ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0025.4—2018
代替 JR/T 0025.4—2013

中国金融集成电路（IC）卡规范 第4部分：借记/贷记应用规范

China financial integrated circuit card specifications—
Part 4: Debit/credit application specification

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4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 0025.4—2013《中国金融集成电路（IC）卡规范　第4部分：借记/贷记应用规范》，与JR/T 0025.4—2013相比主要技术变化如下：

——对终端发起冲正的条件做出调整；

——对应用锁定后返回数据内容做出了修正（见6.2.11.6.1　）。

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、上海浦东发展银行、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、杨倩、聂丽琴、杜宁、周玥、张宏基、程胜、黄本涛、汤沁莹、陈则栋、吴晓光、李春欢、洪隽、张栋、王红剑、张永峰、刘志刚、胡吉晶、吴潇、范抒、魏猛、余沁、尚可、侯晓晨、李新、李一凡、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、张萌、张国栋、俞益宁、曾静静、李铭铭。

本部分代替了JR/T 0025.4—2013。

JR/T 0025.4—2013的历次版本发布情况为：

JR/T 0025.4—2005、JR/T 0025.4—2010。

引　言

本部分为JR/T 0025—2018的第4部分，与JR/T 0025—2018的第5部分、第6部分和第7部分一起构成借记/贷记规范。

本部分提供了卡和终端之间处理的技术性概述，用于理解此处理和在借记/贷记交易流程中有关事宜的步骤。

本部分的目的在于：

——帮助银行和供应商理解 IC 卡给借记/贷记支付服务所带来的变化，特别是在 IC 卡和终端之间的处理方面；

——提出对基于芯片卡借记/贷记项目的最低需求；

——确定银行和供应商为适应市场需求所能够执行的选项；

——定义关于可选择 JR/T 0025—2018 特性的实施；

——提供卡片和终端之间处理的技术性概述，用于理解此处理和在借记/贷记交易流程中有关事宜的步骤。

中国金融集成电路（IC）卡规范
第4部分：借记/贷记应用规范

1 范围

本部分规定了借记/贷记应用中卡片和终端之间的数据处理流程以及对基于IC卡的借记/贷记流程的基本要求。

本部分适用于与借记/贷记应用相关的卡片设计、制造、管理、发行、受理以及应用系统的研制、开发、集成和维护等。

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 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：应用标识符的编号体系和注册规程

JR/T 0025.1—2018 中国金融集成电路（IC）卡规范 第1部分：总则

JR/T 0025.5—2018 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 0025.6—2018 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

JR/T 0025.7—2018 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

3 术语和定义

下列术语和定义适用于本文件。

3.1

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。

3.2

发卡行行为代码 issuer action code

发卡行根据TVR的内容选择的动作。

3.3

终端行为代码 terminal action code

收单行根据TVR的内容选择的动作。

4 缩略语

下列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）
ADA——应用缺省行为（Application Default Action）
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 Risk 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）
DIR——目录（Directory）
DOL——数据对象列表（Data Object List）
EF——基本文件（Elementary File）
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）
MAC——报文鉴别码（Message Authentication Code）
MDK——主密钥（Master Key）
MF——主文件（Master File）
n——数字型（Numeric）
P1——参数1（Parameter 1）
PAN——主账号（Primary Account Number）
PDOL——处理选项数据对象列表（Processing Options Data Object List）
PKI——公钥索引（Public Key Index）
PIN——个人识别码（Personal Identification Number）
PIX——扩展的专用应用标识符（Proprietary Application Identifier Extension）
PSE——支付系统环境（Payment System Environment）

RID——注册的应用提供商标识（Registered Application Provider Identifier）
SAD——被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 1）
SW2——状态字2（Status Word 2）
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 文件、数据元、数据对象列表

5.1 文件

5.1.1 概述

JR/T 0025—2018中的文件组织结构来自且符合GB/T 16649.4—2010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，卡片上的文件是一种树形结构。树的每一个分支是一个ADF或一个DDF。一个ADF是一个或者多个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DDF的入口点。

IC卡中能够读/写的数据文件中的数据对象是以记录方式保存的。文件的结构和引用方法取决于该文件的用途。文件的结构和引用的方法将在下面描述。除了5.1.5 描述的DIR文件以外，其他的IC卡可读/写数据文件的布局均由发卡行定义。

5.1.2 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FCI的数据对象的文件，见JR/T 0025.5—2018的表B.27。

5.1.3 应用基本文件（AEF）

短文件标识符（SFI）范围为1-10的AEF，包含一个基本数据对象或由多个“基本编码规则－标签长度值”（BER-TLV）的数据对象根据JR/T 0025.5－2018附录A组成的结构BER-TLV数据对象（记录）。一旦选定之后，范围为1-10的AEF只能如5.1.6.2 所述通过他的SFI来引用。

一个数据文件包括一组按记录号引用的记录序列。1-10号SFI引用的数据文件中只包括那些不由卡片解释的数据，即不在卡片内部过程中使用的数据。这种文件的结构定义成线性结构。根据GB/T 16649.4－2010规定，文件结构既可以是固定的，也可以是线性可变的。这由发卡行自行选择，并且不会影响对文件的读操作。

5.1.4 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 DF 映射为一个 ADF 或一个 DDF。可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 MF；

——GB/T 16649.4－2010 定义的一个 EF 对应一个 AEF。EF 不是另一个文件的入口点。

在JR/T 0025－2018中，若嵌入了DF，对与之相连的EF的访问是透明的。

5.1.5 目录结构

当卡片上存在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DIR文件中列出，支付系统DIR文件的位置由PSE的FCI指出。

目录结构允许以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（使用6.2.1.4 中的SELECT命令）。

根据GB/T 16649.5－2002的定义，DIR文件是一个AEF（亦即EF）和含下列数据对象的记录结构：

——本部分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。

5.1.6 文件引用

5.1.6.1 通过文件名引用

卡片中的任何ADF或DDF都可以通过他的DF名引用。ADF的DF名与他的AID对应或以AID作为DF名的开头。卡片中的每个DF名字应在该卡内是唯一的。

5.1.6.2 通过 SFI 引用

SFI用于选择AEF。在一个给定的应用中可以通过SFI来引用任何一个AEF。该SFI使用5个位（bit）来编码，其值在1～30的范围内。SFI编码将在使用他的各命令中描述，SFI的结构见表1。

表1 SFI 结构

数值	意义
1～10	JR/T 0025—2018 定义
11～20	支付系统定义
21～30	发卡行定义
注：每个SFI在一个应用以内应是唯一的。范围为11～20的SFI引用的AEF由支付系统分配管理。	

5.2 数据元

定义并解释借记/贷记应用数据交换过程中卡片和终端所需的相关数据元，包括数据元的名称、标识及功能等，见JR/T 0025.5－2018附录A和JR/T 0025.6-2018第8章。

5.3 数据对象列表（DOL）

有时，终端应卡片的要求需要建立可变的数据元列表用来向卡片发送。为了减少IC卡内对这些数据的处理，这个列表不需要进行TLV编码，而只是把若干数据单元连接成一个复合域。因为复合域中的数据单元不是TLV编码的，所以当IC卡收到数据时，需要知道该复合域的格式。因此，应在IC卡内包含DOL来定义复合域中的数据格式。JR/T 0025—2018使用的DOL包括：

——CDOL1：在第一次 GENERATE AC 命令中需要传送给卡片的数据对象列表。CDOL1 是终端在读应用记录处理过程中从卡片中读出的；

——CDOL2：在第二次 GENERATE AC 命令中需要传送给卡片的数据对象列表。CDOL2 是终端在读应用记录处理过程中从卡片中读出的；

——TDOL：列出生成 TC 哈希计算的数据对象（标签和长度）；

——DDOL：指定在 INTERNAL AUTHENTICATE 指令中，卡片要求终端送入卡片的终端数据标签和长度列表。

一个DOL是用一些条目连接而成的列表。每个条目代表一个加入复合域的单个数据元。每个条目的格式包括1～2个字节的标签来表明需要的数据对象，然后是1个字节的长度部分，表明本数据对象在命令数据中占据的字节长度。只有那些在JR/T 0025.5－2018附录A中定义为基本数据对象的标签才可以在DOL中使用。

终端应完成下列步骤以建立结构域：

a） 从 IC 卡读取 DOL；

b） 连接 DOL 中列出的所有数据单元。

数据单元在表上的连接顺序应与相应的数据对象在 DOL 中出现的顺序对应。应按照下列规则进行拼接：

——若 DOL 条目中指定的数据对象标签无法被终端识别，或这个标签代表了一个结构数据对象，终端将提供一个长度为 DOL 指定长度的数据元，并应把该数据元所有的数值部分设置为 16 进制的 0；

——若 DOL 条目中指定的数据对象可被终端识别，但该数据对象的值尚未被终端获取到，那么在命令区域上代表数据对象的部分应用 16 进制的 0 来填满；

——若 DOL 条目中指出的长度小于实际数据对象的长度，则应将实际的数据对象削减至 DOL 指出的长度。若数据对象是数字型（n）的，则从数据单元的最左端开始削减字节，否则从数据单元的最右端开始削减字节；若指出的长度比实际的数据长度大，需要把实际的数据填充至指定长度：

- 若数据对象是数字型（n）的，则从数据单元头部开始填充 16 进制的 0；
- 若数据对象是压缩数字型（cn）的，则在数据单元的末尾填充 16 进制的 FF；
- 若数据对象是其他格式的，则在数据单元末尾填充 16 进制的 0。

——若 DOL 条目中指定的数据对象可被终端识别，但不代表在当前交易中适用的数据，代表该数据对象的命令域部分将填充 16 进制的 0。

6 借记/贷记交易处理流程

6.1 流程描述

6.1.1 概述

图1中所规定的功能在借记/贷记交易处理中得到使用。尽管在标记为必备的功能中有些步骤是可选择的，但标记为必备的功能还是应在所有交易中得到执行。标记为可选的功能是可选择的并根据卡或终端的参数，或根据两者的参数共同决定。

具体交易流程实例见图1。

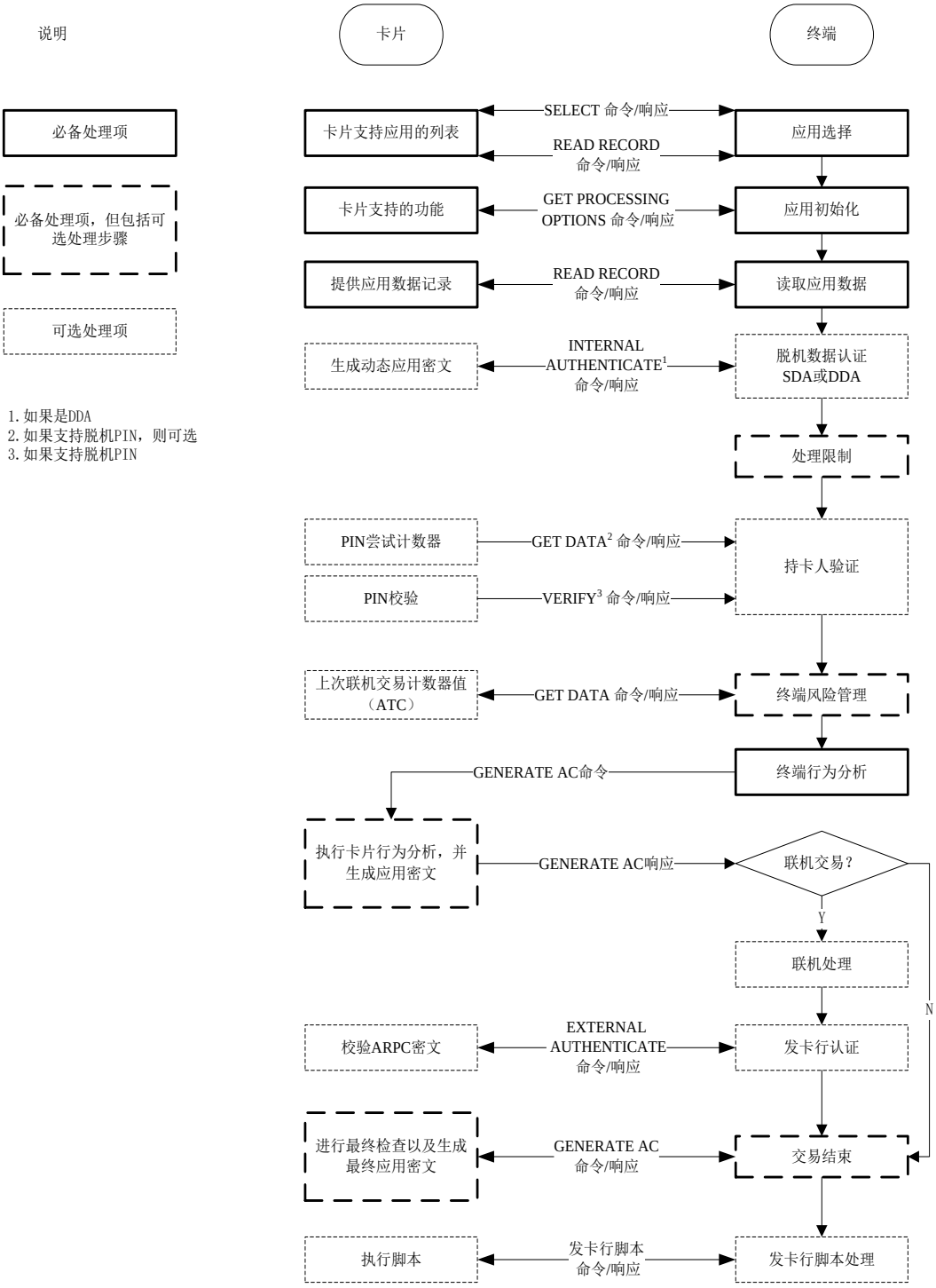

图1 交易流程实例

6.1.2 应用选择（必备）

当卡片插入终端时，终端决定哪些应用由卡片和终端共同支持，终端有两种选择应用的方式：

a) 终端检测终端和卡片都支持的应用并将这些应用显示，供用户选择；

b) 终端根据发卡行事先定义的优先级别自动选择卡片上优先级最高的应用。

终端发送SELECT命令选择应用，卡片返回FCI。若卡片支持SM算法，则FCI应包括请求SM算法指示器（标签为“DF69”）。

6.1.3 应用初始化（必备）

在终端选择应用之后，应请求卡片读取该应用的应用数据。由这些数据得知卡片具备的功能以及需要提供给卡片哪些支持。终端读取卡片指示的数据并使用支持的功能列表来决定要执行的处理。

