命令请求上次联机ATC寄存器和ATC，卡片在命令响应中返回这些数据。

如果无法用取数据（GET DATA）命令从IC卡中得到这两个数据对象，终端应把TVR中的“超过连续脱机交易下限”和“超过连续脱机交易上限”位都设为‘1’，并结束频度检查。

如果成功得到上次联机ATC寄存器和ATC，终端作如下处理：

——如果 ATC 减去上次联机 ATC 寄存器的差值大于连续脱机交易次数下限，终端将 TVR 中的“超过连续脱机交易次数下限”位设为‘1’；

——如果 ATC 减去上次联机 ATC 寄存器的差值大于连续脱机交易次数上限，终端将 TVR 中的“超过连续脱机交易次数上限”位设为‘1’。

7.8.9　新卡检查

执行频度检查的终端也应执行新卡检查，如果上次联机ATC寄存器值为0，则终端将TVR中的“新卡”位置‘1’。对第1次使用的卡片设置TVR中相应标志，要求交易联机处理。如果取数据（GET DATA）命令未能取回上次联机ATC寄存器的值，则不能置TVR中的“新卡”位为‘1’。

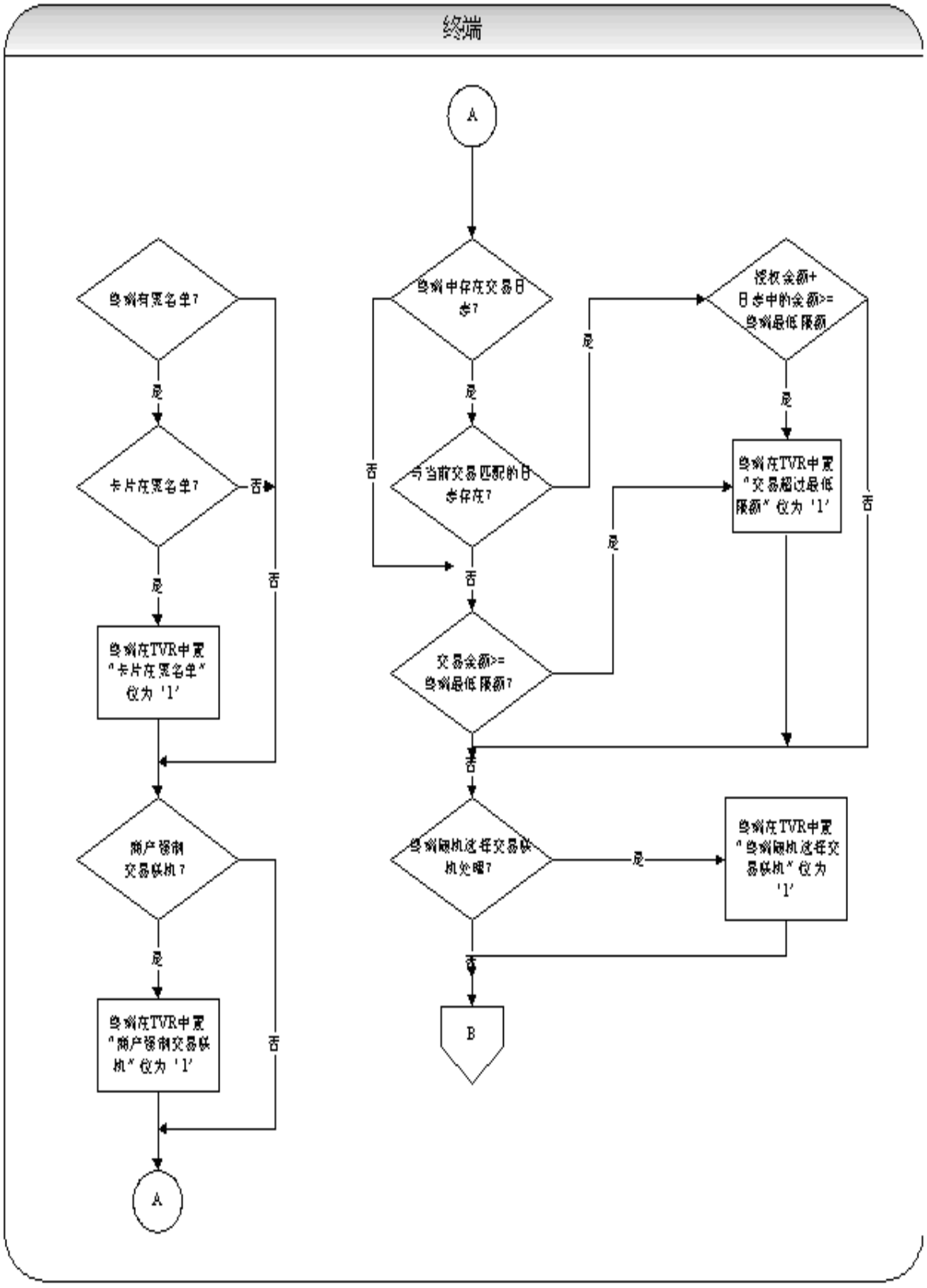

图18　终端风险管理处理流程（1）

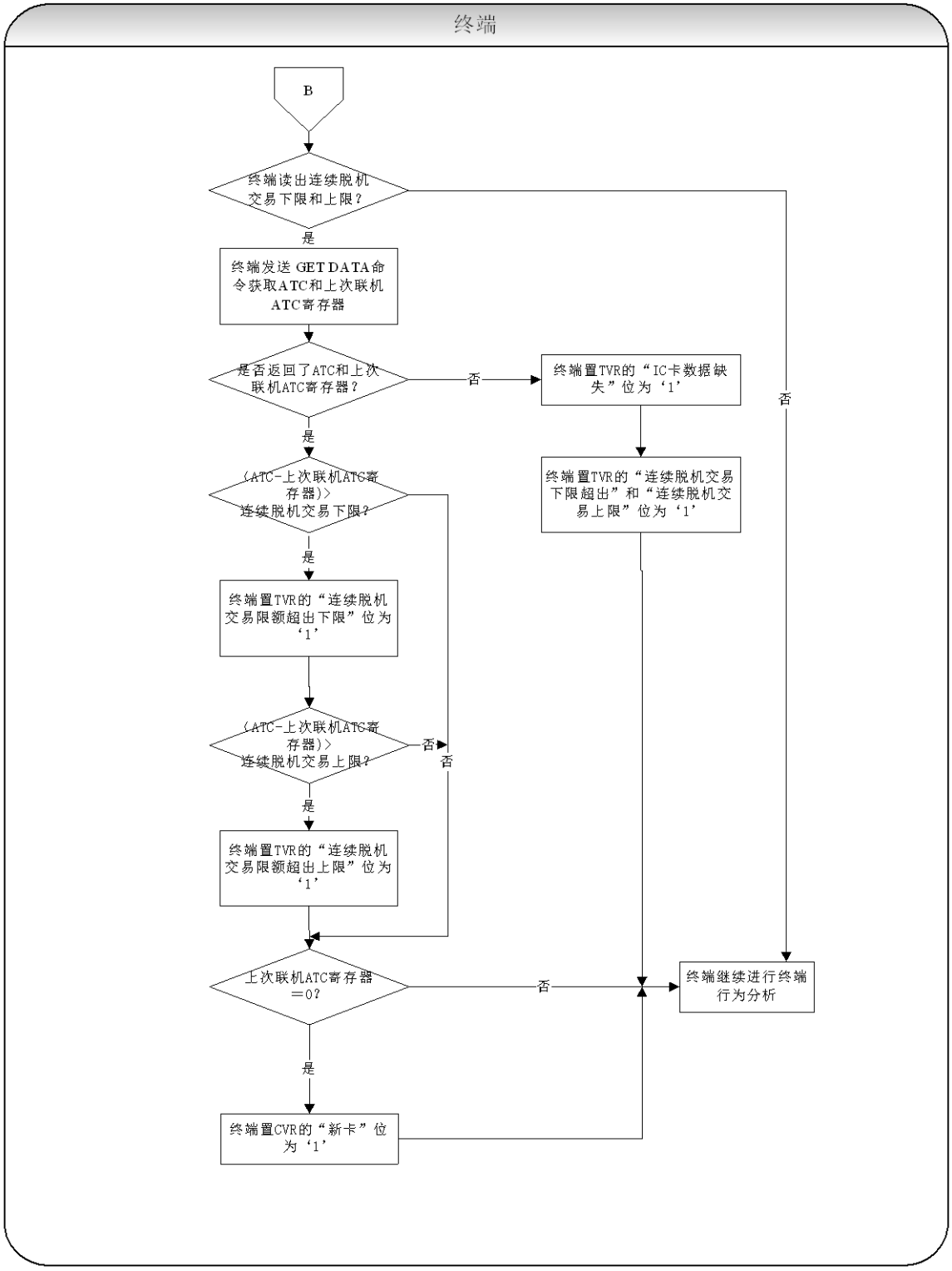

图19　终端风险管理处理流程（2）

7.8.10　前期相关处理

读应用数据

下列数据从卡中读取：

——主账号用于检查终端异常文件；

——如果卡上存在连续脱机交易上限值和下限值，它们用于终端频度检查。

7.8.11 后续相关处理

终端行为分析

终端根据卡和终端的设置来决定如果出现下列情况采取怎样的行动：

——卡片出现在终端异常文件中；

——商户强制交易联机；

——交易超过最低限额；

——交易被随机选择进行联机处理；

——频度检查交易笔数超限；

——新卡。

7.9 终端行为分析

在终端行为分析过程中，终端分别应用发卡行在卡片中和收单行在终端中设定的规则，判断脱机处理的结果，以决定交易是否可以脱机批准、脱机拒绝或者联机索取授权。

终端行为分析包括两个步骤：

——检查脱机处理结果－终端检查 TVR 中的脱机处理结果，以决定交易是否脱机批准、脱机拒绝或者请求联机授权。本过程终端需要将 TVR 与由发卡行设定在卡片中的规则－发卡行行为代码（IAC）和收单行设定在终端中的规则－终端行为代码（TAC）进行比较；

——请求密文处理－终端根据第 1 步的判断结果向卡片请求相应的应用密文。

7.9.1 卡片数据

终端行为分析过程中涉及如表24中的卡片数据。

表24 终端行为分析－卡片数据

数据元	描述
发卡行行为代码（IAC）	发卡行行为代码有三个数据元，即发卡行行为代码-拒绝、发卡行行为代码-联机、发卡行行为代码-缺省。每个发卡行行为代码由一组与终端验证结果（TVR）中的位相对应的位组成 • IAC－拒绝位设置为“1”反映了交易被脱机拒绝的终端验证结果条件 • IAC－联机位设置为“1”代表需要联机授权条件 • IAC－缺省位设置为“1”是当联机处理不可行时脱机拒绝所需的条件