具体见JR/T 0025.7－2018中13.4.3的规定。

6.1.4 读应用数据（必备）

终端使用读记录命令（READ RECORD）读出交易处理中使用的卡片数据，卡片在应用初始化的响应中提供AFL标记了这些数据所在的文件与记录号，终端应存储读出的所有可以识别的数据对象，不论是必备还是可选数据，以备将来交易使用。终端无法识别的数据对象（即终端无法识别他们的标签）不必存储，但是包含这种数据对象的记录可能仍然要以整体形式参与脱机数据认证过程，这取决于AFL的编码。

6.1.5 脱机数据认证（可选）

终端根据卡片和终端对这些方法的支持，决定是否使用脱机静态或动态数据认证来脱机认证卡片。若终端支持脱机数据认证功能，并且检测到卡片支持SDA或DDA，则终端应进行脱机数据认证。

SDA验证卡片在个人化以后重要的应用数据是否被非法修改。终端使用卡片上的发卡行公钥验证卡片静态数据，同时卡片上还包括发卡行公钥证书以及数字签名。若数字签名验证正确，则证实了卡片数据并未被修改。

DDA主要是用于防止伪造卡片。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（DDA/AC-CDA）两种。终端要求卡片提供由IC卡私钥签名动态交易数据生成的动态签名，动态交易数据是由终端和卡片为当前交易产生的唯一数据。终端用从卡片数据中获取的IC卡公钥来验证动态签名。若验证正确，则证实了此卡片不是由合法卡片复制出的赝品卡。复合动态数据认证/应用密文生成把动态签名生成与卡片的应用密文生成相结合，确保卡片行为分析时返回的应用密文来自于有效卡。

6.1.6 处理限制（必备）

终端通过处理限制来检查应用交易是否允许继续。检查内容包括应用生效期、应用失效期、应用版本号以及其他发卡行定义的限制控制条件，发卡行可以使用应用用途控制来限定卡片用于国内还是国际间，或能否用于现金、购物或服务。

6.1.7 持卡人验证（可选）

终端应具备持卡人身份验证功能。持卡人身份验证用来确认持卡人的合法性，以防止丢失或被盗卡片的使用。终端通过检查卡片的CVM列表确定使用何种验证方法：

——脱机明文 PIN 验证；

——联机 PIN 验证；

——签名；

——CVM 失败；

——不执行 CVM；

——签名与脱机明文 PIN 验证组合；

——身份证件验证。

6.1.8 终端风险管理（必备）

终端应具备风险管理功能，但其中的检查项是可以选择的。终端通过终端和卡片提供的数据可以进行最低限额（Floor Limit）检查、交易频度检查、新卡检查、终端异常文件检查、商户强制交易联机、随机选择联机交易等方式完成风险管理。

6.1.9 终端行为分析（必备）

终端应具备终端行为分析功能。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）。再由卡片返回给终端的IAC域设立卡片规则，在TAC设立终端规则。

决定交易处理之后，终端向卡片请求应用密文。不同的应用密文对应不同的交易处理：以TC为批准，ARQC为联机请求，AAC为拒绝。

6.1.10 卡片行为分析（必备）

卡片可执行发卡行定义的风险管理算法以防止发卡行被欺诈。当卡片收到终端的应用密文请求时，卡片执行卡风险管理检查，来决定是否要改变终端设定的交易处理，检查可能包括：先前未完成的联机交易、上一笔交易发卡行认证失败或脱机数据认证失败、达到了交易笔数或金额的限制等。卡片可以决定以下方式继续交易：

——同意脱机完成；

——联机授权；

——拒绝交易。

完成检查后，卡片使用应用数据及一个存储在卡上的应用密文过程密钥生成应用密文，将这个应用密文返回到终端。对于脱机批准的交易，TC以及生成TC的数据通过清算消息传送给发卡行，以备未来发生持卡人争议或退单时使用。当持卡人对交易有争议时，TC可以作为交易的证据还可验证商户或收单行（是否）未改动交易数据。

6.1.11 联机处理（可选）

若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，终端将卡片产生的ARQC报文送至发卡行进行联机授权，此报文包括ARQC密文，用来生成ARQC的数据以及表示脱机处理结果的指示器。在联机处理中，发卡行在联机卡片认证方法（CAM）过程中验证ARQC来认证卡片。发卡行可在他的授权决定中考虑这些CAM结果和脱机处理结果。

传送回终端的授权响应信息可包括发卡行生成的ARPC（由ARQC、授权响应码和卡片应用密文过程密钥产生）。此响应也可包括发卡行脚本，对卡片进行发卡后更新。

若授权响应包含ARPC而且卡片支持发卡行认证，卡片通过确认ARPC而执行发卡行认证，来校验响应是否是来自真实的发卡行（或其代理）。要在卡片里重新设置某些相关的安全参数必需成功得到发卡行认证，阻止犯罪者通过模拟联机处理来剽窃卡片的安全特性，以及通过欺诈性地批准交易来重设卡片的计数器和指示器。若发卡行认证失败，随后的卡片交易将发送联机授权，直到发卡行认证成功。若发卡行认证失败，发卡行有权设置卡片拒绝交易。

6.1.12 发卡行脚本处理（可选）

若发卡行在授权响应报文中包含了脚本，虽然终端可能对脚本不能理解，但终端仍需要将这些脚本命令发送给IC卡。在使用这些更新之前，卡片执行安全检查以确保脚本来自有效的发卡行，且在传输中

未有变动。这些命令对当前交易并不产生影响，主要会影响卡片的后续功能，如卡片应用解锁、卡片锁定、修改PIN等。

6.1.13 交易结束（必备）

除非交易在前几个步骤因处理异常被终止，否则终端应执行此功能用来结束交易。

卡片和终端执行交易结束来完成交易。一个经发卡行认可的交易可能因卡片中的发卡行认证结果和发卡行写入的参数而被拒绝。卡片使用交易处理、发卡行校验结果、以及发卡行写入的规则来决定是否重设基于芯片卡计数器和指示器。卡片生成TC来认可交易，生成AAC来拒绝交易。

若终端在授权消息之后传送清算信息，则TC应包括在该清算信息里。

6.2 交易步骤

6.2.1 应用选择

6.2.1.1 概述

应用选择是一个过程，决定哪个由卡片和终端共同支持的应用将被用于进行交易。这个过程分为两步骤：

a) 终端建立一个共同支持的应用的候选列表；

b) 列表中的某个应用被选择并确认用来处理交易。

应用选择应符合JR/T 0025.7—2018中13.4.2的规定，应用选择处理流程见图2。

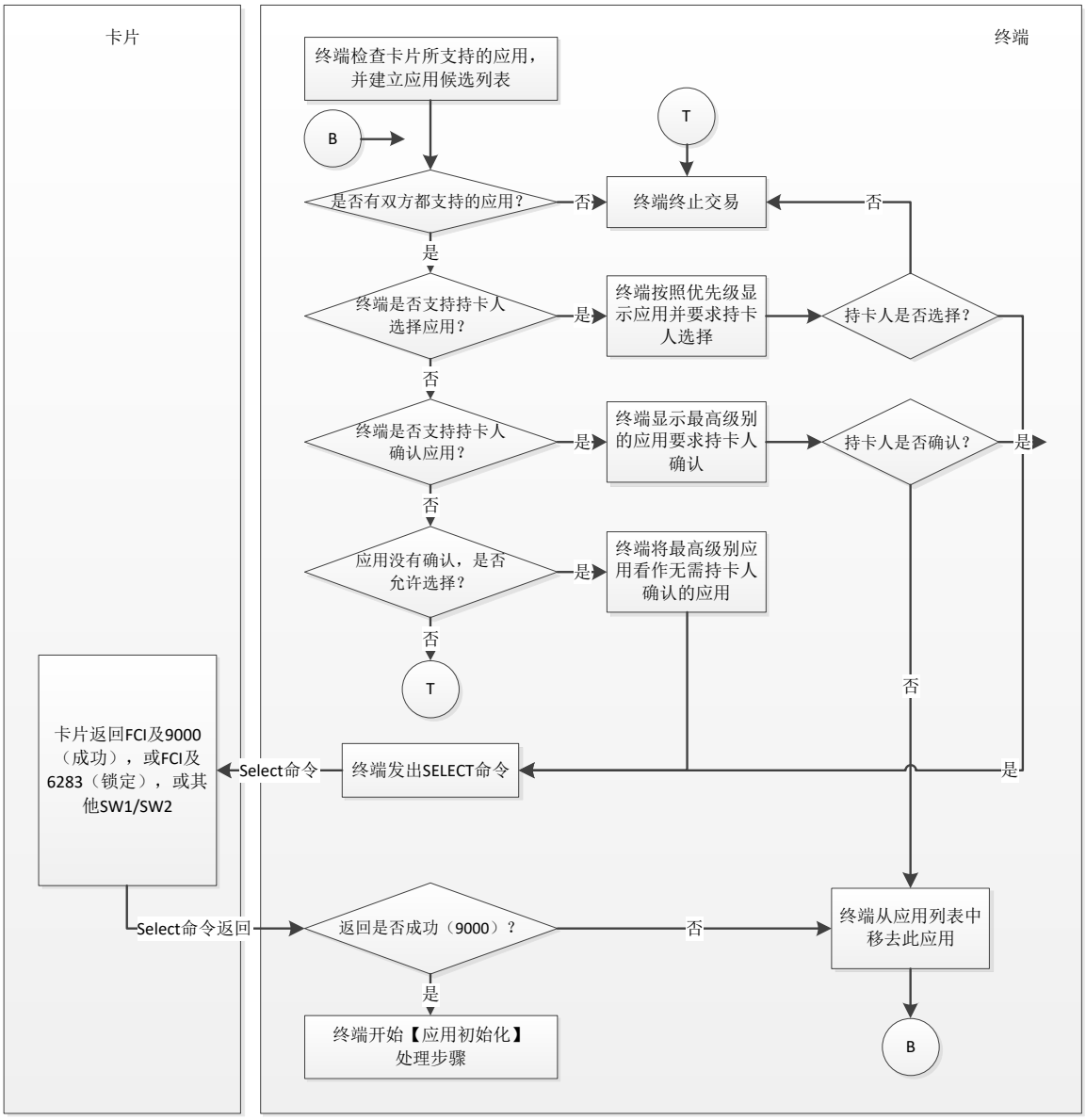

图 2　应用选择处理流程图

6.2.1.2　卡片数据元

应用选择流程中卡片数据元见表2。

表2　应用选择—卡片数据元

数据元	说明
ADF	ADF 是一个文件，他是包含应用数据元的 AEF 的入口。ADF 包含有关应用的信息。例如应用的名称、首选语言以及应用优先权。
AEF	AEF 包含处理中应用所用到的数据元。
AID	AID 由 RID 以及 PIX 组成。
DIR 文件	DIR 文件是列出目录里所包含文件的文件。终端使用 READ RECORD 命令来访问他。
FCI	FCI 是来自卡的有关应用的信息，提供对由终端发出的 SELECT 命令做出响应。

数据元	说明
支付系统目录	支付系统目录是包含有符合 JR/T 0025 应用的目录文件。
PSE	PSE 是名为“1PAY.SYS.DDF01”的 DDF。指明在 PSE 下面的文件结构的目录文件叫做支付系统目录。
PDOL	PDOL 是卡所需终端数据的标签和长度列表。终端在 SELECT 命令的卡片响应中获得他。终端在 GPO 命令下提供列表中所要求的数据给卡片。
日志入口（Log Entry）	包含交易明细记录所在卡片文件的 SFI 和记录的最大条数。
SFI	SFI 是 EF 的指示器。

6.2.1.3 终端数据

应用选择流程中终端数据元见表3。

表3 应用选择—终端数据元

数据元	说明
AID	AID 由 RID 以及 PIX 组成。
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（长度和内容都应一样），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。
支持应用列表	终端应当保存终端支持应用的 AID 列表。

6.2.1.4 命令

该流程中涉及的命令包括：

——SELECT：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，包括应用优先权、应用名称和首选语言等；在卡片对 SELECT 命令的响应中，响应码用来表示处理结果。若卡片做出响应包括 PDOL，则在应用初始化时处理 PDOL。在卡片对 SELECT 命令的响应中可能包含交易日志入口（Log Entry），若出现该数据元则表示该卡片支持交易日志；

——READ RECORD：终端发送 READ RECORD 命令到卡片，读取 PSE 中的记录（若支持目录选择）。命令包括读取文件的 SFI 以及文件里的记录号。卡片对 READ RECORD 命令作出响应，为终端提供所要求的记录。

6.2.1.5 建立候选应用列表

终端可通过两个途径建立共同支持应用的列表：

——终端首先尝试目录选择方法。若尝试失败，终端就使用 AID 列表选择方法。目录选择法中，终端从卡片读取一个文件。这个文件是卡片支持的应用列表。终端将卡片应用列表和终端应用列表里共同支持的所有应用包括在候选目录中；

——AID 列表选择方法对于卡片和终端都是必备的。在 AID 列表选择方法中，终端对终端应用列表中包含的每个应用都向卡片发送一个 SELECT 命令。若卡片响应表示卡片也支持该应用，终端就将应用添加到候选目录中。

若没有共同支持的应用，交易将被终止。若至少有一个共同支持的应用，处理过程如6.2.1.6 所述。

6.2.1.6 标识并选出应用

6.2.1.6.1 终端决定应用

若终端不支持持卡人选择应用或确认应用，终端会向不要求确认的具有最高优先级的应用发送一个SELECT命令。若卡片中有超过一个应用有最高优先级，终端可以向其中任意一个发送SELECT命令。

若用目录选择法来建立应用列表，SELECT命令的响应可能说明该应用已被锁定。若发生此种情况，而且在可用应用列表上有更多可用的应用，终端应向下一个优先级最高的应用发送SELECT命令。

6.2.1.6.2 持卡人决定应用

若终端支持显示供持卡人选择的应用列表，终端应向持卡人按优先级顺序给出应用列表以供选择。若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选择一个处理。持卡人从列表中选择应用，终端应发送SELECT命令选择应用。若用目录选择法建立应用列表，卡片对SELECT命令的响应可能说明应用已被锁定。若发生此种情况，而且在应用列表上有更多可用的应用，终端应显示“重试”并显示已排除了被拒绝应用的可用应用列表。若持卡人不选择应用，终端应终止交易。

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，终端应首先将优先级最高的应用提供给持卡人确认。若超过一个应用有同样的优先级，终端可根据遇到的先后次序或自行选择其中一个应用。若持卡人确认这个选择，终端应发送SELECT命令选择应用。若持卡人不确认，终端应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。若用目录选择法来建立应用列表，卡片对SELECT命令的响应可能说明该应用已被锁定。若发生此种情况，而且在应用列表上有更多可用的应用，终端应将该应用从可用应用列表中移除，并选择下一个可用的应用进行持卡人确认。

6.2.1.7 后续相关处理

后续相关处理包括：

——初始化应用处理：终端发送到卡片的 GPO 包括 PDOL 指定的所有终端数据元。若 PDOL 得到支持，应用选择时 PDOL 会被包括在 SELECT 响应里；

——读交易明细记录：对于需要访问交易明细记录的终端，发送 GET DATA 命令从卡片获取日志格式数据元，然后发送 READ RECORD 命令给卡片，逐条读取交易记录。

6.2.2 应用初始化

6.2.2.1 概述

在应用初始化处理中，终端向卡片发送GPO命令，表示交易处理开始。当发此命令时，终端向卡提供PDOL请求的数据元。PDOL是卡片在应用选择时提供给终端的标签和数据元长度的列表，处理选项数据对象列表（PDOL）是可选数据元。

卡片在GPO命令的响应中提供AFL，AFL是终端需要从卡片读取的文件和记录的列表。卡片还提供AIP，AIP是处理交易时卡片所执行功能的列表。

6.2.2.2 卡片数据

初始化应用处理的卡片数据见表4。

表4 初始化应用处理—卡片数据

数据元	说明
AFL	指示交易处理过程中终端需要的卡片数据所在卡片文件的 SFI 和记录范围。
数据元	说明

AIP	指示在此应用中卡片支持特定功能的能力列表，包括 SDA、标准 DDA、持卡人验证、终端风险管理、发卡行认证以及 DDA/AC。
FCI	FCI 是卡片相关应用的信息，在终端发送的 SELECT 命令的响应中。
PDOL	PDOL 是卡片请求的终端数据元的标签和长度的可选列表。他是终端在 SELECT 命令响应中得到的卡片 FCI 的一部分。终端在 GPO 命令中向卡片提供该列表所请求的数据元。

6.2.2.3 终端数据

终端将卡片需要的数据元通过PDOL传送给卡片。

6.2.2.4 命令

涉及的命令为GPO。

终端发送GPO命令通知卡片交易处理开始。终端在GPO命令提供卡片PDOL中指定的终端数据。

6.2.2.5 处理流程

应用初始化处理流程见图3。

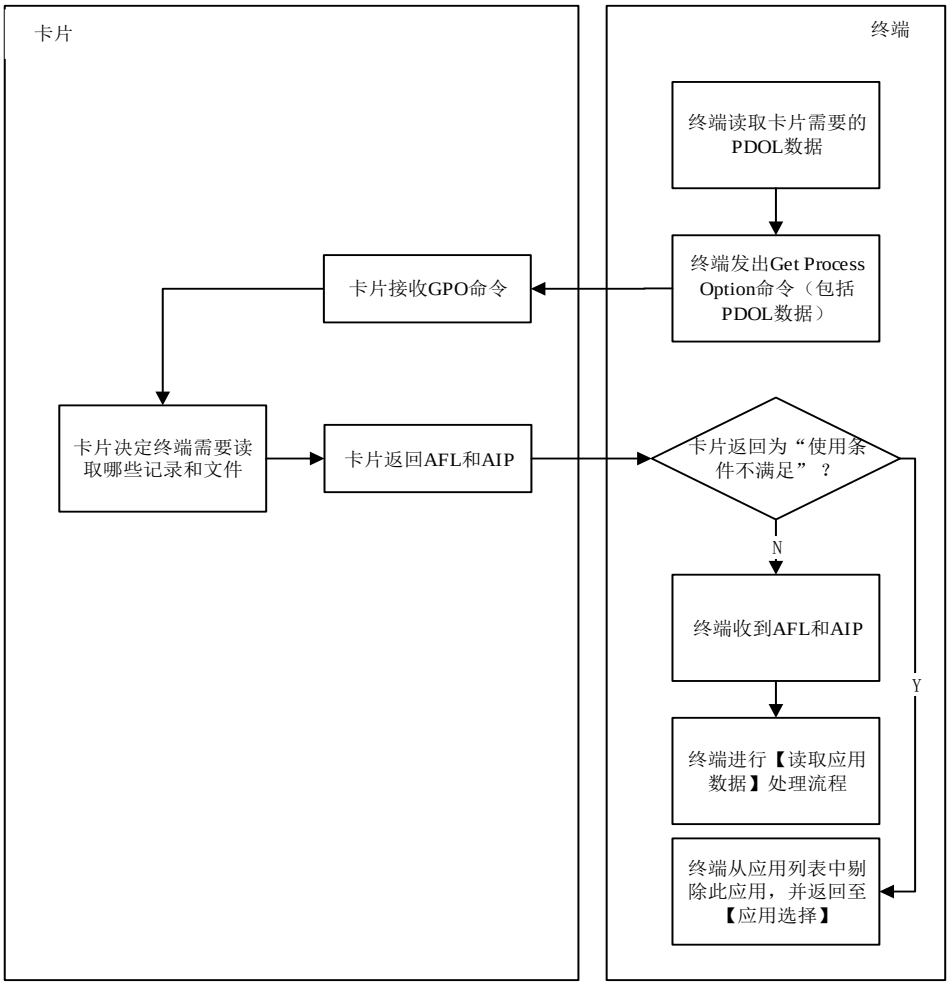

图 3 应用初始化处理流程图

步骤1：终端向卡片发送GPO命令。若终端在应用选择时获取PDOL，终端应组织所有卡片在PDOL中请求的数据元并传给卡片；

步骤2：卡片收到GPO命令，将要读取的文件或记录并定位或建立AFL；终端可能在GPO响应中得到不同的AIP返回；

步骤3：终端接收卡片对GPO命令的响应。若响应中包含AIP和AFL做出响应，终端开始读取应用数据。若卡片响应为“使用条件不满足”，终端将该应用从可用应用列表里移除，返回应用选择流程。

6.2.2.6 前期相关处理

前期相关处理为应用选择。卡片在SELECT命令响应中将PDOL（若存在）作为FCI的一部分提供给终端。

6.2.2.7 后续相关处理

后续相关处理包括：

——读取应用数据：终端根据 GPO 命令响应中由卡片提供的 AFL，确定从卡片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：终端根据 GPO 命令响应中由卡片提供的 AIP，确定卡片是否支持脱机数据认证；

——持卡人验证：终端根据 GPO 命令响应中由卡片提供的 AIP，确定卡片是否支持持卡人验证；

——联机处理：终端根据 GPO 命令响应中由卡片提供的 AIP，确定卡片是否支持发卡行认证。

6.2.3 读应用数据

6.2.3.1 概述

读取应用数据时，终端读取交易处理中必要的卡片数据，并决定SDA或DDA中使用的数据。

6.2.3.2 卡片数据

读应用数据中上次卡片返回的卡数据见表5，读应用数据中的卡片数据见表6 。

表5 读应用数据—上次卡片返回的卡数据

数据元	说明
AFL	指示包含终端将要读取的用来交易处理的卡片数据的文件和记录范围。 每个条目指定了要从文件读取的最初记录和最终记录号以及哪些记录要用在脱机数据认证中。

表6 读应用数据—卡片数据

数据元	说明
AEF	卡片数据文件，包含应用处理中使用的数据。AEF 由一系列记录号定址的记录组成。终端用 READ RECORD 命令读取这些记录。READ RECORD 命令包含要读取的由终端从 AFL 获得的 SFI 和记录号。
SFI	SFI 是用来唯一标识应用定义文件的符号。在 AFL 里列出，终端用他来标识要读取的文件。

表7列出了读记录时，IC卡中应具备的数据对象。JR/T 0025—2018中定义的其他IC卡数据对象都是可选的。

表7 读应用数据－卡片必备数据对象

标签	值	存在性
“5F24”	应用失效日期	必备
“5A”	应用主账号	必备
“8C”	卡片风险管理数据对象列表 1	必备
“8D”	卡片风险管理数据对象列表 2	必备

6.2.3.3 终端数据

读取应用数据功能中不使用终端数据。

6.2.3.4 命令

涉及的命令为READ RECORD。终端为每个要读取的记录向卡片发送一条READ RECORD命令。此命令包括标识文件的一个SFI以及一个记录号来标识文件里的记录。

卡片在READ RECORD命令的响应提供被请求的记录。

6.2.3.5 处理流程

终端根据卡片的应用文件定位器（AFL）决定从卡片读取哪些记录。

对于每个AFL条目，终端用READ RECORD命令请求读取首条指定的记录。当此记录从卡返回，终端就为随后的处理保留该数据对象。若AFL条目指明脱机数据认证时对静态数据的认证需要此记录，终端将记录数据放入静态数据认证输入列表。终端继续读取文件记录直到最后一条指定要读取的记录为止。

卡片读应用数据处理流程见图4。

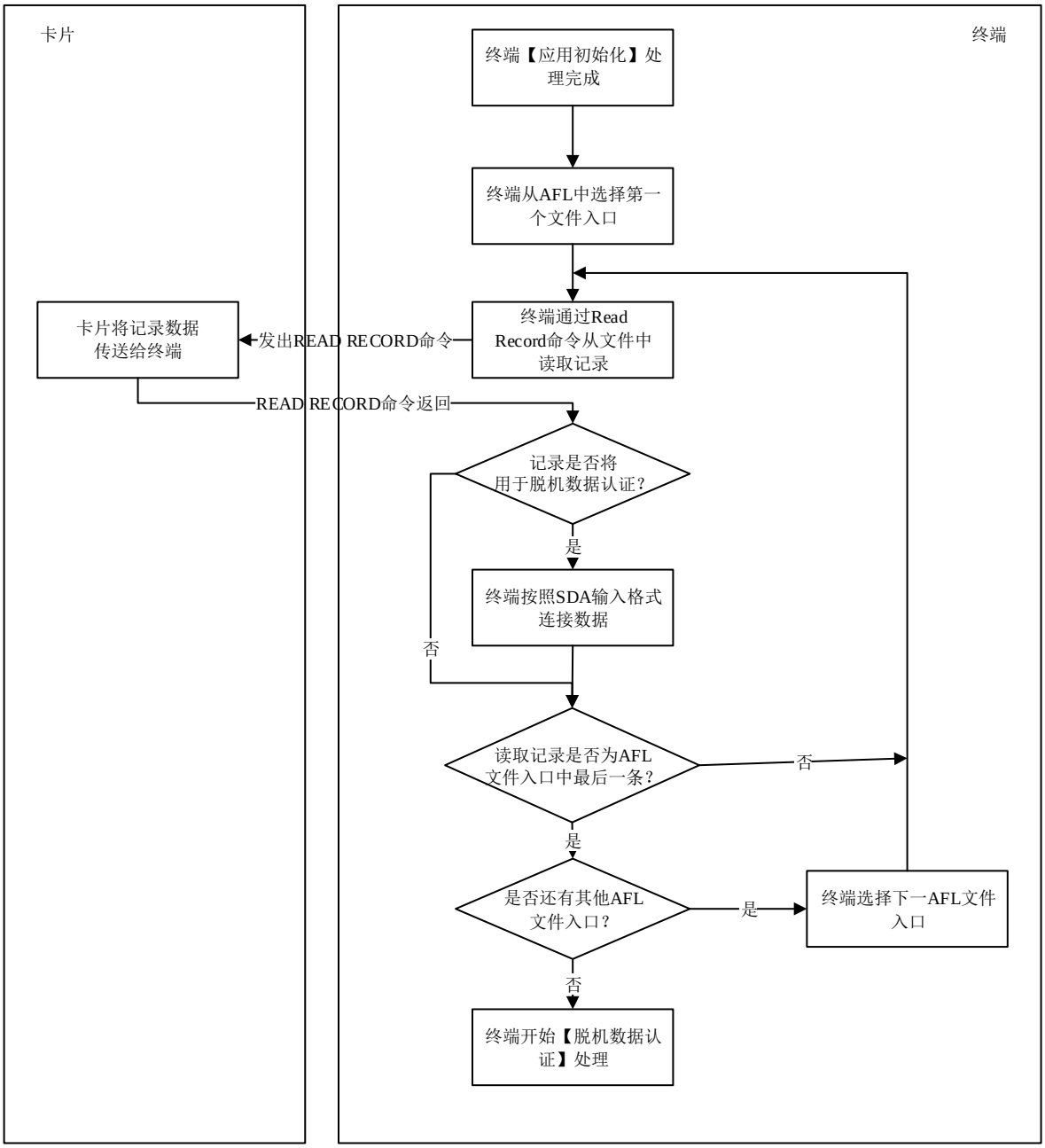

图 4 读应用数据处理流程图

6.2.3.6 前期相关处理

前期相关处理包括：终端使用应用初始化时卡片提供的AFL，以读取应用数据。

6.2.3.7 后续相关处理

后续相关处理包括：

——脱机数据认证：SDA 和 DDA 用读取应用数据时得到的参与认证的静态数据来验证带签名的静态应用数据；

——其他功能：用读取应用数据时得到的数据进行处理。

6.2.4 脱机数据认证

6.2.4.1 概述

脱机数据认证是终端使用公钥密码技术认证来自卡片数据的处理过程。

脱机数据认证有两种形式：静态数据认证（SDA）和动态数据认证（DDA）。

在静态数据认证处理中，终端认证卡的静态（不变的）数据。静态数据认证确保发卡行选择的卡片数据元自卡片个人化以来没有被改变。

在动态数据认证处理中，终端不仅认证静态的卡数据，也认证卡片使用能够唯一标识一笔交易的交易数据生成的签名。动态数据认证除了确保发卡行选择的卡片数据元自卡片个人化以来没有受到改变，还确认卡片是真卡而不是通过从有效卡复制数据制作的伪卡（非法复制）。动态数据认证可以是标准动态数据认证（DDA），也可以是复合动态数据认证（CDA）/应用密文生成。

脱机数据认证结果决定了卡片和终端是脱机批准交易、进行联机认证还是脱机拒绝交易。联机认证系统在他们的认证响应决定中可以使用脱机数据认证结果。

所有允许脱机交易的终端应支持SDA和DDA，CDA可选支持。对于不允许脱机交易的卡片而言，脱机数据认证支持是可选的。支持脱机交易的卡片应支持DDA，CDA可选。

6.2.4.2 密钥及认证

密钥及认证见JR/T 0025.7－2018。

6.2.4.3 确定脱机数据认证的方法

任何交易只执行一种脱机数据认证方法，复合动态数据认证/应用密文生成优先权最高，标准动态数据认证其次，最后是静态数据认证。表8表明了根据卡片和终端的共同支持情况决定所要执行的脱机数据认证方法。