7.9.2 终端数据

终端行为分析涉及终端数据见表25。相关数据的定义见8.1。

表25 终端行为分析－终端数据

数据元	描述
授权响应码	两字节 ASCII 码，表示终端对交易的判断结果。
终端行为代码(TAC)	TAC 有三个数据元，它们都是由一系列的位组成的，这些位对应于 TVR 中的数据位。分别为： ● TAC－拒绝 收单行设置的能够导致交易脱机拒绝的 TVR 条件位 ● TAC－联机 收单行设置的能够导致交易联机的 TVR 条件位 ● TAC－缺省 收单行设置的在交易联机无法进行的情况下能够导致脱机拒绝的 TVR 条件位
终端验证结果 TVR	TVR 是在交易处理过程中被设置的一系列数据位，这些数据位表示从终端角度看到的交易处理状态

7.9.3 处理流程

对脱机处理结果的检查一般在终端风险管理之前进行，但为了避免不必要的冗余处理，此过程亦可提前。例如，终端行为分析可以在静态数据认证（SDA）失败后立即进行，以避免不必要的持卡人验证过程。

检查过程完全由终端利用先前从卡片获取的IAC数据和终端保存的TAC数据进行，无需与其它设备进行交互处理。

在处理过程中，终端比较IAC和TAC中与终端验证结果（TVR）对应的位。如果TVR和IAC或TAC中相应的位都被设置为“1”，则采纳对应的IAC或TAC。示例如下：

示例：IAC 用法示例

发卡行希望在脱机动态数据认证失败或者 PIN 输入次数超限时脱机拒绝交易，所以卡片中的 IAC－拒绝数据置位如下：

脱机 DDA 失败　　PIN 输入超限

| |

IAC－拒绝　00001000 00000000 00100000 00000000 00000000

交易 1：应用过期，TVR 如下：

应用过期

|

TVR－　　00000000 01000000 00000000 00000000 00000000

IAC－拒绝 00001000 00000000 00100000 00000000 00000000

由于 TVR 和 IAC－拒绝没有任何对应位同时置为‘1’，不采用脱机拒绝。

交易 2：脱机 DDA 失败且应用过期，所以 TVR 的设置如下：

脱机 DDA 失败 应用过期

| |

TVR－ 00001000 01000000 00000000 00000000 00000000

IAC－拒绝 00001000 00000000 00100000 00000000 00000000

由于 TVR 和 IAC－拒绝的脱机 DDA 失败位都被置为‘1’，脱机拒绝被采纳。

对其它的 IAC 和 TAC 也要进行类似的比较。

终端的处理步骤如下：

步骤 1：终端比较 IAC－拒绝和 TVR。如果不存在 IAC－拒绝，则采用缺省值‘0000000000’。如果 IAC－拒绝和 TVR 的任何对应位同时设为‘1’，终端必须：

——把授权响应码置为‘Z1’(脱机拒绝)；

——把 GENERATE AC（产生应用密文）命令的 P1 参数设为请求应用认证密文（AAC）；

——进行请求应用密文步骤。

步骤 2：终端对 TAC－拒绝和 TVR 进行类似的比较。如果不存在 TAC－拒绝，则采用缺省值‘0000000000’。如果 TAC－拒绝和 TVR 的任何对应位同时设为‘1’，终端必须采取与 IAC－拒绝相同的处理。

步骤 3：如果终端具有联机处理能力（仅联机的终端除外），则它应该使用 IAC－联机和 TAC－联机与 TVR 比较。如果 IAC－联机不存在，则使用缺省值‘FFFFFFFFFF’，如果 TAC－联机不存在，则使用缺省值‘0000000000’。如果 IAC－联机和 TVR 的任何对应位同时置为‘1’，则终端：

——把产生应用密文（GENERATE AC）命令的 P1 参数设为授权请求密文（ARQC），以进行联机授权

请求；

——进行请求应用密文步骤。

对于仅联机的终端，如果在步骤 1 和步骤 2 中未决定脱机拒绝，则终端不必进行 IAC－联机和 TAC－联机与 TVR 的比较，而直接按照 IAC－联机或 TAC－联机和 TVR 的任何对应位同时置为‘1’的情况来处理，通过请求联机来继续进行交易。

步骤 4：如果终端是仅脱机终端或者当有联机处理能力的终端出于某种原因不能联机时，则使用 IAC-缺省和 TAC-缺省与 TVR 比较。如果没有 IAC－缺省，则使用缺省值‘FFFFFFFFFF’，如果 TAC-缺省不存在，则使用缺省值‘0000000000’。如果比较结果的任何对应位同时为‘1’，则终端：

——把授权响应码置为‘Z3’（不能联机，脱机拒绝），仅脱机终端授权响应码置为‘Z1’；

——把产生应用密文（GENERATE AC）命令的的 P1 参数设置为请求 AAC；

——进行请求应用密文步骤。

对于仅联机的终端，当无法进行联机时，它可以选择正常的处理TAC/IAC－缺省，也可以选择跳过TAC/IAC-缺省的处理。对于跳过TAC/IAC-缺省处理的终端应该直接按照TAC/IAC-缺省与TVR匹配进行处理，并且在第2个GENERATE AC请求AAC。对于正常处理TAC/IAC-缺省的终端，应该根据TAC/IAC-缺省与TVR匹配的结果生成应用密文，这时仅联机的终端可能脱机完成交易。

步骤 5：如果在以上的比较中没有出现对应位同时为‘1’的情况，则终端：

——把授权响应码置为‘Y1’（脱机批准）；

——把 GENERATE AC（请求应用密文）命令的 P1 参数设置为请求交易证书（TC）；

——进行请求应用密文步骤。

生成应用密文（GENERATE AC）

终端比较IAC、TAC和TVR之后，根据比较的结果，向IC卡发送第1次GENERATE AC命令，请求适当的密文。如果需要进行复合动态数据认证（CDA），终端在GENERATE AC命令的P1参数中说明见JR/T 0025.5的附录B.6章中的表B.6和表B.7。

图20是终端行为分析的处理流程图。

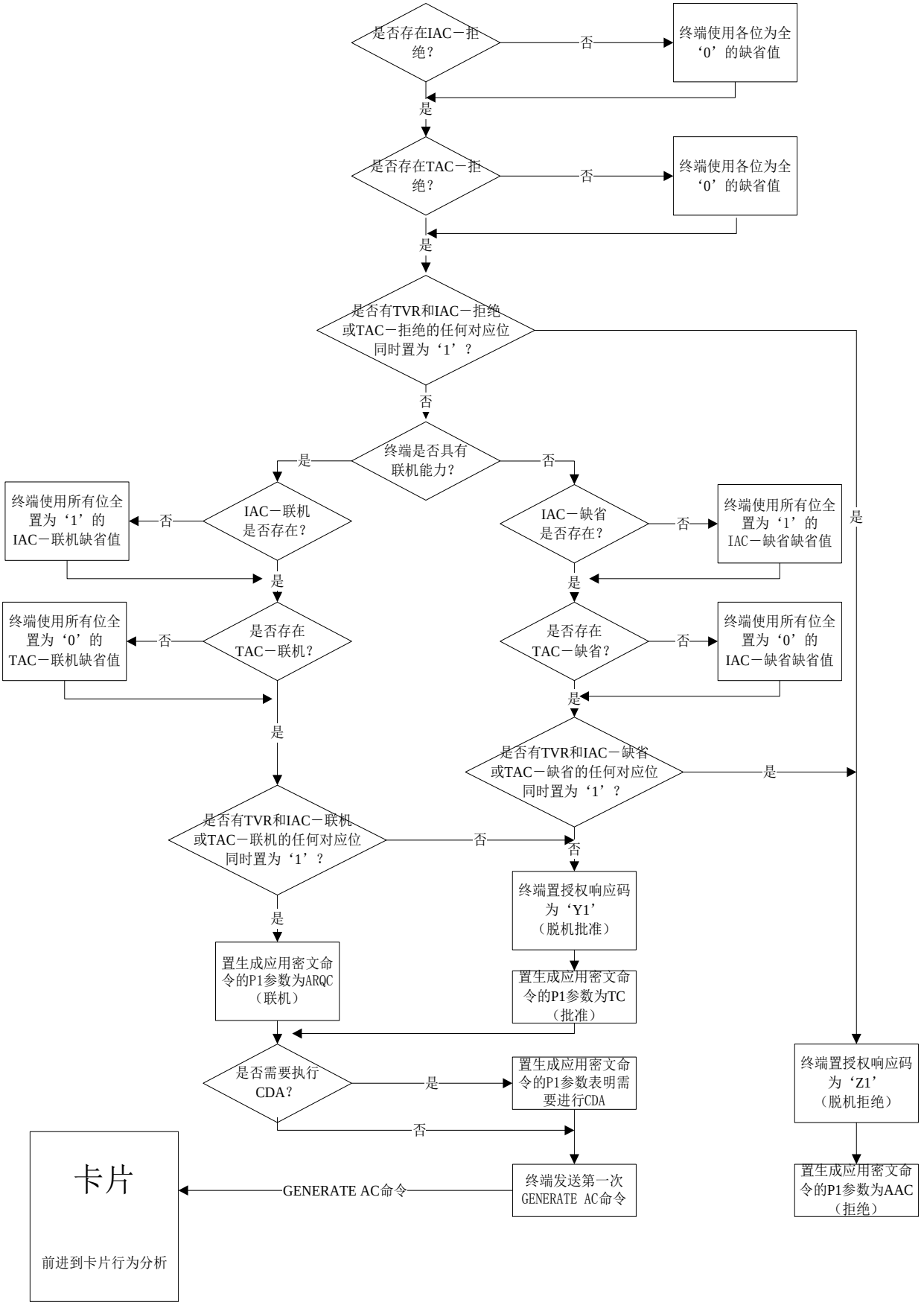

图20　终端行为分析处理流程图

7.9.4 前期相关处理

读取应用数据

终端从卡片读取应用数据。此数据包括卡片风险管理数据对象列表1（CDOL1）和发卡行行为代码（IAC）。

脱机数据认证、约束处理、持卡人验证及终端风险管理

根据处理结果，这些脱机功能在终端验证结果（TVR）中设置相应的位。终端行为分析中，通过将TVR与发卡行行为代码（IAC）和终端行为代码（TAC）相应的位进行比较来决定交易处理。