表8 脱机数据认证处理优先权

AIP 表明卡支持	终端支持 SDA	终端支持 SDA 和 DDA	终端支持 SDA，DDA 及 CDA
SDA	SDA	SDA	SDA
SDA DDA	SDA	DDA	DDA
SDA DDA CDA	SDA	DDA	CDA

6.2.4.4 静态数据认证（SDA）

6.2.4.4.1 概述

表9和表10描述终端和卡片为执行SDA时确认此卡片数据未被改变所使用的重要数据。

表9 SDA 中使用的终端数据

数据元	说明
CA 公钥	储存在终端的支付系统公钥，用于验证来自卡的用 CA 私钥签署的发卡行公钥证书。
CA PKI	与 RID 一同使用，用来指定哪个 CA 公钥用于脱机数据认证。

RID	标识支付系统的应用标识符的一部分。
TVR	标识从终端角度来看的处理功能情况。

表10 SDA 中使用的卡片数据

数据元	说明
CA PKI	用来标识脱机数据认证的每个公钥，与注册的应用提供商标识一起标识每个认证公钥。
发卡行公钥证书	发卡行公钥证书包含用 CA 私钥签署的发卡行公钥。
发卡行 RSA 公钥指数	在 RSA 算法中使用该指数来恢复签名静态应用数据。
发卡行 RSA 公钥余项	若有必要，发卡行 RSA 公钥余项包含发卡行 RSA 公钥未列入发卡行公钥证书的部分。
SDA 失败指示器	内部指示器，若 SDA 失败且交易被脱机拒绝进行，则他由卡片设置并保存。
SAD	静态应用数据是用发卡行私钥签名，若是用 RSA 算法签名的，则包含卡片重要数据的哈希值。

6.2.4.4.2 处理流程

SDA处理流程见图5。

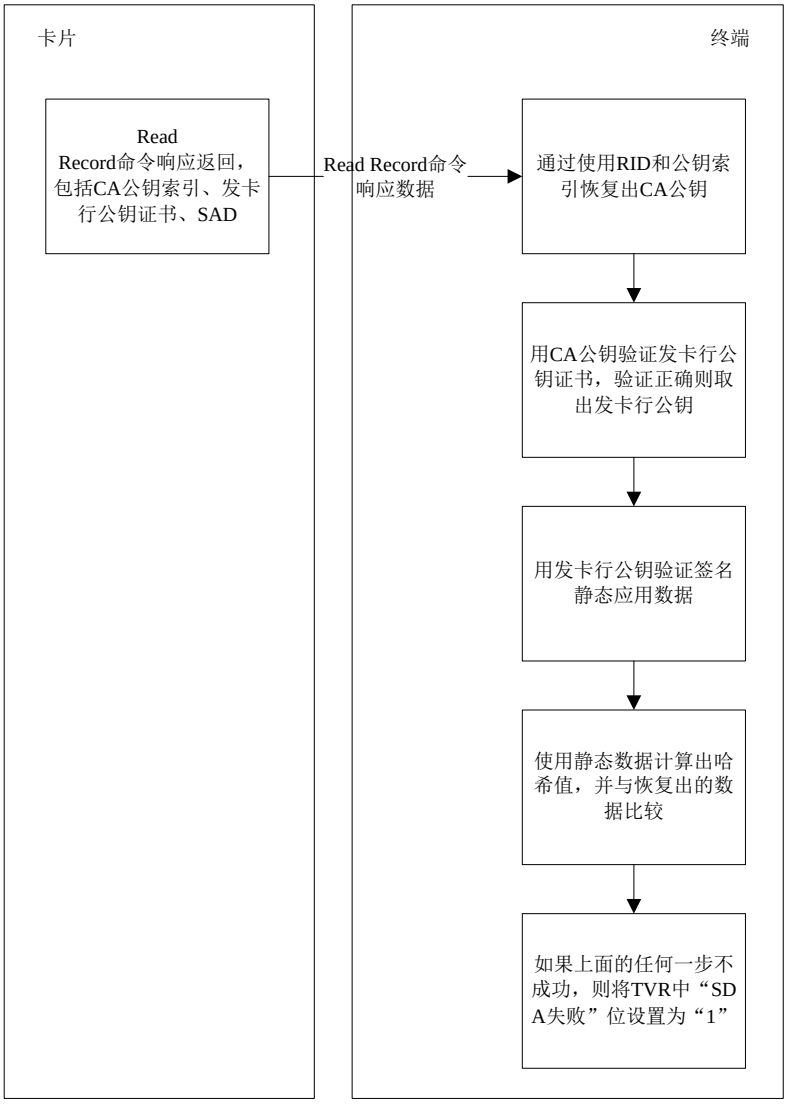

图 5　SDA 处理流程图

SDA过程中，卡片没有执行任何处理，以下概述了终端执行的处理步骤：

a）　CA 公钥的获取。终端使用卡片上的 CA PKI 以及 RID 来获取存储在终端的 CA 公钥和相关信息；

b）　发卡行公钥的获取。终端用 CA 公钥验证发卡行公钥证书，验证正确则从发卡行公钥证书中取出发卡行公钥；

c）　SAD 的验证。终端用发卡行公钥验证签名静态应用数据，若验证不正确，则数据可能被改变过，SDA 认证失败。

若以上所有步骤得以成功执行，则SDA通过。

若SDA失败，终端设置终端验证结果中的相应指示器，以显示SDA结果，并在随后的处理中使用该指示器决定交易的处理。

6.2.4.5　动态数据认证

6.2.4.5.1　概述

若要执行脱机动态数据认证，终端用发卡行公钥和CA公钥验证卡片的静态数据，处理过程和SDA相似。验证了静态数据后，终端向卡片申请动态签名。这要求使用内部认证命令实现DDA以及使用第一个AC生成命令实现CDA/应用密文生成。

卡片用卡片私钥对终端随机数和来自卡片的动态数据进行签名，生成一个数字签名，叫做签名动态应用数据。用CDA/应用密文生成方法产生的签名数据包括应用密文，卡片把这个动态签名发送给终端。

终端用已从卡片公钥证书中获取的卡片公钥验证卡片的动态数据签名。若验证正确，意味着卡片数据没有被改变且不是伪卡。

6.2.4.5.2 动态数据认证处理的数据元

终端将用SDA的终端数据和表11中描述的附加动态数据认证数据进行动态数据认证。

表11 动态数据认证中使用的终端数据

数据元	说明
DDOL	若卡片不提供动态数据认证数据对象列表，则终端使用缺省的动态数据认证数据对象列表，该列表包含终端不可预知数字的标签。
不可预知数字	由终端生成的不可预知的、唯一标识一笔交易的数字，该数字通过内部认证命令发送到卡片。

所有的静态数据认证数据，除SAD以外，都用于动态数据认证。此外，表12中描述的数据也用于动态数据认证。

表12 动态数据认证中使用的卡片数据

数据元	说明
DDA 失败指示器	内部指示器，若标准动态数据认证失败且交易被脱机拒绝，则他由卡片设置并保存。
DDOL	动态数据认证处理中，要传递给卡片的终端数据对象的标签列表。
卡片动态数字	卡片生成的唯一数字，并作为 CDA/应用密文生成中动态签名的部分由终端验证。
卡片私钥	卡片用他生成动态签名。
卡片公钥证书	包含用发卡行私钥签名的卡片公钥。
卡片 RSA 公钥指数	在 RSA 算法中使用该指数来恢复签名动态应用数据。
卡片 RSA 公钥余项	若有必要，卡片 RSA 公钥余项包含卡片 RSA 公钥未列入卡片公钥证书的部分。

所有在SDA中使用的数据元，除动态数据认证数据对象列表以外，都用于CDA/应用密文生成。此外，表13中描述的数据也被使用。

表13 CDA/应用密文生成中使用的卡片数据

数据元	说明
应用密文	卡片在 GENERATE AC 命令响应里返回的加密密文。若复合动态数据认证/应用密文生成在 ARQC 或 TC 中返回，ARQC 或 TC 是动态签名验证的一部分。
密文信息数据	卡片提供密文类型信息，终端在复合动态数据认证/应用密文生成中验证。

6.2.4.5.3 标准 DDA 处理流程

卡片DDA处理流程见图6。

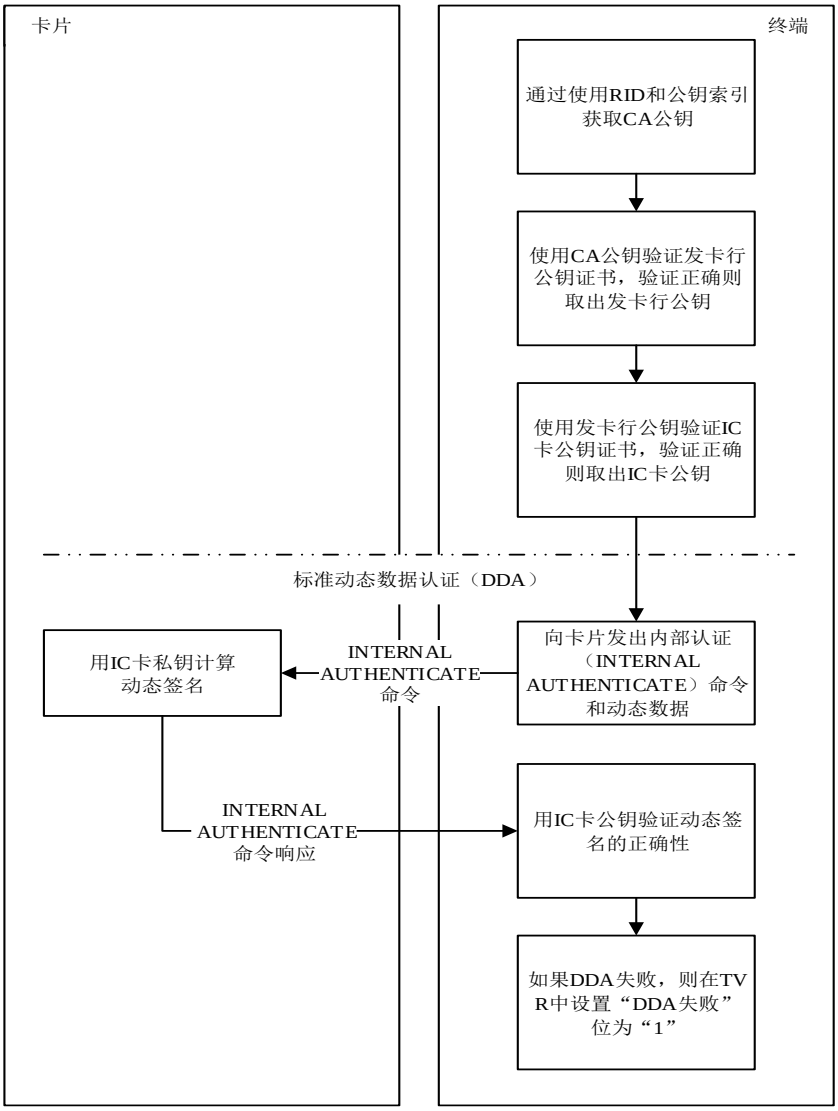

图 6 DDA 处理流程

这个处理过程，除了动态签名由卡片生成以外，其他都是由终端执行的。处理过程如下：

步骤1：CA公钥的获取。终端用CA PKI以及卡片中的RID来获取储存在终端中的CA公钥以及相关信息；

步骤2：发卡行公钥的获取。终端用CA公钥验证发卡行公钥证书，验证正确则从发卡行公钥证书中取出发卡行公钥；

步骤3：IC卡公钥的获取。终端用发卡行公钥验证IC卡公钥证书，验证正确则从IC卡公钥证书中取出IC卡公钥。若IC卡公钥证书验证不正确，则DDA失败；

步骤4：动态签名生成。终端发送包括动态随机数的INTERNAL AUTHENTICATE命令给卡片。卡片用IC卡私钥生成一个动态签名，把此动态签名传递给终端；

步骤5：动态签名校验。终端用IC卡公钥验证动态签名，若验证不正确，则DDA失败。

6.2.4.5.4 CDA 处理流程

对于CDA，终端执行DDA的步骤1到3。终端要求使用第一个GENERATE AC命令生成的动态密文。不使用INTERNAL AUTHENTICATE命令。对此密文的要求和认证包括以下步骤：

a) 动态签名生成（仅 CDA）。终端行为分析中，若终端要求一个联机密文（授权请求密文）或脱机批准密文（交易证书），第一个 GENERATE AC 命令表明 CDA 即将被执行。若卡片决定的应用密文是一个交易证书或授权请求密文，卡片就用 IC 卡私钥签名应用密文及相关数据，并在 GENERATE AC 命令响应中把动态签名返回给终端；
b) 动态签名校验（仅 CDA）。卡片行为分析中，若最初的 GENERATE AC 响应包含一个交易证书或授权请求密文，终端用 IC 卡公钥验证动态签名。若签名验证正确，交易就根据所收到的密文的类型继续进行。若签名验证失败，则交易脱机拒绝。

6.2.4.6 前期相关处理

前期相关处理包括读取应用数据。终端从卡片读取应用数据，此数据包括为支持脱机数据认证方法所要求的数据。AFL和SDA标签列表指明了SDA中用于认证静态数据哈希值的数据以及动态数据认证中认证IC卡公钥证书的数据。

6.2.4.7 后续相关处理

后续相关处理包括：

——终端行为分析：终端用脱机数据认证结果，卡片和终端参数来决定交易是否要被脱机拒绝，还是进行联机认证，或脱机批准。当要执行 CDA 且交易要被发送联机或脱机批准时，终端在 GENERATE AC 命令里设置了 CDA 指示器；

——卡片行为分析：对于 SDA 或 DDA，若上笔交易静态数据认证失败且交易被脱机拒绝，卡片就设置 CVR 中的相关指示器。若上笔交易动态数据认证失败且交易被脱机拒绝，卡片也在 CVR 设置一个类似的指示器。若 SDA 或 DDA 失败了，且要脱机拒绝交易，应设置 SDA 失败指示器或 DDA 失败指示器。对于 CDA，若从终端收到 GENERATE AC 命令表明将要执行 CDA，卡片就返回授权请求密文和交易证书应用密文，该密文用 IC 卡私钥签名；