在脱机数据认证过程中，终端决定是否进行复合动态数据认证（CDA）。如果要进行CDA，终端保存这一信息，以便正确设置第1次GENERATE AC命令中的引用控制参数。

7.9.5 后续相关处理

卡片行为分析

卡片行为分析中，卡片执行附加的风险管理来决定是否同意终端在终端行为分析中脱机批准或请求联机的决定。

7.10 卡片行为分析

卡片行为分析允许发卡行进行卡片内部的风险管理，如频度检查等。本步骤的风险管理内容包括：

——检查上次交易行为；

——新卡检查；

——频度计数器检查。

卡片行为分析应按照JR/T 0025.5的第14章的规定进行。

7.10.1 卡片数据

以下是卡片上与卡片行为分析相关的数据说明。这些数据的描述见JR/T 0025.5的附录A.1的描述。

表26 卡片行为分析－卡片数据

数据元	描述
卡风险管理数据对象列表中要求的数据（CDOL1）	表明卡片在第 1 个 GENERATE AC 命令中需要从终端获得的数据列表
应用密文	卡片响应 GENERATE AC 命令而返回的密文 返回表示拒绝交易的应用认证密文，称为 AAC 返回表示批准交易的交易证书，称为 TC 指示交易联机处理的授权请求密文，称为 ARQC
应用交易计数器（ATC）	卡片中的应用交易计数序号
密文信息数据（CID）	包括： 卡片返回的应用密文类型 ——TC ——ARQC ——AAC 及其它卡片的信息如：服务不允许，需要通知消息等
发卡行应用数据	卡片通过终端发送给发卡行的私有交易应用数据，包括 CVR，具体描述见 JR/T 0025.5 附录 A.1
卡片验证结果（CVR）	根据本次和上次交易脱机处理结果进行设置的验证结果指示符

7.10.2 终端数据

CDOL1所要求的终端数据。

7.10.3 命令

卡片在卡片行为分析的最后向终端返回GENERATE AC命令的响应数据，其中包括上表中提及的数据。GENERATE AC命令的细节见JR/T 0025.5。本命令的参数P1－引用控制参数－表明是否执行复合动态数据认证（CDA）。

7.10.4 处理流程

7.10.4.1 终端对卡片分析结果的处理

终端对交易结果的判断不是最终的，还要通过GENERATE AC命令得到卡片对交易的评估结果。终端根据终端判断结果请求对应的交易应用密文（AC），并按卡风险管理数据对象列表1（CDOL1）向卡发送交易数据。卡片根据交易数据和终端判断结果，进行卡片验证过程，对交易结果作出判断，并返回对应交易应用密文。卡片的验证过程和应用密文的计算见JR/T 0025.5。

根据终端请求的不同密文，卡片可能返回的处理结果见表27。

表27 卡片响应密文类型

		卡片响应		
		AAC	ARQC	TC
终端请求	AAC	拒绝	—	—
	ARQC	拒绝	联机	—
	TC	拒绝	联机	批准

如果CDOL1中包含交易证书数据对象列表（TDOL），则终端应对TDOL进行处理，并计算出哈希结果。如果卡片中没有TDOL数据，则使用终端上缺省为空的TDOL进行计算。

7.10.4.2 复合动态数据认证

如果交易要求进行复合动态数据认证（CDA），且卡片决定返回TC或ARQC，则在GENERATE AC命令返回签名数据后终端要进行CDA处理。

7.10.5 前期相关处理

读取应用数据

终端从卡片读取卡片风险管理数据对象列表1（CDOL1）。

终端行为分析

终端根据终端行为分析的结果向卡片请求相应的应用密文并向卡片提供其在CDOL1中请求的终端数据。

7.10.6 后续相关处理

联机处理

如果卡片返回ARQC，终端则向主机发送联机报文，报文中包括ARQC。

交易结束

如果要求联机处理，但终端无法联机发送报文，则执行附加的终端和卡片处理。

终端用发卡行行为码IAC-缺省和终端行为码TAC-缺省来执行附加分析（类似终端行为分析）以决定在第2个GENERATE AC命令中要求的密文类型（AAC或TC）。

7.11 联机处理

联机处理使得发卡行后台可以根据基于后台的风险管理参数检查并授权批准或拒绝交易。除了传统的联机欺诈和信用检查外，发卡行后台授权系统还可以使用卡片生成的动态密文进行联机卡片认证并在授权决策中考虑脱机处理的结果。

发卡行的返回数据中可以包括对卡片的发行后更新命令和发卡行生成的密文，该密文可以用于卡片对发卡行的合法性进行认证，这一过程称为发卡行认证。

7.11.1 卡片数据

从卡片返回的GENERATE AC命令响应数据按JR/T 0025.5的附录B.6.4响应报文的数据域中所描述的格式1或格式2编码。

如果响应数据为格式1，则值域包含表28所列的数据。

表28　联机处理－第 1 个 GENERATE AC 响应数据

数据元	描述
密文信息数据（CID）	包含表明卡片返回密文类型的指示符，最高两位为‘10’表示返回的是 ARQC
应用交易计数器（ATC）	应用置入卡片以来执行的交易总数计数器
应用密文（AC）	8 字节密文值
发卡行应用数据	包含需要向发卡行发送的发卡行私有数据

如果响应数据为格式2，则返回数据数据是包含在标签‘77’中的BER-TLV编码格式的数据。如果格式2响应数据中包含签名动态应用数据（标签“9F4B”），则应用密文也被包含在动态签名中。见JR/T 0025.7的5.3.6。

联机处理用到的其它卡片数据见表29。

表29　联机处理－其它卡片数据

数据元	描述
应用交互特征（AIP）	AIP 包含指示卡片是否支持发卡行认证的位

7.11.2　终端数据

联机处理中发卡行认证用到的终端数据见表30。

表30　联机处理－终端数据

数据元	描述
终端验证结果(TVR)	当发卡行认证失败时，其中相应位将置为 1
交易状态信息(TSI)	当发卡行认证执行过后，其中相应位置为 1

发卡行经由收单行返回给终端的数据见表31。

表31　新的发卡行联机返回数据

数据元	描述
发卡行认证数据	包括以下子项： —— 授权响应密文（ARPC）：由发卡行主机系统产生的密文 —— 授权响应码：在产生 ARPC 时用到的响应码
发卡行脚本	由发卡行发送给卡片的命令数据，用于更新卡片数据

上表中的授权响应码由发卡行在联机处理中生成，并用于计算授权响应密文（ARPC）。授权响应码在从发卡行传输到终端的过程中不应被改变。终端将其作为发卡行认证数据的一部分传送给卡片。

7.11.3　命令

联机处理过程中使用生成应用密文(GENERATE AC)命令的响应及外部认证(EXTERNAL AUTHENTICATE)命令和响应。

在发送联机请求之前，终端首先从卡片接收GENERATE AC命令的响应。只有卡片在GENERATE AC命令的响应中返回ARQC，终端才需要进行联机处理。该命令的描述见JR/T 0025.5中附录B.6。

如果收到联机响应以后需要进行发卡行认证，则终端必须向卡片发送外部认证（EXTERNAL AUTHENTICATE）命令进行发卡行认证。

本命令的具体描述见JR/T 0025.5中附录B.5。

如果发卡行认证成功，卡片返回SW1 SW2 “9000”。

7.11.4　处理流程

联机处理包括联机请求处理、联机响应处理以及可能的发卡行认证处理。

7.11.4.1　联机请求

接收到第1次GENERATE AC命令的响应之后，终端或者执行标准的联机处理过程，如果在脱机数据认证中要求执行CDA，则进行复合动态数据认证（CDA）处理。

7.11.4.1.1 复合动态数据认证处理

如果 IC 卡响应 AAC，那么终端不认为复合动态数据认证（CDA）失败，拒绝交易。

如果 IC 卡响应 TC 或 ARQC，那么终端执行以下步骤。

步骤 1：如果签名的动态应用数据的长度不同于 IC 卡公钥模的长度，那么复合动态数据认证（CDA）失败；

步骤 2：用 IC 卡公钥解开动态签名（签名动态应用数据），恢复出签名中的数据；

步骤 3：检查恢复数据的头、尾、数据格式是否正确；

步骤 4：检查解开的密文信息数据和 GENERATE AC 命令响应中接收到未加密的密文信息数据是否一致；

步骤 5：将不可预知数加在恢复数据后面，计算哈希结果，并与恢复出的哈希值比较是否一致；

步骤 6：将 PDOL 数据，CDOL1 数据和 GENERATE AC 命令返回数据（动态签名除外）连在一起计算哈希结果，与从动态签名恢复出的 IC 卡动态数据中包含的交易数据哈希码比较是否一致。

如果以上任何步骤失败，则CDA失败，TVR的“复合动态数据认证/应用密文生成（CDA）失败”位置‘1’，并进行下一步处理。

如果以上步骤全部成功，终端继续进行下一处理过程的描述。

7.11.4.1.2 标准联机处理

步骤 1：置 TSI 的“卡片风险管理已执行”位为‘1’；

步骤 2：如果以下条件全部成立，则终端发送联机请求：

——终端在 GENERATE AC 命令中请求 TC 或 ARQC；

——卡片返回的密文信息数据表明返回了 ARQC；

——终端有联机处理能力。

步骤 3：如果以下任何一项成立，则终端必须终止交易：

——终端请求应用认证密文（AAC）而卡片返回 ARQC 或 TC；

——终端请求 ARQC 而卡片返回 TC。

步骤 4：如果出现以下任一条件，则终端必须转而执行后面所描述的交易结束功能：

——执行了 CDA 但结果失败；

——卡片响应 AAC 或 TC；

——卡片响应 ARQC 但终端没有联机处理能力。

7.11.4.2 联机响应

在联机响应处理阶段，终端接收来自发卡行主机的联机响应，并决定是否应该进行发卡行认证：

——如果以下两个条件同时满足，终端将按照 7.11.4.3 描述进行发卡行认证。

- 联机授权响应中包含发卡行认证数据；
- 应用交互特征（AIP）显示卡片支持发卡行认证。

——如果满足以下任一条件，终端将进行交易结束处理。

- 联机授权响应中不包括发卡行认证数据；
- 应用交互特征（AIP）表明卡片不支持发卡行认证。

终端应能正确读取并处理收单行返回的数据：授权码，授权响应代码，发卡行认证数据，发卡行脚本等。

授权响应码的处理：联机成功后，收单行会在响应报文里传送发卡行的两字节授权响应码，表示发卡行对交易的授权结果，如批准交易、拒绝交易或发卡行要求的授权参考。

7.11.4.3 发卡行认证

如主机响应数据中包含发卡行认证数据，且终端和卡都支持发卡行认证，则终端通过向卡发外部认证（EXTERNAL AUTHENTICATE）命令执行发卡行认证。

其具体步骤如下：

步骤 1：终端将交易状态信息（TSI）的“发卡行认证已执行”位置为‘1’；

步骤 2：终端向卡片发送外部认证（EXTERNAL AUTHENTICATE）命令；

步骤 3：卡片执行发卡行认证，并在外部认证（EXTERNAL AUTHENTICATE）命令的响应中表明认证是否成功；

步骤 4：如果外部认证（EXTERNAL AUTHENTICATE）命令的响应显示发卡行认证失败（SW1 SW2 不等于“9000”或“6985”），则终端置终端验证结果（TVR）的“发卡行认证不成功”位为‘1’；