——联机处理：对于 CDA，当返回的应用密文是动态签名，终端用 IC 卡公钥验证此签名。若验证成功，终端根据应用密文把处理继续下去。若验证失败，则交易脱机拒绝；

——交易结束：联机认证后，卡片允许根据发卡行认证选项和结果来重设 SDA 失败指示器或 DDA 失败指示器。若 SDA 或 DDA 失败了，且因联机认证不能完成，交易要被脱机拒绝，就设置 SDA 失败指示器或 DDA 失败指示器；

——CDA：若 CDA 失败且返回的应用密文是 ARQC，则终端发送第二个 GENERATE AC 命令请求 AAC。若 CDA 失败且返回的应用密文是 TC，则交易被脱机拒绝并不要求第二个 GENERATE AC 命令。

6.2.5 处理限制

6.2.5.1 概述

终端使用终端和卡片的数据元执行处理限制功能，终端应支持对应用版本、生效日期和失效日期以及交易点条件的有关检查。

6.2.5.2 卡片数据元

表14列出并描述了处理限制中用到的卡片数据元。这些数据元及其用法的详细说明见JR/T 0025.5－2018附录A。

表14 处理限制—卡片数据元

数据元	说明
应用版本号	该数据元（标签“9F08”）显示了卡片的应用版本。终端将其用于应用版本号的检查。
AUC	AUC 是可选数据元，他表明了发卡行有关卡片应用在地域以及所允许的服务方面的所有限制，由终端用于应用用途控制检查。
发卡行国家代码	发卡行国家代码是 JR/T 0025－2018 的数据元，表明发卡的国家，由终端用于应用用途控制检查。
应用生效日期	应用生效日期是应用开始使用的日期。
应用失效日期	应用失效日期过后，应用即被禁止。

6.2.5.3 终端数据元

表15列出了处理限制中用到的终端数据元。这些数据元及其用法的详细说明见JR/T 0025.5－2018附录A。

表15 处理限制—终端数据元

数据元	说明
应用版本号	该数据元（终端标签“9F09”）表明了终端的应用版本，他被终端用于应用版本号的检查，遵循此规范的卡应用版本号待定。
终端性能	表明终端关于卡片数据输入，持卡人验证和安全的性能。由终端用于应用用途控制的检查。
终端国家代码	该数据元表明终端所在的国家，由终端用于应用用途控制检查。
交易日期	这是终端提供的交易发生的当地日期，由终端用于应用生效日期和失效日期检查。
交易类型	该数据元表明金融交易的类型，由终端用于应用用途控制检查。

6.2.5.4 处理限制流程图

处理限制流程见图7。

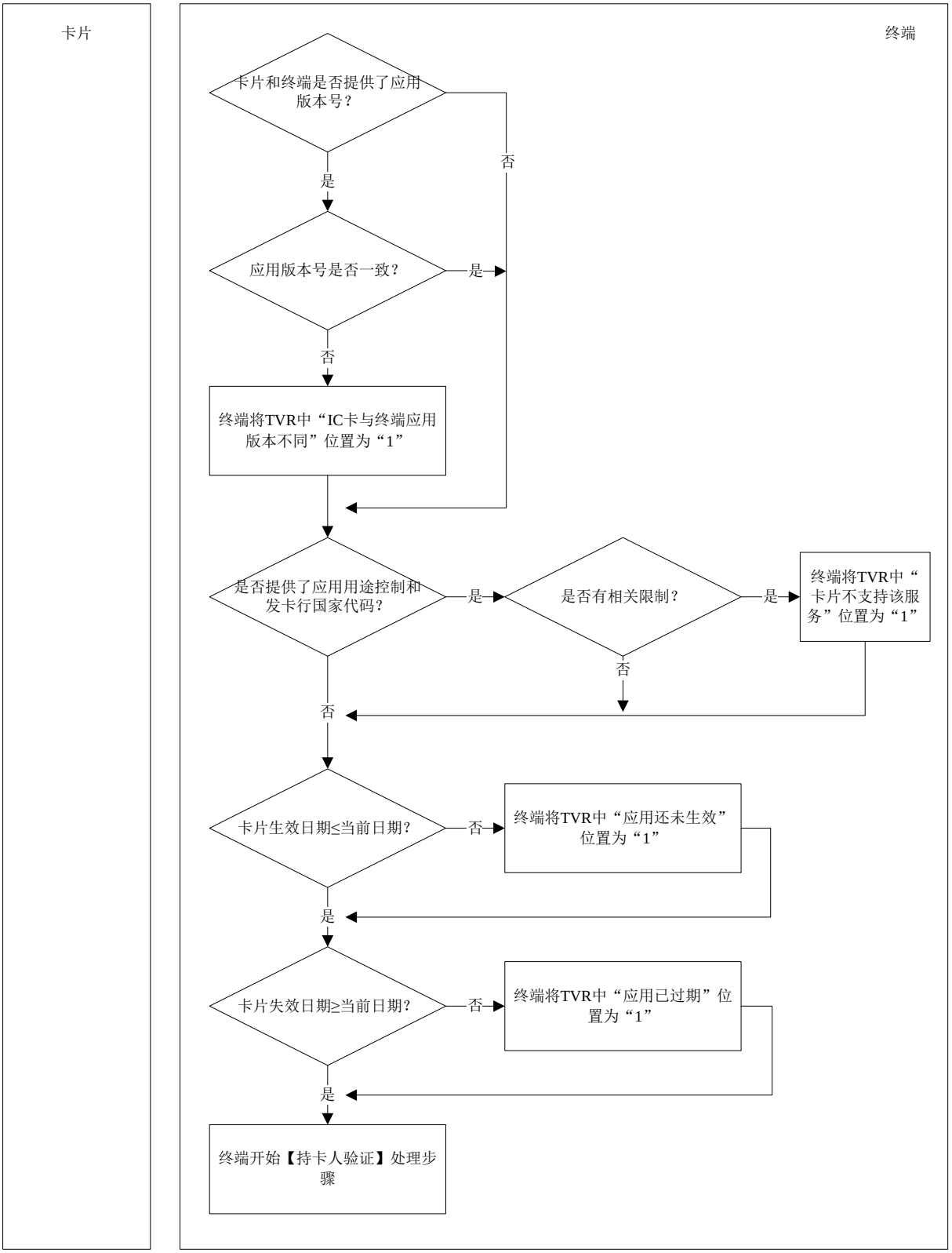

图 7　处理限制流程图

6.2.5.5　应用版本号检查

终端把卡片的应用版本号和终端的应用版本号相比较，看他们是否相同。若不相同，终端在TVR里显示出应用版本不一致。

6.2.5.6 应用用途控制检查

应用用途控制检查过程中，终端检查了交易点各方面的情况以决定处理是否要继续。下列交易包括这些限制检查：

——是否可用于国内现金/商品/服务业务；

——是否可用于国际现金/商品/服务业务；

——是否可用于 ATM；

——是否可用于除 ATM 外的设备。

6.2.5.7 应用生效日期检查

应用生效日期检查通过验证卡片的应用生效日期（若存在）早于等于终端的当前交易日期，确认应用已经生效。若生效日期晚于交易日期，终端就在终端验证结果中指示应用还未生效。

对于卡片，应用生效日期是可选的。对于终端，若卡片存在该数据元，应用生效日期的检查就是必备的。

6.2.5.8 应用失效日期检查

应用失效日期检查通过确认卡片的应用失效日期晚于等于终端的当前交易日期，验证应用还未失效。若失效日期早于交易日期，终端就在终端验证结果中显示应用已经失效。

6.2.5.9 前期相关处理

前期相关处理为读取应用数据。终端使用READ RECORD命令获得应用版本号以及卡片的应用失效日期。若存在，应用用途控制、发卡行国家代码和应用生效日期，则他们也被从卡片中读取出来。

6.2.5.10 后续相关处理

后续相关处理为终端行为分析。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若应用版本不一致、卡片未生效或卡片已失效、卡片不支持所请求的服务时，应采取怎样的处理。

6.2.6 持卡人验证

6.2.6.1 概述

持卡人验证用来确保持卡人是合法的，卡片不是丢失的或被盗的。

持卡人验证中，终端选择使用的CVM并执行该处理。CVM处理的结果在随后的处理中起作用。支持的持卡人验证方法包括：

——脱机明文 PIN 验证；

——联机 PIN 验证；

——签名；

——CVM 失败；

——不执行 CVM；

——签名与脱机明文 PIN 验证组合；

——身份证件验证。

签名、身份证件验证可以和脱机PIN验证方式结合起来。持卡人验证方法处理被设计为可支持附加的持卡人验证，比如被采用的生物识别技术。用脱机PIN方式在卡片内部完成了PIN的确认。脱机PIN验证结果包括在联机授权报文中，在发卡行的授权决定里应予以考虑。

终端从卡片规定的持卡人验证方法列表中选择要采用的持卡人验证方法。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。若持卡人验证失败，持卡人验证方法列表也会指定终端的行为。

6.2.6.2 卡片数据

终端将表16、表17和表18中描述的卡片数据用于CVM列表处理。这些卡片数据元及其用法的详细说明见JR/T 0025.5－2018附录A。

表16 CVM 列表处理—卡片数据元

数据元	说明
AIP	包含一个指示器，标明卡片是否支持持卡人验证。此指示器应设置为“1”。
CVM 列表	卡片应用 CVM 列表先后顺序。卡片可以包含多种 CVM 列表以用于不同的环境，比如国际和国内交易。CVM 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二个金额； ● CVM 条目：CVM 列表可能包括不止一个条目，每个条目包含子域和说明，详见表 17。

表17 CVM 列表

子域	说明
CVM 代码	若持卡人验证失败，即指定要采取的行动。可以选择处理下一个 CVM 或中止持卡人验证处理。
CVM 类型	CVM 要执行的类型，例如脱机 PIN 验证。
CVM 条件	当要用到 CVM 条目时的条件，例如，若终端支持该 CVM 类型（脱机 PIN）。
注：示例见JR/T 0025.5－2018第11章。	

表18 脱机 PIN 验证处理—卡片数据元

数据元	说明
ADA	若脱机 PIN 重试次数超限，卡片用该数据元来决定要采取怎样的行动。
CVR	包含卡片为下列情况设置的指示器： ● 执行了脱机 PIN 验证； ● 脱机 PIN 验证失败； ● PIN 重试次数超限； ● 因 PIN 重试次数超限，应用锁定。
PIN 重试次数计数器	剩余的脱机 PIN 重试次数。每次持卡人脱机 PIN 验证失败时，PIN 重试次数计数器都减 1。若持卡人输入与存储在卡中参考 PIN 一致的 PIN 或重置 PIN 重试次数计数器的脚本命令执行成功，PIN 重试次数计数器被重置为 PIN 重试次数上限。
PIN 重试次数上限	针对某一应用，发卡行指定的所能允许的连续输入错误 PIN 的最大次数。
参考 PIN	持卡人 PIN，储存在卡片的安全位置。

6.2.6.3 终端数据

表19 中描述的终端数据用于持卡人验证处理。这些数据元及其用法的详细说明见JR/T 0025.6—2018附录A。

表19 持卡人验证处理—终端数据元

数据元	说明
加密 PIN 数据	在密码键盘加密交易 PIN 用于联机验证。
密码键盘保密密钥	密码键盘使用的用来加密输入的脱机 PIN 的保密密钥，且读卡器用他来给加密 PIN 解密。当密码键盘和读卡器没有集成为一个不受外界干预的一体设备，这个密钥是必须的。此密钥和用于脱机加密 PIN 的密钥不同。
终端性能	表明了终端支持的持卡人验证方法。
TVR	在终端验证结果里为下列情况设置指示器： ● 持卡人验证不成功； ● 不可识别的持卡人验证方法； ● PIN 输入次数超限； ● 需要 PIN 输入而没有密码键盘或密码键盘不能工作； ● 需要 PIN 输入，有密码键盘但 PIN 没有输入； ● 输入联机 PIN。
交易 PIN	包含持卡人为 PIN 验证输入的数据。

6.2.6.4 命令

以下命令用于脱机PIN处理：

——GET DATA：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 输入次数是否超限，或接近超限。GET DATA 命令包含了 PIN 重试计数器标签。若 PIN 输入计数器在一个私有数据文件内，卡就将一个错误响应返回给 GET DATA，于是终端避开检查 PIN 输入次数计数器，继续脱机 PIN 验证处理；

——VERIFY：用于脱机明文 PIN 验证。若卡片和终端支持脱机 PIN 处理，则他们支持 VERIFY 命令。VERIFY 命令包括持卡人输入的 PIN 并开始卡片对这个 PIN 与储存在卡上的参考 PIN 的比较。卡片的响应指出下列情况中的一种：

- PIN 匹配；
- PIN 不相符，且 PIN 重试的剩下次数是“n”。若“n”等于“0”，则在当前交易中 PIN 输入次数已经超过了；
- 先前交易中，PIN 输入次数就已超过了。