步骤 5：当外部认证（EXTERNAL AUTHENTICATE）命令响应“6985”则终端置终端验证结果（TVR）的“发卡行认证不成功”位为‘1’或终止交易；

步骤 6：然后终端转向交易结束处理。

图 21 显示了联机处理的流程。

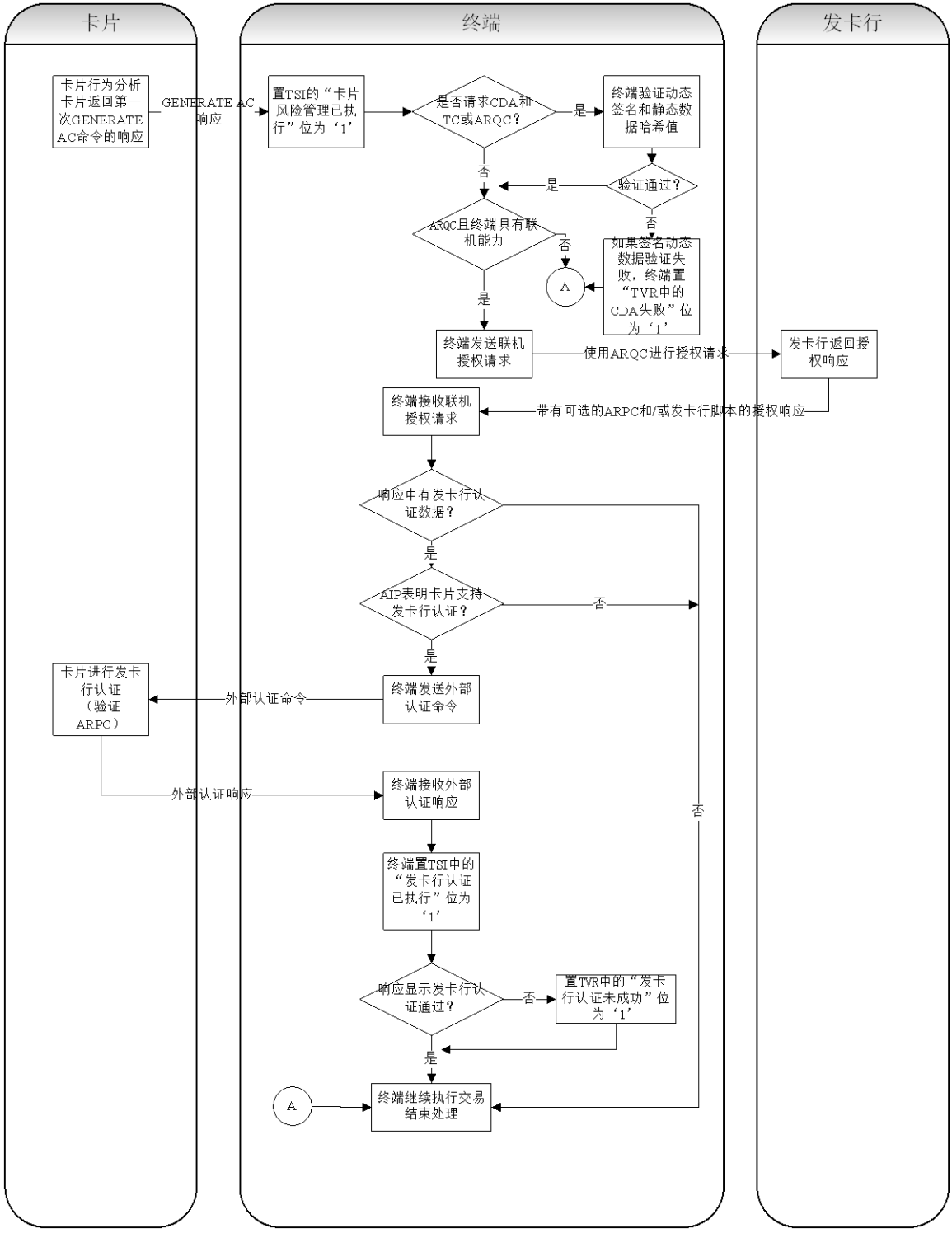

图21　联机处理流程图

7.11.5　前期相关处理

卡片行为分析

如果经过卡片行为分析后需要联机授权，则卡片在GENERATE AC命令的响应中设置密文信息数据（CID）表明返回的密文类型为ARQC。

7.11.6　后续相关处理

发卡行脚本处理

如果联机处理返回报文中包括发卡行脚本命令，终端需要将这些脚本命令发送给卡片执行。

交易结束

在完成处理过程中，卡片参考发卡行认证结果和卡片参数决定交易如何处理以及是否重置相关指示符和计数器。如果脱机数据认证要求执行CDA，则终端在第2个GENERATE AC命令响应中要处理CDA。

7.12 发卡行脚本处理

发卡行脚本处理允许发卡行更新卡片上已经个人化的数据而不必重新发卡。发卡行在授权响应报文中包含由发卡行命令组成的脚本，终端接收到脚本以后，把其中的命令发向卡片。只要满足相应的安全需求，卡片就执行这些命令。

7.12.1 终端数据

表32是终端上与脚本处理相关的数据说明。

表32 发卡行脚本处理－终端数据

数据元	描述
终端验证结果（TVR）	包括两个与脚本执行结果相关的标志位： 如果标签为‘71’的发卡行脚本处理失败，“在第 2 个 GENERATE AC 命令之前，发卡行脚本失败”位被置为‘1’ 如果标签为‘72’的发卡行脚本处理失败，“在第 2 个 GENERATE AC 命令之后，发卡行脚本失败”位被置为‘1’
交易状态信息(TSI)	当发卡行脚本处理被执行时，TSI 中对应的位被设为‘1’
发卡行脚本结果	发卡行脚本结果通过清算报文、冲正报文、下一个联机授权报文或脱机通知报文传送到发卡行。它是一个 5 个字节的域。它们的定义如下： 第 1 个字节：高半字节包含脚本处理的结果，低半字节包含脚本处理失败时脚本的命令序号。如果脚本处理成功，这个序列号为 0 第 2 至 5 字节：包含发卡行脚本中收到的发卡行脚本标识符

7.12.2 联机响应数据

从主机返回的授权响应报文中可能包含以下的与脚本处理相关的数据。一个标签72的BER-TLV编码的结构数据对象称为一个发卡行脚本。一个发卡行脚本里应当包含一条或多条准备发送给IC卡的发卡行脚本命令，每一条发卡行脚本命令以标签为86的BER-TLV格式编码。一个发卡行脚本还可以包含且仅包含一条发卡行脚本标识，发卡行脚本标识的标签为9F18。发卡行脚本中是否包含发卡行脚本标识是可选的，终端和卡片无须解释该标识的含义。发卡行脚本的具体格式请见表33和表34。

表33 发卡行脚本格式

标签	长度	标签	长度	发卡行脚本标识	发卡行脚本命令
‘72’	该脚本后续所有数据的长度总和	‘9F18’	0x04	发卡行自定	（见表 34）

表34 发卡行脚本命令格式

标签 1	长度 1	值 1	标签 2	长度 2	值 2	…
‘86’	值 1 的长度	发送给 IC 卡的命令	‘86’	值 2 的长度	发送给 IC 卡的命令	…

7.12.3 命令

JR/T 0025支持的脚本命令有：

应用锁定（APPLICATION BLOCK）：用来锁住卡片上某个选中的应用，如果在交易处理过程中锁定一个应用，则该应用将继续进行到结束，应用锁定将从下一次交易开始有效；

应用解锁（APPLICATION UNBLOCK）：对锁定的应用解锁，仅在发卡行指定的特殊终端设备上具备此功能；

卡片锁定（CARD BLOCK）：锁住卡片，该命令将锁住卡片中所有的应用。卡片锁定后，卡片无法再使用，也没有解锁命令可以将其恢复；

PIN更改/解锁（PIN CHANGE/UNBLOCK）：用于对因PIN输入次数超限而锁住PIN的卡片进行PIN解锁或PIN更改和解锁。该命令只在发卡行控制的终端上使用；

更新数据（PUT DATA）：更新卡片中的基本数据；

更新记录（UPDATE RECORD）：更新卡片文件中的一个记录。

7.12.4 处理流程

终端按以下步骤进行发卡行脚本处理。

7.12.4.1 发卡行脚本

如果收单行在响应报文中收到发卡行脚本，则它必须向终端发送发卡行脚本。当前版本的借贷记规范只支持最多一个发卡行脚本，但在一个发卡行脚本中可以包含多条命令。无论发卡行是否批准交易，也无论卡片是否批准交易，终端都应当执行发卡行脚本。

响应报文中应当只包含标签为‘72’的发卡行脚本，这表明发卡行脚本命令在第2个GENERATE AC命令之后进行。

如果联机响应报文中包含发卡行脚本且其中的命令全部执行成功，则终端必须把TSI中的“发卡行脚本已执行”位置为‘1’，但不得置TVR的“脚本处理失败”位，同时发卡行脚本结果的第1字节置为‘20’。

如果终端接收到发卡行脚本，但未能正确解析，因而没有向IC卡发送脚本命令，此时应置TSI的“发卡行脚本已执行”位和TVR的“脚本处理失败”位，发卡行脚本结果第1字节置‘00’。