6.2.6.5 处理流程

6.2.6.5.1 概述

持卡人验证处理分成两部分，为卡片的CVM列表处理与执行持卡人验证。

6.2.6.5.2 CVM 列表处理

卡片在CVM列表处理中除了给终端提供CVM列表以及其他必需数据外不起别的作用。CVM列表处理流程见图8。

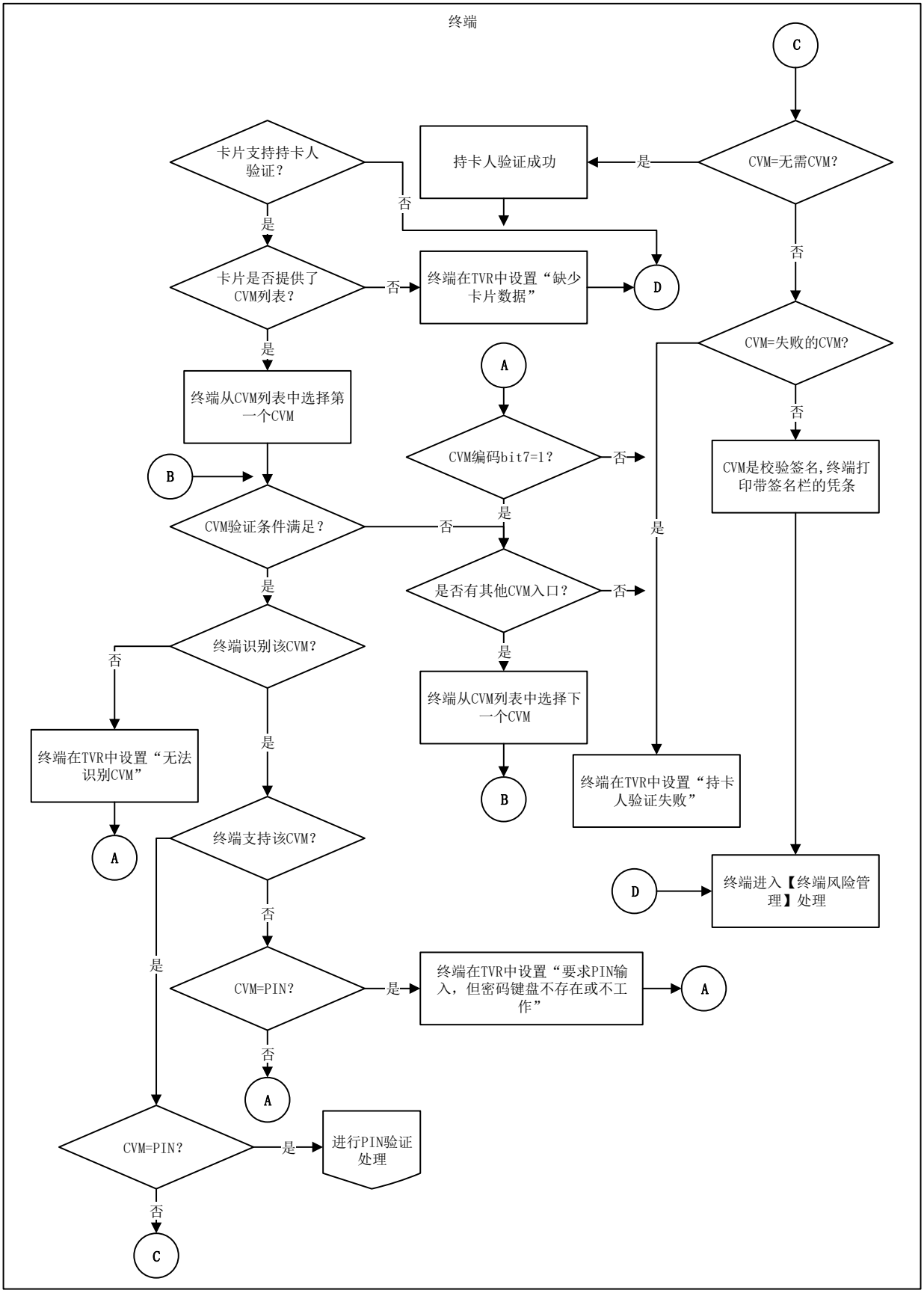

图8 CVM列表处理流程图

终端执行下列步骤：

a) 决定是否执行持卡人验证。若卡片支持持卡人验证（如 AIP 所说明），且读取应用数据时，卡片提供一个 CVM 列表，那么终端继续持卡人验证。反之，终端进行终端风险管理；

b) 处理 CVM 条目。由 CVM 列表中的第一个条目开始，终端执行以下行为：

1) 检查持卡人验证条件是否符合。若不符合，终端进行下一个 CVM 条目；

2) 若持卡人验证条件符合，终端将进一步检查此 CVM 代码是否可以识别。若可以识别，终端判断是否支持此 CVM，若支持，则进入步骤 4）；若终端不支持此 CVM 代码，则进行判断，此 CVM 是否和 PIN 验证相关，若为 PIN 验证则终端设置 TVR“要求输入 PIN，但密码键盘不存在或不工作”位为“1”，进入步骤 3）。若此 CVM 代码无法被终端识别，终端将在 TVR 中设置“未识别 CVM”位为“1”，进入步骤 3）；

3) 终端检查 CVM 代码 bit7 位。若为“1”，则继续处理下一个 CVM 条目；若 CVM 列表中无未处理的 CVM 条目，则持卡人验证失败，终端结束持卡人验证。若为“0”，则持卡人验证失败，终端设置持卡人验证不成功标志为“1”，结束持卡人验证；

4) 执行指定的持卡人验证方法。若持卡人验证不成功（例如脱机 PIN 验证失败），终端进入步骤 3）。若持卡人验证成功，终端进行终端风险管理。

c) 若终端到达了持卡人验证方法列表的末端还没有一个成功的持卡人验证，则持卡人验证处理失败—终端在终端验证结果里设置持卡人验证不成功标志“1”并进行终端风险管理。

6.2.6.5.3 持卡人验证处理

6.2.6.5.3.1 脱机明文 PIN 验证

脱机明文PIN验证处理中，卡片将持卡人输入的交易PIN与卡里储存的参考PIN对比以做检查。不同于联机PIN，脱机PIN不包括在联机授权报文中。若交易联机进行，脱机PIN验证结果包括在联机授权报文中。终端可用GET DATA命令向卡片请求PIN重试次数计数器，若卡片不支持传送PIN重试次数计数器，终端要求继续输入PIN。若返回的PIN重试次数计数器为零（没有剩余PIN重试次数），则脱机PIN验证失败。若返回的PIN输入次数计数器为一，则终端显示“最后一次尝试”。

若允许PIN重试，终端要求持卡人在密码键盘上输入PIN。若密码键盘和读卡器没有集成为一个不受外界干预的整体设备，PIN被密码键盘保密密钥加密并由读卡器解密。终端用VERIFY命令将持卡人输入的交易PIN从读卡器以明文方式传递给卡。

卡片将交易PIN与卡片里储存的参考PIN加以对比：

——若他们匹配，卡片将返回一个指示器，显示脱机 PIN 已被验证，持卡人验证完成；

——若不相配，卡片 PIN 重输次数计数器递减并返回一个显示剩余 PIN 重输次数的指示器。

若没有剩余PIN重输次数，脱机PIN验证失败。

若还有PIN重输次数剩余，终端要求持卡人重新输入PIN，重复校验过程。

PIN验证处理流程见图9和图10。

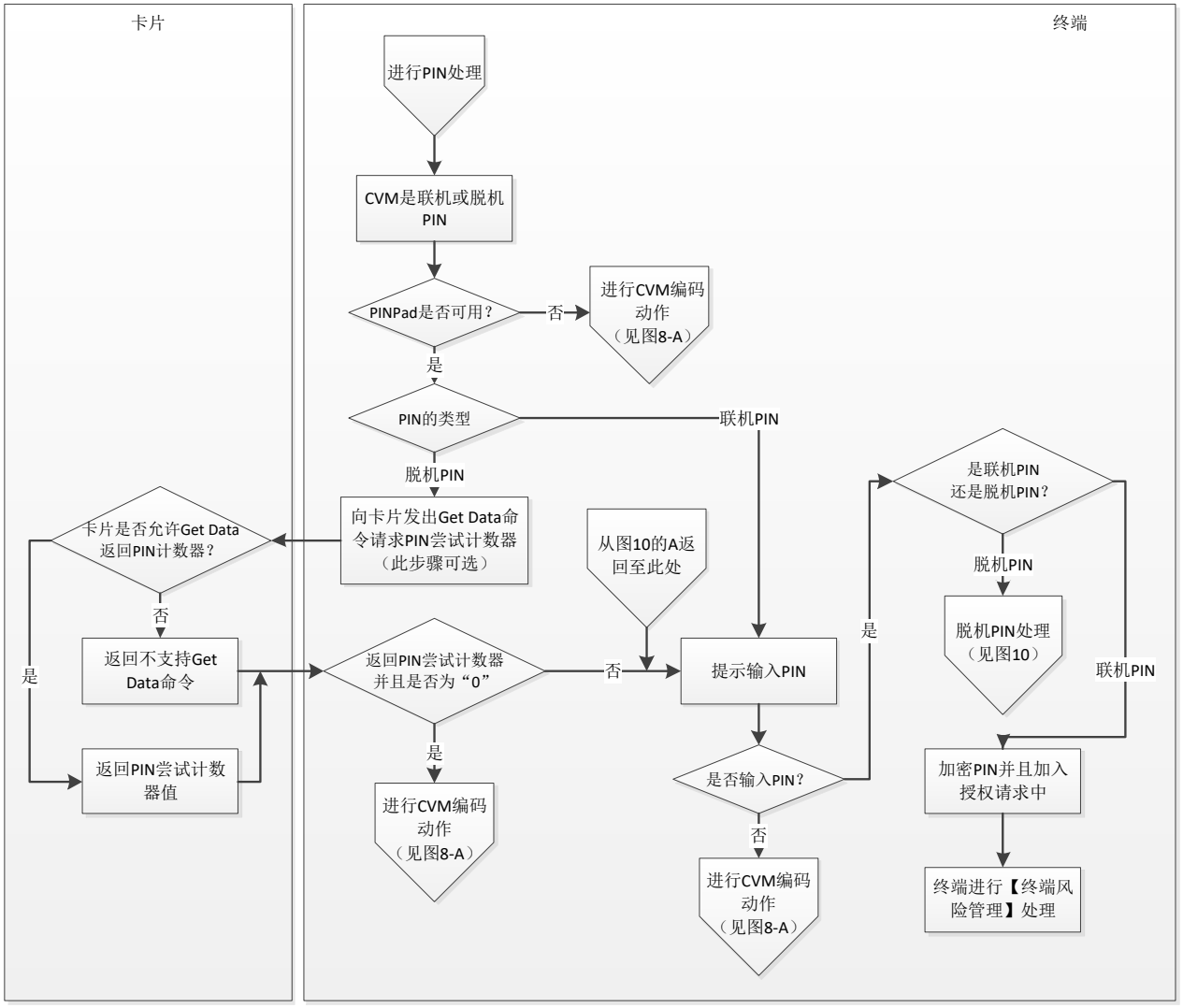

图9 PIN验证处理流程图（1）

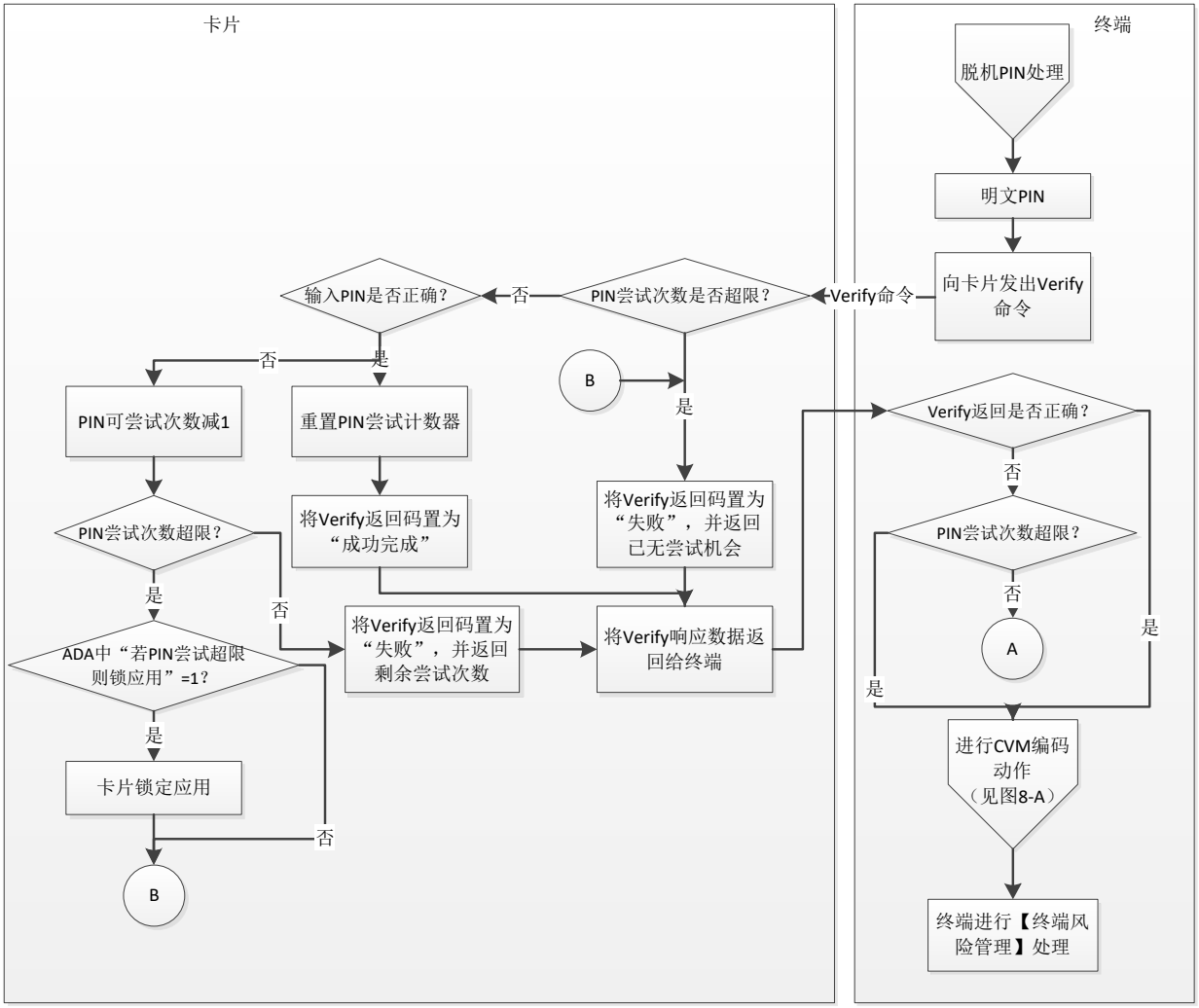

图10 PIN验证处理流程图（2）

6.2.6.5.3.2 联机 PIN 验证

在联机PIN验证处理过程中，输入后的PIN被加密，并包含在联机授权报文里，由发卡行的联机系统加以验证。

联机PIN处理流程不在JR/T 0025—2018中描述。

6.2.6.5.3.3 签名

当选择签名作为持卡人验证方法时，终端打印一张附有给持卡人签名档的收据。

6.2.6.5.3.4 不执行 CVM

当持卡人验证方法是“不执行CVM”时，不执行任何持卡人验证方法。

6.2.6.5.3.5 持卡人验证失败

当持卡人验证方法是“持卡人验证失败”时，认为持卡人验证处理失败。

6.2.6.5.3.6 持卡人证件验证

终端提示持卡人出示身份证件，并将卡片中得到的证件类型和证件号码显示给服务员，进行持卡人身份比对验证。

6.2.6.6 前期相关处理

前期相关处理包括：

——初始化应用处理：从卡片中获取 AIP，指示卡片是否支持持卡人验证；

——读取应用数据：终端从卡片中读取 CVM 列表以及其他持卡人验证处理中使用的数据。

6.2.6.7 后续相关处理

后续相关处理包括：

——终端行为分析：终端使用持卡人验证结果，以及称为发卡行行为代码和终端行为代码的卡片和终端参数来决定交易是被脱机拒绝、是联机发送授权请求、还是脱机批准；

——卡片行为分析：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，还是进行联机授权请求；

——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，发卡行的授权决定中应该考虑这些结果。联机授权报文里不包括脱机 PIN；

——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；

——发卡行到卡脚本命令处理：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 重试次数上限相等，并改变参考 PIN。APPLICATION UNBLOCK 命令可用来解锁在持卡人验证处理中锁定的应用。

6.2.7 终端风险管理

6.2.7.1 概述

终端风险管理使大额交易联机授权，并确保芯片交易能够周期性地进行联机以防止在脱机环境中也许无法觉察的风险。

虽然发卡行被强制要求在AIP中将终端风险管理位设置为“1”以触发终端风险管理，但终端应执行终端风险管理而不必考虑卡片的设置情况。

终端风险管理处理流程见图11和图12。

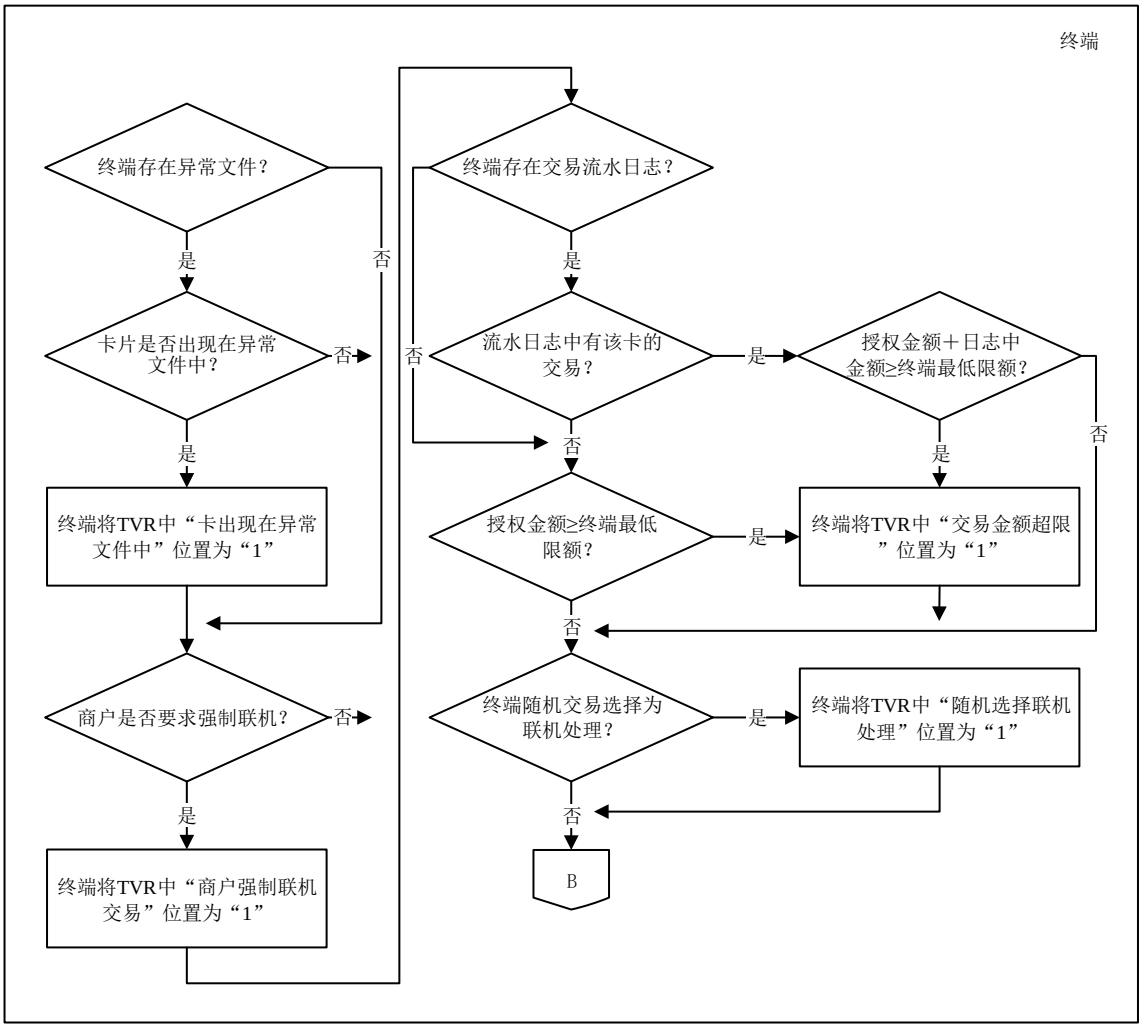

图 11　终端风险管理处理流程图（1）

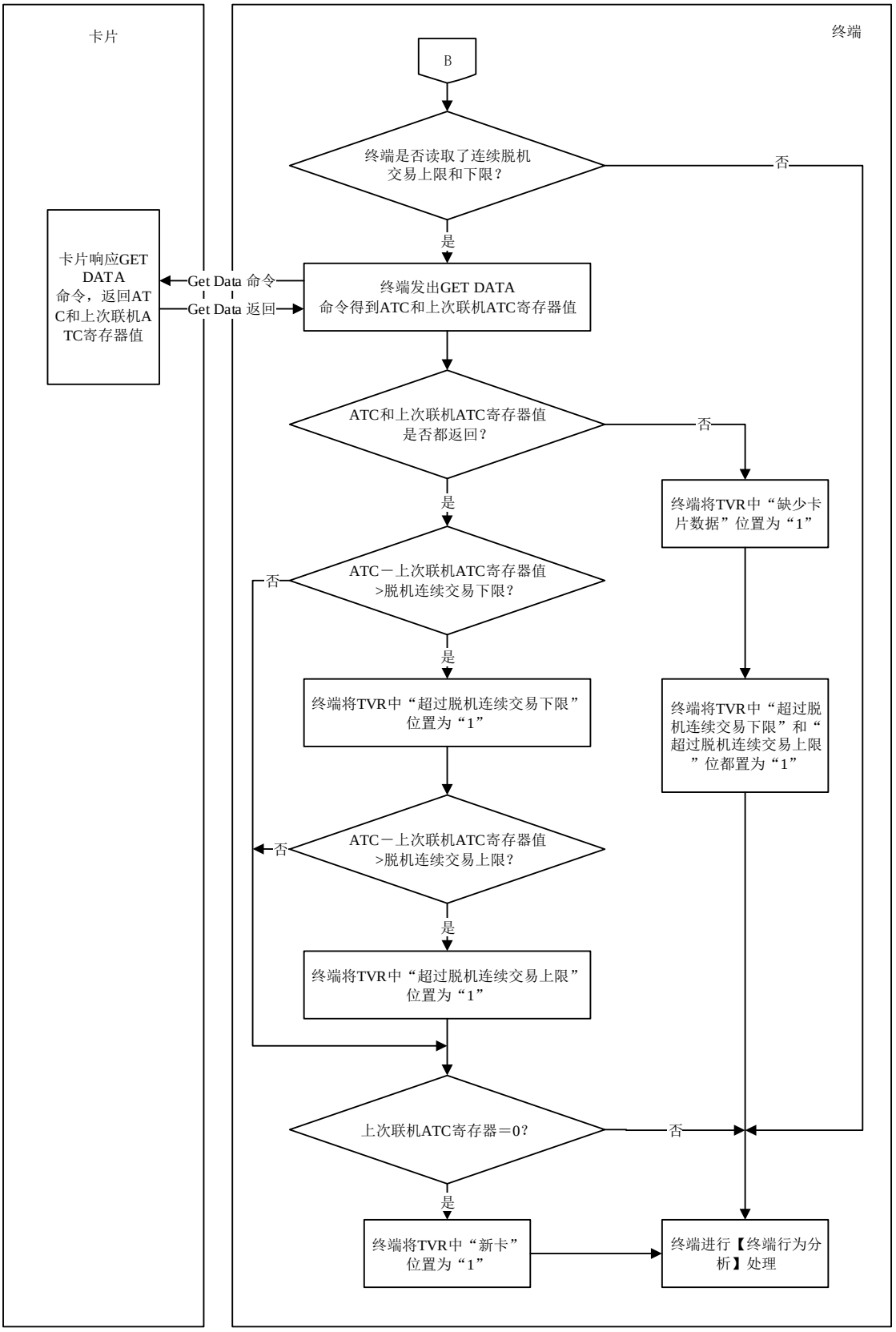

图 12　终端风险管理处理流程图（2）

6.2.7.2　卡片数据

表20列出并描述了终端风险管理中使用的卡片数据元。这些数据元及其用法的详细说明见JR/T 0025.5－2018附录A。

表20 终端风险管理—卡数据元

数据元	说明
PAN	终端异常文件检查时使用的有效的持卡人账号。
ATC	自卡片个人化以后处理的交易数量，在终端频度检查中使用。
上次联机 ATC 寄存器	上次联机 ATC 的值。若卡片要求终端进行终端频度检查或新卡检查，则这个数据元以及下面所列出的数据元都应提供。
连续脱机交易下限	若终端可以联机，该数据元（标签“9F14”）是发卡行定义的在交易应联机之前所允许的最大连续脱机交易笔数，他用于终端频度检查。
连续脱机交易上限	该数据元（标签“9F23”）是发卡行定义的在脱机交易应被拒绝之前所允许的最大连续脱机交易笔数。他用于终端频度检查。

6.2.7.3 终端数据

表21列出并描述了终端风险管理中使用的终端数据元。这些数据元及其用法的详细说明见JR/T 0025.6－2018附录A。

表21 终端风险管理—终端数据元

数据元	说明
授权金额	该数值型数据元（标签“9F02”）存储了当前交易金额（不包括调账交易）。用于最低限额检查。
用于偏置随机选择的最大目标百分数	用于随机选择交易联机处理。
用来随机选择的目标百分数	用于随机选择交易联机处理。
终端最低限额	该数据元（标签“9F1B”）表示与应用标识符相关联的终端最低限额。用于最低限额检查和随机选择交易联机处理。
TVR	记录终端脱机处理结果的一系列指示器。他们用来记录终端风险管理检查的结果。
偏置随机选择与阈值	用于随机选择交易联机处理的数值。
交易日志	为防止分开销售，终端可能记录了已批准交易的日志。此日志至少包含了应用主账号和交易金额，并可选择地包含了应用主账号序列号和交易日期。要存储和维护的交易日志数量不在 JR/T 0025 规定范围内。若有此日志，则他可被用于终端最低限额检查。
TSI	标明终端执行的功能，联机授权和清算报文中不提供此数据元，终端用他来表示已经执行了终端风险管理。

6.2.7.4 命令

若先前终端没有读取，则终端用GET DATA命令从卡片中读取上次联机交易ATC寄存器和ATC。

6.2.7.5 终端异常文件检查

若出现终端异常文件，终端就检查卡片的PAN是否列在终端异常文件上。

若卡片的PAN列在终端异常文件中，终端在TVR中设置“卡号出现在终端异常文件中”的位为“1”。

6.2.7.6 商户强制交易联机

在可以联机的终端，商户可以将终端设置为交易应该联机处理。

若商户强制交易联机，终端将TVR中“商户强制交易联机”的位设置成“1”。

6.2.7.7 最低限额检查

执行最低限额检查，可以使超过终端最低限额的交易执行联机授权。

终端将授权金额和终端最低限额进行比较，若交易额大于等于最低限额，终端将TVR中“交易金额超过最低限额”的位设置成“1”。即使终端最低限额为0，终端也应执行最低限额检查，并将终端验证结果中“交易金额超过最低限额”的位设置成“1”。

若终端包含一个交易日志,终端就检查同一张卡片先前的交易金额加上现在的交易金额是否超过了最低限额。

6.2.7.8 随机交易选择

可以支持脱机和联机交易的终端会随机选择交易进行联机处理。

若随机选择了一个交易，终端会标注在终端验证结果中。此处理的例子见JR/T 0025.6－2018的7.8。

6.2.7.9 终端频度检查

频度检查允许发卡行在一个预先设定的连续脱机交易的数量之后要求进行联机处理。允许脱机的终端应支持终端频度检查。发卡行可以选择终端不支持频度检查。

若卡片在读取应用数据处理时提供连续脱机交易下限（标签“9F14”）和连续脱机交易上限（标签“9F23”），终端将执行终端频度检查。若这些数据中的任意一个都没有出现在卡里，终端将避开这个处理。

终端发送GET DATA命令向卡读取上次联机ATC寄存器与ATC。卡在命令响应中返回这些数据元。

终端将ATC与上次联机ATC寄存器对比：

——若 ATC 减去上次联机 ATC 寄存器大于连续脱机交易下限值，终端将终端验证结果中“超过连续脱机交易下限”的位设置成“1”；

——若 ATC 减去上次联机 ATC 寄存器大于连续脱机交易上限值，终端将终端验证结果中“超过连续脱机交易上限”的位设置成“1”。

注：卡片行为分析中，卡片也可以执行相似的频度检查。卡的频度检查不会影响终端验证结果。

6.2.7.10 新卡检查

在终端所做的新卡检查中，若存在连续脱机交易上限值和连续脱机交易下限值，终端就检查上次联机ATC寄存器（若卡片提供的话）。根据发卡行认证结果和卡片参数，交易被联机批准后，该寄存器被重新复位。

终端发送GET DATA命令向卡片读取上次联机ATC寄存器（若该数据元并未出现在终端里）。卡片用上次联机ATC寄存器作为对GET DATA命令的响应。

终端检查上次联机ATC寄存器，若为“0”，终端将TVR中的“新卡”位设置为“1”。

注：卡片行为分析中，卡片也可以执行相似的新卡检查。

6.2.7.11 前期相关处理

前期相关处理包括读取应用数据。

从卡片读取下列数据：

——主账号用于检查终端异常文件；

——若卡上存在连续脱机交易上限值和下限值，他们用于终端频度检查。

6.2.7.12 后续相关处理

后续相关处理包括终端行为分析。

终端根据卡片和终端的设置来决定采取怎样的行动，若以下情况之一出现：

——卡片 PAN 在终端异常文件上；

——商户强制交易联机；

——超过了最低限额；

——交易被随机选择进行联机处理；

——频度检查金额或笔数超限；

——新卡。

6.2.8 终端行为分析

6.2.8.1 概述

终端行为分析中，终端把发卡行设置在卡片里及收单行设置在终端里的规则应用于脱机处理结果，以决定交易是应该被脱机批准、应该被脱机拒绝，还是请求联机授权。

终端行为分析牵涉到两个步骤：

a）检查脱机处理结果—终端检查由终端记录在终端验证结果里的脱机处理结果，决定交易要请求联机授权、脱机批准，还是脱机拒绝。此过程考虑了卡片中发卡行定义的规则（即IAC）以及终端定义的规则（即TAC）；

b）请求密文处理—终端要求一个来自卡片的密文。终端行为分析中，脱机批准或申请联机处理的决定并不是最终的。作为卡片行为分析（见6.2.9）的结果。卡片可以不考虑终端的决定，但脱机拒绝的决定是不可以忽略的。