如果终端没有接收到发卡行脚本，则TSI的“发卡行脚本已执行”位和TVR的“发卡行脚本处理失败”位均不置位，且无发卡行脚本结果。

7.12.4.2 多条命令

脚本中可能包含多条命令。终端必须正确解析出每条命令，并按顺序向卡片发送。每条命令之后，终端都必须累加发卡行脚本结果中的序列号。如果某条命令的未能接收到“9000”，“62xx”或“63xx”应答，则应该停止继续向卡片发送其它的脚本命令，并结束脚本处理。

7.12.4.3 脚本错误

如果卡片对脚本命令的响应的SW1不为‘90’、‘62’或‘63’，表示命令处理失败，则终端必须：

——结束对该条发卡行脚本的处理；

——在终端验证结果（TVR）中，置“最后一次 GENERATE AC 命令之后脚本处理失败”位为‘1’；

——置发卡行脚本结果第 1 字节第 5 位为‘1’；

——置发卡行脚本结果低半字节为出错的命令序号。

7.12.4.4 多个脚本

正常情况下，终端不应该接收到多个脚本。但如果收到多个脚本，则终端应见EMV4.3第四册6.3.9的描述进行处理。

7.12.4.5 带标签‘71’的脚本

正常情况下，终端不应该接收到标签为‘71’的脚本。但如果收到这样的脚本，则终端应见EMV4.3第四册6.3.9的描述进行处理。

7.12.4.6 终端消息

在脚本处理完成之前，终端都不能显示交易批准和拒绝的信息，以确保在脚本处理阶段持卡人不会拔出卡片。

7.12.4.7 给发卡行的通知

终端必须具备将发卡行脚本结果传送给发卡行的能力。脚本处理完成之后，终端应当在下一笔联机交易报文（包括但不仅限于冲正、批上送、批结算、联机授权、通知）报文向发卡行传送脚本处理结果。这些报文可以仅仅传送脚本处理结果，也可以包含其它信息。

7.12.4.8 处理流程

发卡行脚本处理的流程见图22。

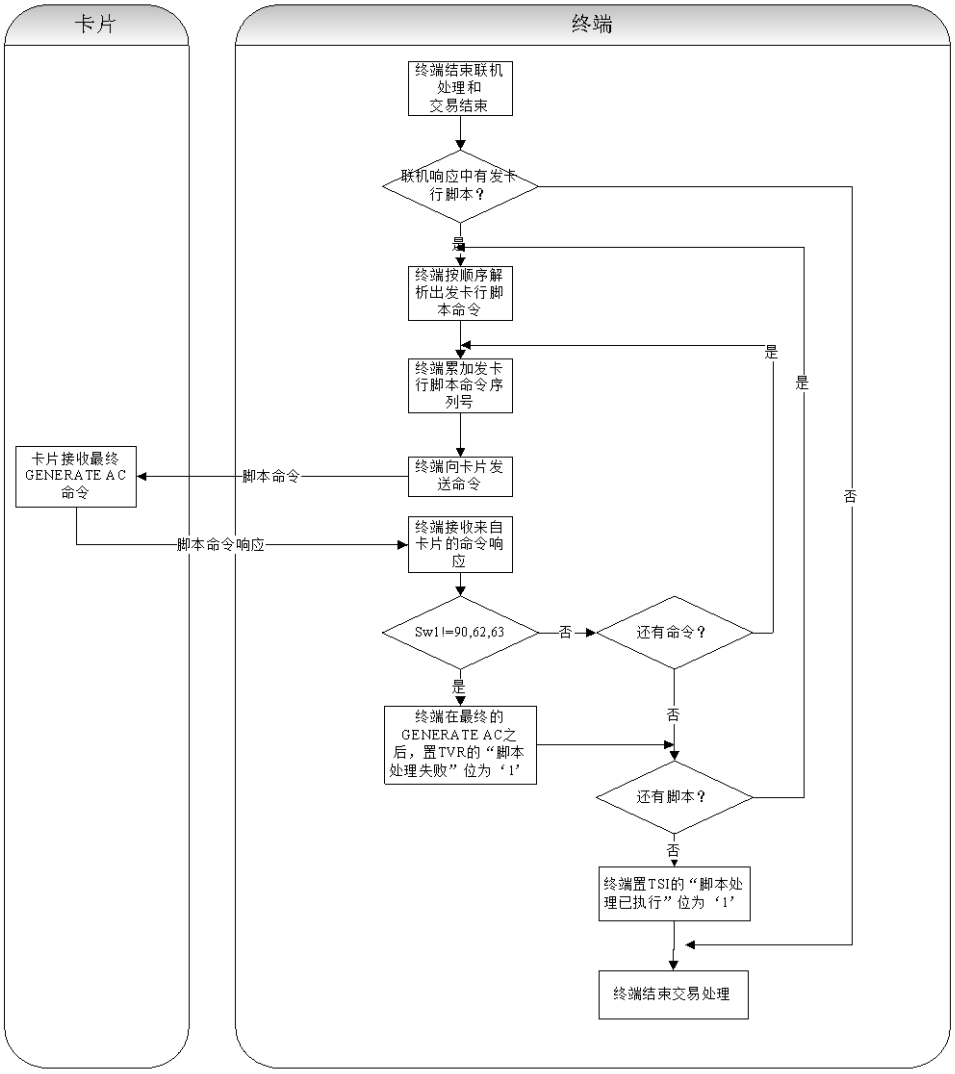

图22　发卡行脚本处理流程图

7.12.5　前期相关处理

联机处理

终端在联机授权响应中可能收到发卡行脚本。

7.12.6　后续相关处理

交易结束

终端设置发卡行脚本执行结果，并保存到相应的记录文件中。

7.13　交易结束

终端和卡片执行交易结束以完成对交易的最终处理。交易结束包括以下处理：

——如果请求了联机处理但终端不支持联机处理或联机处理未能完成，则终端和卡片进行附加的分析，以决定是否脱机批准或拒绝；

——如果执行了复合动态数据认证（CDA）且执行失败，则终端必须进行以下处理：

- 如果第 1 次 GENERATE AC 命令请求 TC，则终端必须脱机拒绝交易；
- 如果在第 1 次 GENERATE AC 命令中请求 ARQC，则终端必须在第 2 次 GENERATE AC 命令中请求 AAC。

——根据发卡行认证结果和卡片选项，发卡行的联机批准可能被改为拒绝；

——根据发卡行认证结果和卡片选项，在联机授权之后，某些指示符和计数器可能需要复位。

终端可能在交易结束后再执行附加的功能，如验证持卡人签名、打印凭单和获取用于清算的数据等。只要与此处定义的结束处理不冲突，终端就可以执行附加的结束功能。

7.13.1 卡片数据

交易结束处理阶段，终端使用表35的卡片数据元。

表35 交易结束－卡片数据

数据元	描述
卡片风险管理数据对象列表 2（CDOL2）	终端需要在第 2 个 GENERATE AC 命令中向卡片传送的数据对象（标签和长度）列表
发卡行行为代码（IAC）－缺省	包含一个五字节二进制位序列，与 TVR 对应。如果发卡行希望在 TVR 中某位被置为‘1’而又不能完成联机授权时进行脱机拒绝，则在 IAC－缺省中对应的位应置为‘1’ 关于 IAC－缺省的详细描述，见 JR/T 0025.5

表36 交易结束－第 2 个 GENERATE AC 响应数据

数据元	描述
密文信息数据（CID）	包含表明卡片返回密文类型的指示符： —— 表示拒绝的 AAC —— 表示批准的 TC
应用交易计数器（ATC）	应用置入卡片以来执行的交易总数计数器
应用密文（AC）	8 字节密文值
发卡行应用数据	包含需要向发卡行发送的发卡行私有数据。其中包括 CVR
卡片验证结果（CVR）	卡片根据当前交易和上次交易的脱机处理结果进行置位的验证结果数据

如果第2个GENERATE AC命令的响应数据为格式1，则返回数据为包含在标签为‘80’的上表中的数据。

如果响应数据为格式2，则返回数据数据是包含在标签‘77’中的BER-TLV编码格式的数据。如果格式2响应数据中包含签名动态应用数据（标签“9F4B”），则应用密文也被包含在动态签名中其描述见JR/T 0025.7中5.3.6。

7.13.2 终端数据

应用交易结束阶段使用表37的终端数据。

表37 交易结束－终端数据

数据元	描述
授权响应码	终端提供该数据元给卡片，指示终端对交易结果的判断 Y1 = 脱机批准 Z1 = 脱机拒绝 Y3 = 不能联机执行（脱机批准） Z3 = 不能联机执行（脱机拒绝）
终端验证结果（TVR）	用来记录脱机处理结果的终端数据元，比如脱机数据认证失败或者超过最低限额等
终端行为代码（TAC）—缺省	包含一系列和 TVR 对应的定义位，如果联机授权不能完成，但是 TAC－缺省内一个位被置为‘1’而且相应的 TVR 位也为‘1’，就会产生脱机拒绝

7.13.3 命令

交易结束阶段使用GENERATE AC命令请求卡片提供卡片授权响应。

本命令的P1参数表明终端请求的密文类型。P1参数的具体设置，见JR/T 0025.5附录B.6中的表B.6和表B.7。命令的数据部分包含由CDOL2指明的终端数据。

命令的响应包含表36中的数据。

7.13.4 交易脱机授权

如果在第1个GENERATE AC命令中IC卡返回TC或AAC，则交易脱机授权批准或拒绝。

终端必须根据第1个GENERATE AC命令响应返回的密文信息数据（CID）显示相应的消息（批准、拒绝或服务不允许），表明交易的结果。

如果TVR显示复合动态数据认证（CDA）失败，则终端应按如下拒绝交易：

——如果第 1 个 GENERATE AC 命令返回 TC，则以授权响应码‘Z1’拒绝交易；

——如果第 1 个 GENERATE AC 命令返回 ARQC，则终端必须在第 2 个 GENERATE AC 命令中请求 AAC。

表38 脱机交易判断处理

第 1 个 GENERATE AC 命令 返回密文类型	授权响应码	最终交易结果
TC 且 CDA 不执行或成功	Y1	脱机批准
AAC	Z1	脱机拒绝
TC 或 ARQC，且 CDA 失败	Z1	脱机拒绝

7.13.5 交易联机授权

7.13.5.1 向卡片发送第 2 个 GENERATE AC 命令

如果联机授权成功完成，终端向卡片发送第2个GENERATE AC命令请求附加的卡片分析和最终的应用密文。

终端根据在联机处理中接收到的来自发卡行的授权响应码决定向卡片请求何种密文：

——如果发卡行批准交易（授权响应码为‘00’、‘10’或‘11’），终端请求 TC；

如果终端请求TC且脱机数据认证要求执行CDA，则在第2次GENERATE AC命令的P1参数中设置要求执行CDA。

——如果发卡行请求参考（授权响应码为‘01’或‘02’），则终端提示操作员打电话请求授权，根据发卡行授权结果（批准或拒绝）请求相应的密文。如果终端不支持参考，则终端请求 AAC；

——如果授权响应码未指明批准或参考，则终端请求 AAC。

7.13.5.2 终端接收第 2 个 GENERATE AC 响应

终端接收到来自卡片的GENERATE AC响应后，进行以下处理。

7.13.5.2.1 发卡行脚本处理

如果授权响应报文中包含发卡行脚本数据，则终端必须在交易最后完成之前先进行发卡行脚本处理。

终端必须在脚本处理完成以后再向持卡人显示交易批准或拒绝的信息，以防持卡人拔出卡片。

如果进行了脚本处理，则终端必须在适当的时候向发卡行主机发送报文（清算报文、通知报文或下次联机授权报文），传送脚本处理的结果。本部分不规定具体的报文格式。

7.13.5.2.2 复合动态数据认证处理

如果在脱机数据认证阶段要求执行CDA且在第2个GENERATE AC命令的P1参数设置了执行CDA位，则终端处理CDA。

如果IC卡响应AAC，则终端不认为CDA失败而结束交易。

如果IC卡响应TC，终端执行以下步骤：

步骤 1：如果签名的动态应用数据的长度不同于 IC 卡公钥模的长度，那么 CDA 失败；

步骤 2：IC 卡公钥解开动态签名（签名动态应用数据），恢复出签名中的数据；

步骤 3：检查恢复数据的头、尾、数据格式是否正确；

步骤 4：检查解开的密文信息数据和 GENERATE AC 命令响应中接收到未加密的密文信息数据是否一致；

步骤 5：将不可预知数加在恢复数据后面，计算哈希结果，并与恢复出的哈希值比较是否一致；

步骤 6：将 PDOL 数据，CDOL1 数据，CDOL2 数据和 GENERATE AC 命令返回数据（动态签名除外）连在一起计算哈希结果，与从动态签名恢复出的 IC 卡动态数据中包含的交易数据哈希码比较是否一致。

如果以上任何步骤失败，则CDA失败，TVR的“复合动态数据认证/应用密文生成（CDA）失败”位置‘1’。

7.13.5.2.3 终端在第 2 个 GENERATE AC 命令中请求 AAC

如果终端在第2个GENERATE AC命令中请求AAC，则不论在响应中接收到何种密文，终端都必须拒绝交易，并显示相应的交易拒绝消息。

7.13.5.2.4 终端在第 2 个 GENERATE AC 命令中请求 TC

步骤 1：卡片响应 TC

——如果不要求执行 CDA，终端结束交易，并显示交易已经批准；

——如果 GENERATE AC 命令指示要求执行 CDA，则按照前面所述对响应的动态签名应用数据恢复，执行 CDA 过程。如 CDA 成功，终端批准交易；否则终端拒绝交易。

步骤 2：如果卡片响应 AAC，则终端结束交易，并显示交易已经拒绝

注： 在ATM上，如果提现或者转账交易因为发卡行认证失败而被卡片拒绝，则当卡片在第2个GENERATE AC命令中响应AAC之后，ATM应该发送冲正消息。如果查询交易因为同样的原因被拒绝，则ATM不能显示余额。

在POS设备上，如果在联机过程中发卡行批准交易，但因为发卡行认证失败卡片拒绝交易，终端则应向后台发送冲正报文，见JR/T 0001。

7.13.6 要求联机处理但未进行联机

7.13.6.1 检查 IAC－缺省和 TAC－缺省设置

如果要求联机交易，但终端不支持联机处理或联机不成功，终端用IAC－缺省和TAC－缺省执行终端行为分析，并根据结果向IC卡发第2个GENERATE AC命令。具体描述见本部分7.9。

7.13.6.2 发送第 2 个 GENERATE AC 命令

终端根据处理结果在第2个GENERATE AC命令的P1参数中表明请求的是AAC（拒绝）还是TC（批准）。CDOL2中所列的数据作为命令数据传送给IC卡。其中授权响应码的取值见表39。

表39 联机交易处理响应

终端请求	授权响应码	最终交易结果
TC	Y3	不能联机（脱机批准）
AAC	Z3	不能联机（脱机拒绝）

终端随后发送包含授权响应码的第2个GENERATE AC命令。

如果终端请求TC且脱机数据认证要求执行CDA，则在第2个GENERATE AC命令的P1参数中设置要求执行CDA。

7.13.6.3 终端结束交易

接收到卡片对第2个GENERATE AC命令的响应以后，终端进行以下处理。

7.13.6.3.1 终端在第 2 个 GENERATE AC 命令中请求 AAC

如果终端在第2个GENERATE AC中请求AAC，则无论在响应中接收到何种密文，终端都必须显示信息，表明交易已经被拒绝。

7.13.6.3.2 终端在第 2 个 GENERATE AC 命令中请求 TC

如果终端在第2个GENERATE AC中请求TC，则它检查GENERATE AC命令响应报文中返回的密文类型：

步骤 1：卡片返回 TC

——如果不要求执行 CDA，终端结束交易，并显示交易已经被批准；

——如果 GENERATE AC 命令指示要求执行 CDA，则按照 7.13.5.2.2 中所描述对返回的动态签名应用数据恢复，执行 CDA 过程。如 CDA 成功，终端批准交易；否则终端拒绝交易。

步骤 2：卡片返回 AAC

——终端应该结束交易并显示交易已经被拒绝。交易结束处理流程见图 23。

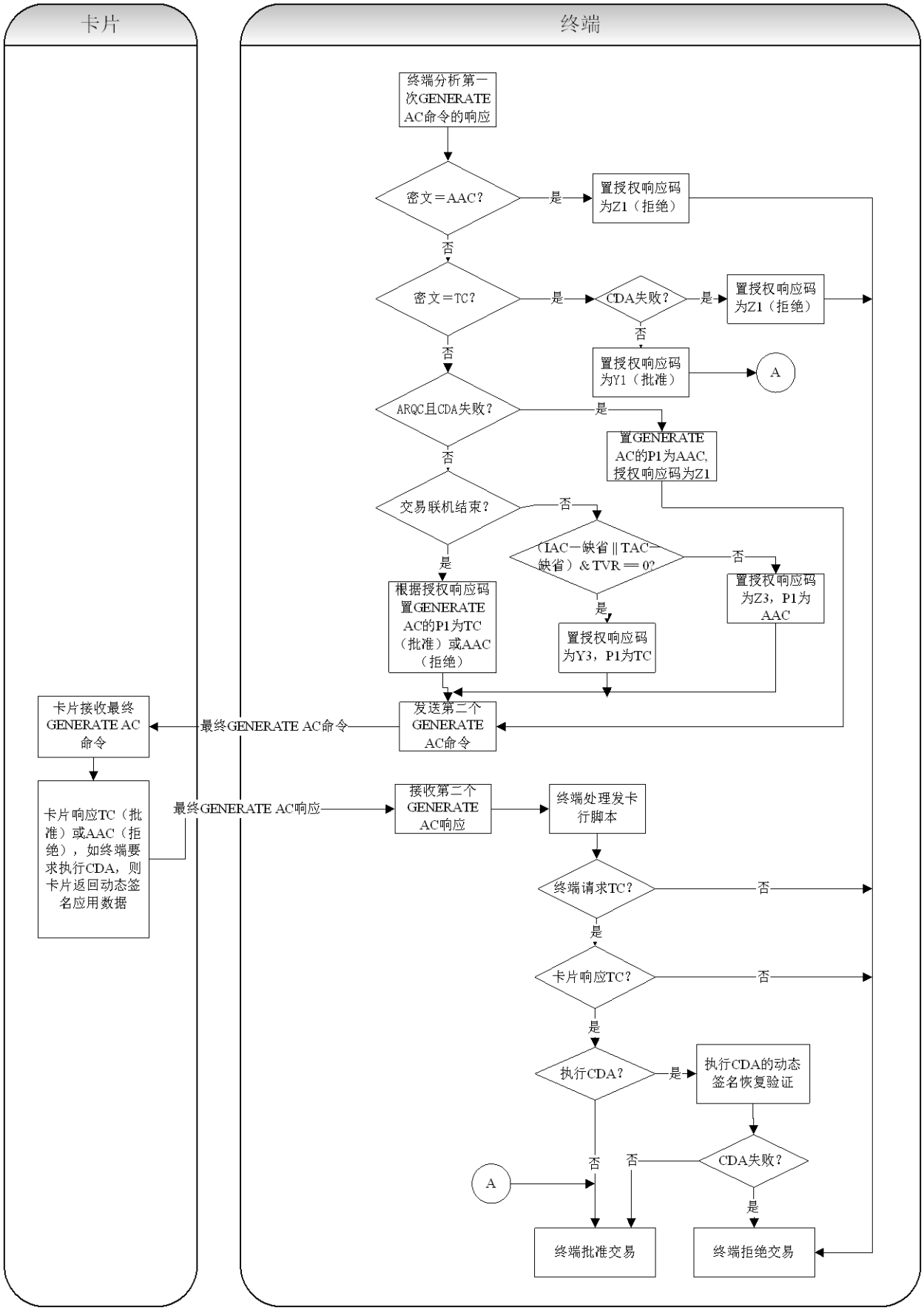

图23　交易结束处理流程图

7.13.7　前期相关处理

卡片行为分析

卡片在第1个GENERATE AC命令的响应中返回TC或AAC指示交易脱机批准或脱机拒绝。

联机处理

终端在联机授权响应中收到授权响应代码表明后台对交易的授权结果。

8　终端数据

8.1　数据元格式约定

a－每个字节包含一个字符的字母数据元（A-Z，a-z）。

an－每个字节包含一个字符字母数字型数据元（A-Z，a-z，0-9）。

ans–字母数字及特殊字符型。

b－二进制（二进制数或者位组合）。

cn－压缩数字，每个字节由‘0’－‘9’中的两个数字组成，数据元左对齐，右补F。如数1234567890123可以以十六进制形式保存在8个字节的PAN数据对象中，形如‘12 34 56 78 90 12 3F FF’。

n－数字型，也称作BCD码。右对齐，左补‘0’。如，数字12345可以保存在n12的授权金额数据对象中，形如‘00 01 23 45’。

var－可变长。变长数据的格式另有说明。

8.2　终端和收单行数据表

表40列出终端和收单行支持的数据元，并说明其来源，含义及TLV格式。

表40　终端和收单行数据元

名称	描述	来源	格式	模版	标签	长度
收单行标识	在每个支付系统中唯一标识收单行	终端	n6-11	—	‘9F01’	6
附加终端性能	表明终端的数据输入输出能力	终端	B	—	‘9F40’	5
授权金额（二进制）	交易授权金额（不包括调整）	终端	B	—	‘81’	4
授权金额（数值型）	交易授权金额（不包括调整）	终端	n12	—	‘9F02’	6
其它金额（二进制）	与交易相关的第 2 金额，表示返现金额	终端	B	—	‘9F04’	4
其它金额（数值型）	与交易相关的第 2 金额，表示返现金额	终端	n12	—	‘9F03’	6
参考货币金额	用参考货币表示的授权金额	终端	B	—	‘9F3A’	4
应用标识（AID）	按 GB/T 16649.5 所定义，用于表示一个应用	终端	B	—	‘9F06’	5-16
应用选择指示器	指示应用选择时终端上的 AID 与卡片中的 AID 是完全匹配（长度和内容都必须一样），还是部分匹配（卡片 AID 的前面部分与终端 AID 相同，长度可以更长）。终端支持的应用列表中的每个 AID 仅有一个应用选择指示器，它的格式如表 5 所示	终端	由终端决定，本数据不在接口之间传递	无	无	见格式
应用版本号	支付系统给应用分配的版本号	终端	B	—	‘9F09’	2

名称	描述	来源	格式	模版	标签	长度
授权响应代码	定义发卡行对交易联机授权的结果	发卡行/终端	An 2	—	‘8A’	2
持卡人验证方法（CVM）结果	表示最后一次持卡人验证方法执行的结果	终端	B	—	‘9F34’	3
认证中心公钥验证和	用安全哈希算法对认证中心公钥所有部分（RID、认证中心公钥索引、认证中心公钥模、认证中心公钥指数）连接的结果进行运算所得的验证值	终端	B	—	—	20
认证中心公钥指数	认证中心公钥的指数部分	终端	B		—	1 或 3
认证中心公钥索引	与 RID 一起标识认证中心公钥	终端	B		‘9F22’	1
认证中心公钥模	认证中心公钥的模部分	终端	B		—	Nca（最大 248）
命令模版	标识命令报文中的数据域	终端	B		‘83’	var.
缺省动态数据认证数据对象列表（DDOL）	卡片中无 DDOL 时用于构造内部认证命令的 DDOL	终端	B		—	var.
缺省交易证书数据对象列表（TDOL）	卡片中无 TDOL 时用于生成 TC 哈希值的 TDOL。本部分中该值为空	终端	B		—	var.
加密的个人识别码（PIN）数据	在密码键盘中加密的用于联机验证或脱机验证（密码键盘和读卡器未集成在一起）的交易 PIN	终端	B		—	8
接口设备（IFD）序列号	厂商分配给终端 IFD 的唯一、永久的序列号	终端	an8	—	‘9F1E’	8
发卡行脚本结果	表示终端脚本处理的结果	终端	B		—	var.
偏置随机选择的最大目标百分数	在终端风险管理中用于随机交易选择的值	终端	—		—	—
商户分类码	按 GB/T 15150 卡片受理业务编码所规定的商户从事业务所进行的分类	终端	N 4	—	‘9F15’	2
商户标识	和收单行标识一起唯一地标识一个特定的商户	终端	ans 15	—	‘9F16’	15
商户名称和位置	表明商户的名称和所处位置	终端	Ans		—	var.
报文类别	表明批数据收集记录是金融记录还是通知	终端	N 2		—	1
密码键盘 密钥	用于密码键盘加密 PIN 和读卡器解密 PIN（密码键盘和读卡器未集成时）所使用的对称密钥	终端	—		—	—
销售点（POS）输入方式	按 GB/T 15150 销售点输入模式，表示 PAN 的输入方式	终端	n 2	—	‘9F39’	1

名称	描述	来源	格式	模版	标签	长度
随机选择的目标百分数	在终端风险管理中用于随机交易选择的值	终端	—		—	—
终端行为代码－缺省	收单行设置的在交易联机无法进行的情况下能够导致交易脱机拒绝的 TVR 条件位	终端	b		—	5
终端行为代码－拒绝	收单行设置的能够导致交易脱机拒绝的 TVR 条件位	终端	b		—	5
终端行为代码－联机	收单行设置的能够导致交易联机处理的 TVR 条件位	终端	b		—	5
终端性能	表示终端的卡片数据输入、CVM 支持和安全能力	终端	b		‘9F33’	3
终端国家代码	按 GB/T 2659 表示的终端国家代码	终端	n 3	—	‘9F1A’	2
终端最低限额	终端中与 AID 相关的导致交易联机处理的最低交易金额	终端	b		‘9F1B’	4
终端标识	表明终端在商户的唯一位置	终端	an 8	—	‘9F1C’	8
终端类型	指示终端环境、通讯能力和操作控制	终端	n 2	—	‘9F35’	1
终端验证结果（TVR）	用于记录终端执行各借记/贷记功能处理结果的一组指示位	终端	b	—	‘95’	5
偏置随机选择的阈值	在终端风险管理中用于随机交易选择的值	终端	—		—	—
交易金额	交易的清算金额，包括消费和其它调整	终端	n 12		—	6
交易证书（TC）哈希值	包含在 CDOL 数据中要求送给卡片，由 TDOL 表示的数据作哈希运算的结果。	终端	b	—	‘98’	20
交易货币代码	按 GB/T 12406 规定的交易货币代码	终端	n 3	—	‘5F2A’	2
交易货币指数	按 GB/T 12406 规定的从交易金额右起的隐含小数点位置	终端	n 1	—	‘5F36’	1
交易日期	交易授权的本地日期	终端	n 6 YYMMDD	—	‘9A’	3
交易 PIN 数据	持卡人输入的 PIN 数据	终端	b	—	‘99’	var.
交易参考货币代码	当交易货币代码和应用货币代码不同时，终端使用的公共货币代码	终端	n 3	—	‘9F3C’	2
交易参考货币兑换比率	从交易货币代码向交易参考货币代码兑换时的比率	终端	n 8		—	4
交易参考货币指数	表示按 GB/T 12406 规定的交易参考货币代码的交易金额右起的隐含小数点位置	终端	n 1	—	‘9F3D’	1
交易序列计数器	终端维护的每笔交易递增一的计数器	终端	n 4-8	—	‘9F41’	2-4
交易状态信息	一组表示交易完成的借贷记功能的指示位	终端	b	—	‘9B’	2
交易时间	交易授权的本地时间	终端	n 6 HHMMSS	—	‘9F21’	3
交易类型	按 GB/T 15150 定义的处理码前 2 位表示的金融交易类型	终端	n 2	—	‘9C’	1

名称	描述	来源	格式	模版	标签	长度
不可预知数	为提供给卡片生成应用密文而由终端提供的动态变化和唯一的数据	终端	b	—	‘9F37’	4
账户类型	标识在交易中选择的账户的类型 编码规则见附录 A 中 A.9	终端	n2	—	‘5F57’	1

当定义的数据对象长度大于实际数据对象的长度时，采用如下规则：

——格式为 n 的数据元右对齐，左补十六进制零；

——格式为 cn 的数据元左对齐，右补十六进制‘F’；

——格式为 an 的数据元左对齐，右补十六进制零；

——格式为 ans 的数据元左对齐，右补十六进制零。

当数据从一处转移到另一处时（例如从卡片到终端），无论各自内部如何存储，必须按从高位到低位的顺序传递。连接数据时也使用同样的规则。

8.3 终端数据管理要求

如下数据应在终端首次安装时初始化：

终端性能、终端附加性能、终端IFD序号、终端国家代码、终端标识、终端类型、终端交易货币和终端货币指数。

如下终端数据应允许在终端布放后通过下载更新：

终端支持应用AID列表、CA公钥、终端行为代码TAC、最低限额（Floor limit）、随机选择阈值、随机选择目标百分数、偏置随机选择最大目标百分数、商户标识、商户分类码和收单行标识。

9 金融交易命令

JR/T 0025借记/贷记应用中终端所应支持的金融交易命令有：

——外部认证（EXTERNAL AUTHENTICATE）命令，用于发卡行认证；

——生成应用密文（GENERATE AC）命令，用于卡片行为分析；

——取数据（GET DATA）命令，用于从 IC 卡中获取交易数据，本部分中允许通过此命令获取的数据有三个：应用交易计数器（ATC），上次联机 ATC 寄存器，PIN 重试次数；

——获取处理选项(GPO)命令，应用选择后获取 IC 卡支持功能及应用文件定位器；

——内部认证（INTERNAL AUTHENTICATE）命令，用于动态数据认证（DDA）过程；

——读记录（READ RECORD）命令，用于读取应用数据文件；

——选择（SELECT）命令，用于应用选择；

——验证（VERIFY）命令，用于 PIN 验证。

附 录 A
（规范性附录）
终端数据元编码

A.1 终端类型

表 A.1 终端类型

环境	操作控制方		
	金融机构	商户	持卡人
有服务员的：			
仅仅联机	11	21	—
有联机能力的脱机	12	22	—
仅仅脱机	13	23	—
自助的：			
仅仅联机	14	24	34
有联机能力的脱机	15	25	35
仅仅脱机	16	26	36

终端类型为‘14’、‘15’和‘16’且具有现金支出能力（附加终端性能的字节1，“现金”位=‘1’）的终端被认为是ATM，所有其它类型的终端都不被认作是ATM。

终端类型的例子有：

——金融机构控制的服务员终端：支付终端；

——商户控制的服务员终端：电子收银机、便携式 POS 终端、独立的 POS 终端和主机集中式 POS 终端；

——金融机构控制的自助终端：ATM 和银行自动售货机；

——商户控制的自助终端：自动加油机、付费电话、自动售票机和自动售货机；

——持卡人控制的自助终端：家庭终端、个人计算机、可视电话、付费电话和数字交互电视/机顶盒。

A.2 终端性能

下面表中的‘1’表示，如果某位的值为‘1’，则对应的“意义”被应用，而‘x’表示该位没有使用。

表 A.2 终端性能

字节 1：卡片数据输入性能

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	手工键盘输入
x	1	x	x	x	x	x	x	磁条
x	x	1	x	x	x	x	x	接触式 IC 卡
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

字节 2：CVM 性能

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	IC 卡明文 PIN 验证
x	1	x	x	x	x	x	x	加密 PIN 联机验证
x	x	1	x	x	x	x	x	签名（纸）
x	x	x	0	x	x	x	x	RFU
x	x	x	x	1	x	x	x	无需 CVM
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	1	持卡人证件验证

如果终端支持签名的CVM，则这个终端必须是服务员终端（终端类型=‘X1’，‘X2’，或‘X3’）并且支持打印机（附加终端性能的字节4“打印，给服务员”位=‘1’）。

字节 3：安全性能

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	静态数据认证（SDA）
x	1	x	x	x	x	x	x	动态数据认证（DDA）
x	x	1	x	x	x	x	x	吞卡
x	x	x	0	x	x	x	x	RFU
x	x	x	x	1	x	x	x	复合动态数据认证/应用密文生成（CDA）
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

A.3 附加终端性能

下面表中的‘1’表示，如果某位的值为‘1’，则对应的‘意义’被应用，而‘X’表示该位没有使用。

表 A.3 附加终端性能

字节 1：交易类型性能

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	现金
x	1	x	x	x	x	x	x	商品
x	x	1	x	x	x	x	x	服务
x	x	x	1	x	x	x	x	返现
x	x	x	x	1	x	x	x	查询
x	x	x	x	x	1	x	x	转账
x	x	x	x	x	x	1	x	付款
x	x	x	x	x	x	x	1	管理

字节 2：交易类型性能

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	存款交易

x	0	x	x	x	x	x	x	RFU
x	x	0	x	x	x	x	x	RFU
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

字节 3：终端数据输入性能

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	数字键
x	1	x	x	x	x	x	x	字母和特殊字符键
x	x	1	x	x	x	x	x	命令键
x	x	x	1	x	x	x	x	功能键
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

字节 4：终端数据输出性能

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	打印，给服务员
x	1	x	x	x	x	x	x	打印，给持卡人
x	x	1	x	x	x	x	x	显示，给服务员
x	x	x	1	x	x	x	x	显示，给持卡人
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	1	x	编码表 10
x	x	x	x	x	x	x	1	编码表 9

编码表序号指ISO 8859对应的部分。

字节 5：终端数据输出性能

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	编码表 8
x	1	x	x	x	x	x	x	编码表 7
x	x	1	x	x	x	x	x	编码表 6
x	x	x	1	x	x	x	x	编码表 5
x	x	x	x	1	x	x	x	编码表 4
x	x	x	x	x	1	x	x	编码表 3
x	x	x	x	x	x	1	x	编码表 2
x	x	x	x	x	x	x	1	编码表 1

A.4 CVM结果

字节 1：执行的 CVM

CVM列表里最近一次被终端实际执行的CVM：

CVM列表的1字节长CVM代码定义见JR/T 0025.5的A.1中的表A.1。

（如果没有CVM被执行则该值为‘3F’）

字节 2：CVM 条件码

CVM列表里1字节长的CVM条件码定义见JR/T 0025.5的A.1中的表A.1。

字节 3：CVM 结果

终端所知的（最近一次的）CVM执行结果：

‘0’ = 未知（例如，签名）；

‘1’ = 失败（例如，脱机 PIN）；

‘2’ = 成功（例如，脱机 PIN）。

A.5 发卡行脚本结果

字节 1：脚本结果

高4位：终端所执行的发卡行脚本处理结果：

——‘0’ = 脚本未被处理；

——‘1’ = 脚本处理失败；

——‘2’ = 脚本处理成功。

低4位：脚本命令序号

——‘0’ = 没有指定；

——‘1’到‘E’= 1 到 14 的脚本序号；

——‘F’ = 15 或以上的脚本序号。

字节 2 – 5：脚本标识

终端收到的发卡行脚本的脚本标识，如没有则填0。如果终端收到不止一个发卡行脚本则必须有。对每个终端处理的发卡行脚本都有如上5个字节的脚本结果。

A.6 授权响应码

从授权响应消息得到的授权响应代码在传输给卡时，应至少包括如下可能信息：

——联机批准；

——联机拒绝；

——语音参考（发卡行发起的）；

——吞卡。

此外，如果交易没有经过联机授权，终端必须能产生和发送给卡如下新的响应代码：

表 A.4 响应码

响应码	值
脱机批准	Y1
脱机拒绝	Z1
无法联机，脱机被批准	Y3
无法联机，脱机被拒绝	Z3

终端不应修改响应报文中返回的授权响应码[1]。

[1] 卡的最终决定可以从密文信息数据而不是授权响应码中反映。

A.7 终端验证结果

表 A.5 终端验证结果(TVR)

字节 1：

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	未进行脱机数据认证
x	1	x	x	x	x	x	x	脱机静态数据认证失败
x	x	1	x	x	x	x	x	IC 卡数据缺失
x	x	x	1	x	x	x	x	卡片出现在终端异常文件中
x	x	x	x	1	x	x	x	脱机动态数据认证失败
x	x	x	x	x	1	X	x	复合动态数据认证/应用密文生成失败
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

字节 2：

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	IC 卡和终端应用版本不一致
x	1	x	x	x	x	x	x	应用已过期
x	x	1	x	x	x	x	x	应用尚未生效
x	x	x	1	x	x	x	x	卡片不允许所请求的服务
x	x	x	x	1	x	x	x	新卡
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

字节 3：

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	持卡人验证失败
x	1	x	x	x	x	x	x	未知的 CVM
x	x	1	x	x	x	x	x	PIN 重试次数超限
x	x	x	1	x	x	x	x	要求输入 PIN，但密码键盘不存在或工作不正常
x	x	x	x	1	x	x	x	要求输入 PIN，密码键盘存在，但未输入 PIN
x	x	x	x	x	1	x	x	输入联机 PIN
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

字节 4：

b8	b7	b6	B5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	交易超过最低限额
x	1	x	x	x	x	x	x	超过连续脱机交易下限
x	x	1	x	x	x	x	x	超过连续脱机交易上限
x	x	x	1	x	x	x	x	交易被随机选择联机处理
x	x	x	x	1	x	x	x	商户要求联机交易
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

字节 5：

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	使用缺省 TDOL
x	1	x	x	x	x	x	x	发卡行认证失败
x	x	1	x	x	x	x	x	最后一次 GENERATE AC 命令之前脚本处理失败
x	x	x	1	x	x	x	x	最后一次 GENERATE AC 命令之后脚本处理失败
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

A.8 交易状态信息

表 A.6 交易状态信息(TSI)

字节 1：

b8	b7	b6	b5	b4	B3	b2	b1	意义
1	x	x	x	x	x	x	x	脱机数据认证已执行
x	1	x	x	x	x	x	x	持卡人验证已执行
x	x	1	x	x	x	x	x	卡片风险管理已执行
x	x	x	1	x	x	x	x	发卡行认证已执行
x	x	x	x	1	x	x	x	终端风险管理已执行
x	x	x	x	x	1	x	x	脚本处理已执行
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

字节 2：

b8	b7	b6	b5	b4	b3	b2	b1	意义
0	x	x	x	x	x	x	x	RFU
x	0	x	x	x	x	x	x	RFU
x	x	0	x	x	x	x	x	RFU
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

A.9 账户类型

有时，在支付卡上的一个金融应用被链接到发卡行的几个账户，如信用账户、储蓄账户等。一些终端在交易时提示持卡人选择交易所用的账户类型。这种提示可能出现在芯片交易和磁条交易中。对于芯片交易，发卡行可能希望选中的账户类型影响卡片应用的行为；例如，卡片应用可能根据账户类型的不同，指定不同的CVM列表或者执行不同的卡片风险管理。这种想法可通过终端在PDOL中传递持卡人指定的账户类型，卡片使用账户类型来调用特定的数据，风险管理的参数等，实现发卡行要求的不同账户类型的处理。

本附录定义了一个新的数据元，用于标识持卡人在终端上选中的账户类型。该数据元的编码见表A.7。

表 A.7 账户类型

数值	账户类型
00	默认-未指定
10	储蓄账户
20	支票账户/借记账户
30	信用账户
其它值保留	

如果终端支持持卡人选择账户类型，那么在应用选择前或应用选择处理中（要早于应用初始化的处理），持卡人被要求选择交易中要使用的账户类型（储蓄账户，信用账户等）。选中的账户类型作为一个数值被存在终端数据元“账户类型”中。如果没有指定账户类型，值被设为“00”（默认-未指定）。

当在PDOL中请求，选中的账户类型的信息在GPO命令数据中发送给卡片。卡片返回相关的AIP/AFL并且执行账户类型指定的卡片风险管理（如果要求）。

A.10 数据元的填充与构造规则

见JR/T 0025.5附录A.1的规则。

附 录 B
（规范性附录）
交易日志的读取

在需要的时候，特定终端可以读取IC卡内的交易日志。明细的格式和内容见JR/T 0025.4和JR/T 0025.5的相关规定。本附录仅描述终端读取交易日志的一般步骤。

B.1 交易日志记录文件

交易日志记录文件是一个定长循环记录文件。记录格式不包括应用基本数据模版（标识‘70’）。记录文件的短文件标识符和记录个数在交易日志入口数据元（标签“9F4D”）中规定，交易日志记录文件的短文件标识符取值范围必须在11-20之间，本部分推荐值为11，交易日志入口数据元是在选择应用的时候，由卡片在发卡行自定义数据中返回。

记录内容由交易日志格式（标签“9F4F”）决定。交易日志格式的值域是一串日志内容数据对象的标识和长度。终端通过取数据（GET DATA）命令取得交易日志格式数据元，可知交易日志记录文件需要记录的内容。

交易日志格式和交易日志记录在应用锁定后仍可以访问。

B.2 交易日志读取的步骤

为了读取交易日志信息，特定设备使用下列步骤：

——执行应用选择，在发卡行自定义数据处获得交易日志入口数据元。如果交易日志入口数据元不存在，应用不支持交易日志功能；

——发送取数据（GET DATA）命令取得交易日志格式数据元；

——发送 READ RECORD 命令读交易日志记录。交易日志记录文件的读权限为自由读，写权限不公开，由卡片操作系统控制。

参考文献

[1] EMV 支付系统集成电路卡规范：4.3，第 1 册～第 4 册
[2] VISA 集成电路卡终端规范，1.4.0 版