6.2.8.2 卡片数据

表22和表23所描述是先前从卡片收到并在终端行为分析中使用的卡片数据元。这些数据元及其用法的详细说明见JR/T 0025.5－2018附录A。

表22 检查脱机处理结果—卡片数据

数据元	说明
IAC	IAC 是三种数据元，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系列与 TVR 中的比特位相对应的比特位组成。 • 发卡行行为代码-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； • 发卡行行为代码-联机位设置为“1”代表需要联机授权条件； • 发卡行行为代码-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； 类似的终端行为代码（TAC）在终端里定义。

表23 要求密文处理—卡片数据

数据元	说明
卡片风险管理数据对象列表 1	CDOL1 包含了终端数据对象的标签和长度，卡片需要用他们来生成第一个应用密文，以

（CDOL1）	及进行其他处理。

6.2.8.3 终端数据

终端数据元及其用法的详细说明见JR/T 0025.6－2018附录A。

检查脱机处理结果的终端数据和要求密文处理的终端数据分别见表24和表25。

表24 检查脱机处理结果—终端数据

数据元	说明
TAC	TAC是三种数据元，即终端行为代码-拒绝，终端行为代码-联机，终端行为代码-缺省。和发卡行行为代码相似，每个终端行为代码由一系列与TVR中的比特位相对应的比特位组成。 • 终端行为代码-拒绝比特位设置为“1”反映了交易被脱机拒绝的终端验证结果条件； • 终端行为代码-联机比特位设置为“1”代表了联机授权条件； • 终端行为代码-缺省比特位设置为“1”是当联机处理不可行时脱机拒绝所需的条件。
TVR	终端验证结果是在交易处理期间被用来代表脱机处理结果而设置的一系列比特位。

表25 要求密文处理—终端数据

数据元	说明
终端数据元	在CDOL1中得以详细说明的终端数据元包括在GENERATE AC命令中。

6.2.8.4 命令

终端发送GENERATE AC命令向卡申请一个应用密文。若执行CDA，终端也会出现此命令。

该命令指明了下列应用密文中的一种：

——TC：用于批准；

——AAC：用于拒绝；

——ARQC：进行联机。

此命令也包括卡在CDOL1里要求的终端数据对象。

当卡片接到GENERATE AC命令，他进行卡片行为分析。终端行为分析期间不返回对此命令的响应。

6.2.8.5 处理流程

6.2.8.5.1 概述

终端行为分析处理包括脱机处理结果的检查和请求密文处理两个步骤。终端行为分析处理流程见图13。

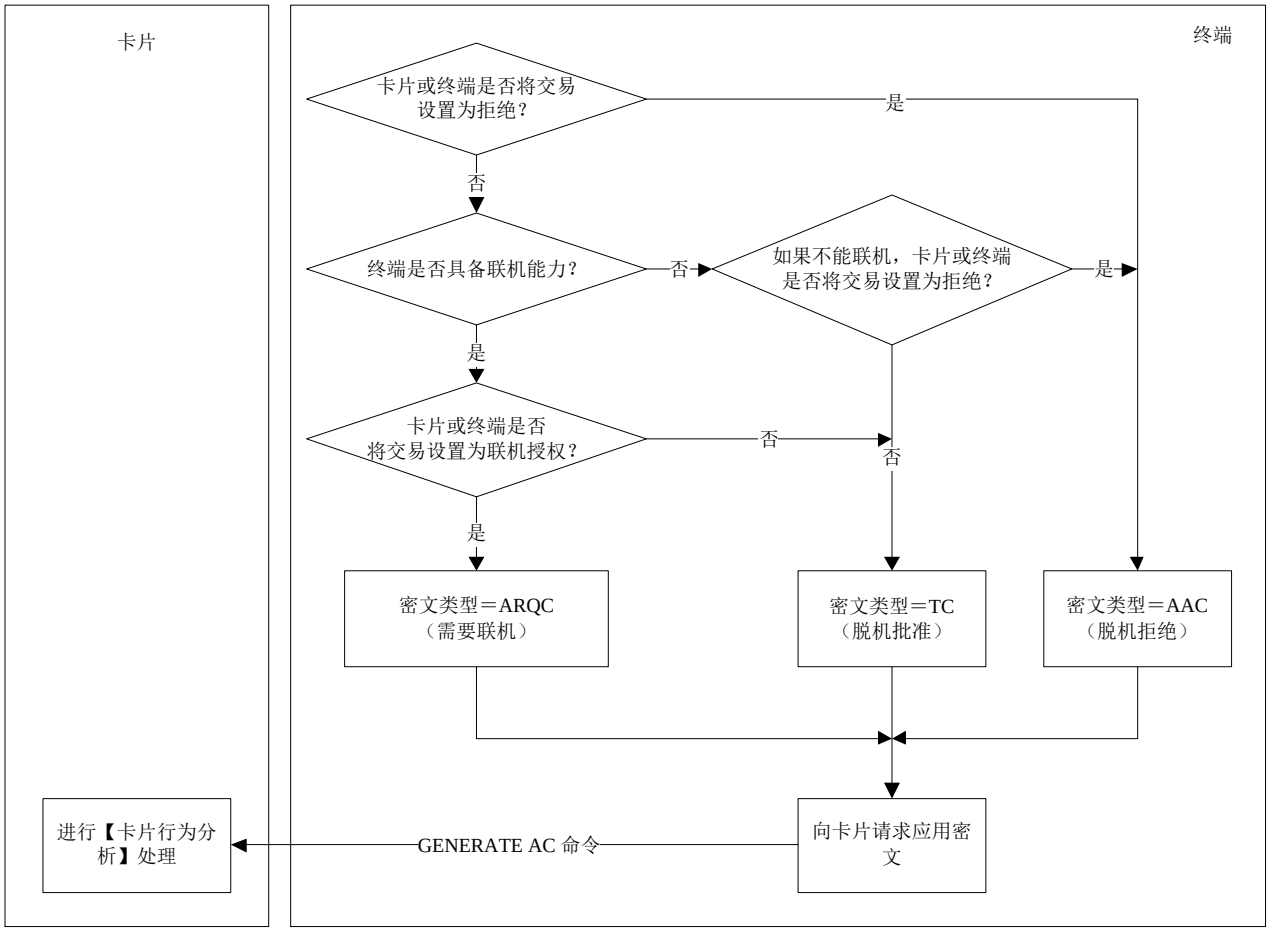

图 13 终端行为分析处理流程图

6.2.8.5.2 检查脱机处理结果

终端检查脱机处理的结果以决定是否交易需要联机、被脱机批准，或被脱机拒绝。这个过程中使用了卡片中发卡行定义的规则（发卡行行为代码）以及JR/T 0025.6—2018定义的规则（终端行为代码）。

注：JR/T 0025.6—2018的终端行为分析中有一个例子：IAC和TAC如何与TVR共同使用以决定交易处理过程。

6.2.8.5.3 请求密文处理

终端行为分析的第二阶段包括向卡片申请一个应用密文。检查脱机处理结果的步骤决定了将申请的密文类型：

——脱机批准：TC；

——进行联机授权：ARQC；

——脱机拒绝：AAC。

若执行CDA，终端也会出现此命令。

6.2.8.6 前期相关处理

前期相关处理包括：

——读取应用数据：终端从卡片读取应用数据，此数据包括 CDOL1 和 IAC；

——脱机数据认证、处理限制、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设置比特位。终端行为分析中，这些比特位设置与 IAC 和 TAC 共同使用来决定交易处理。

6.2.8.7 后续相关处理

后续相关处理为卡片行为分析。卡片执行附加的风险管理来决定是否否定终端行为分析中脱机批准或请求联机的决定。

6.2.9 卡片行为分析

6.2.9.1 概述

卡片行为分析允许发卡行执行频度检查以及其他的卡片内部的风险管理。本条描述的JR/T 0025－2018所专有的卡片风险管理特性包括如下检查：

——上次交易的行为；

——新卡；

——交易频度计数器。

6.2.9.2 卡片数据

表26列出并描述了卡片行为分析中用到的卡片数据元。关于这些数据元及其用途的详细描述见JR/T 0025.5－2018附录A。

表26 卡片行为分析－卡片数据元

数据元	说明
应用密文	卡响应 GENERATE AC 命令而返回的密文，包括请求拒绝的 AAC、请求批准的 TC 以及联机处理申请的 ARQC。
CDOL1	CDOL1 中要求的数据见 JR/T 0025.5—2018 附录 E。

6.2.9.3 终端数据

卡片行为分析中没有使用终端数据。

6.2.9.4 命令

终端用在终端行为分析完成后向卡片发出第一次GENERATE AC命令来要求卡片返回一个标明卡片授权响应结果的密文。在此命令中终端也可以标识是否要执行CDA。

6.2.9.5 处理流程

6.2.9.5.1 概述

卡片行为分析处理流程见图14。

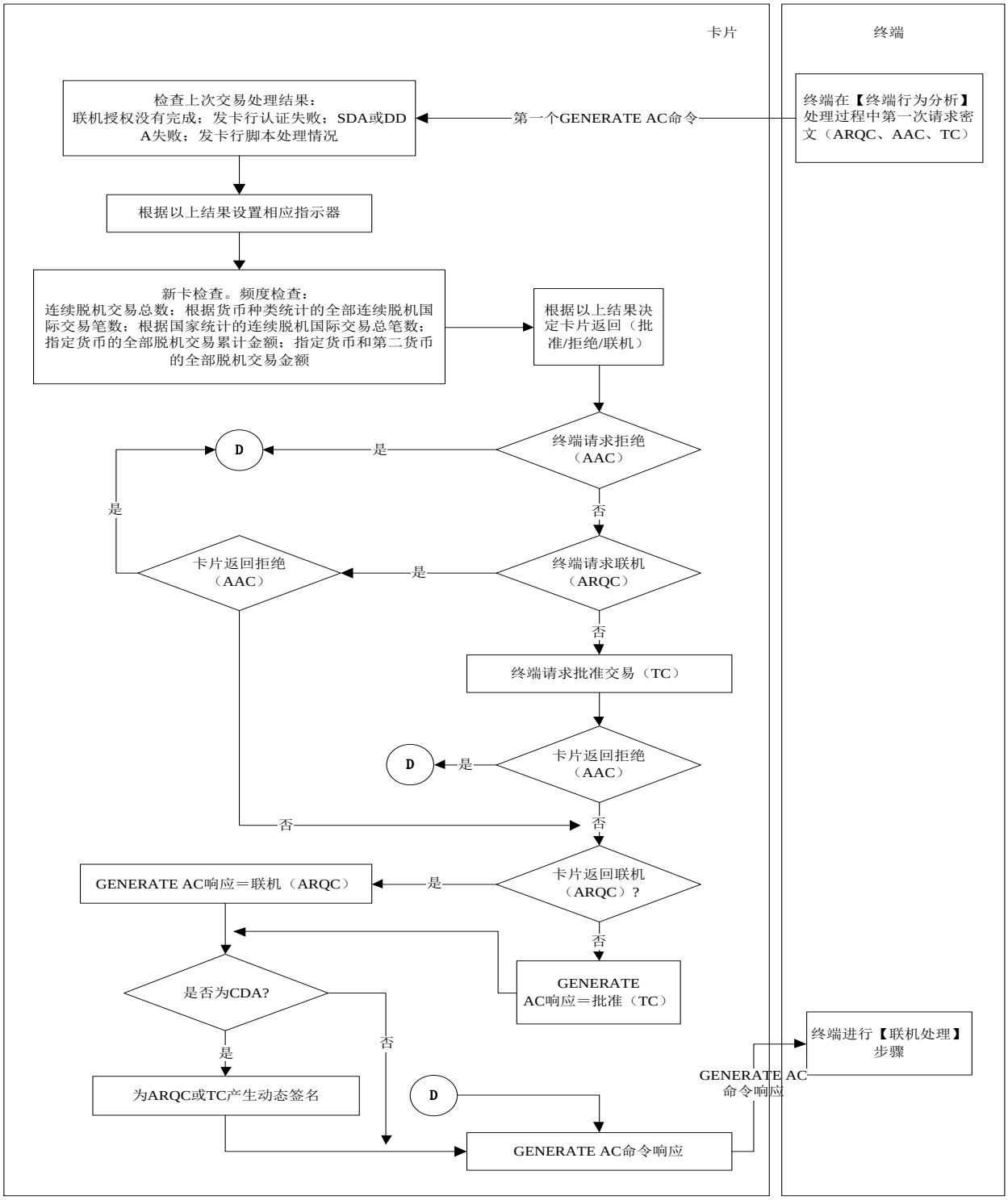

图 14 卡片行为分析处理流程图

终端行为分析之后，终端向卡发送GENERATE AC命令，向卡片提供在CDOL1中要求的数据并请求一个应用密文。6.2.8规定了终端行为分析的处理过程。

卡片从终端收到的GENERATE AC命令中包含了终端请求的密文类型。此密文类型表明了终端进行终端行为分析后对交易所作的决定（脱机批准、拒绝脱机和申请联机授权）。

6.2.9.5.2 卡片风险管理

若卡片支持并且要求的数据可用，则卡片执行下列卡片风险管理行为：

——上次交易行为。检查是否存在以下情况：

- 联机授权未完成；
- 上次联机交易时，发卡行认证失败；
- 上次交易静态数据认证失败；
- 上次交易动态数据认证失败；
- 上次交易发卡行脚本命令执行情况；
- 上次交易 PIN 重试次数超限。

——新卡检查；

——频度检查。查看以下项目的脱机处理次数是否超限：

- 全部连续脱机交易笔数；
- 根据货币种类统计的全部连续脱机国际交易笔数；
- 根据国家统计的全部连续脱机国际交易笔数；
- 指定货币的全部脱机交易累计金额；
- 指定货币和第二货币的全部脱机交易金额。

6.2.9.5.3 卡片响应决定

6.2.9.5.3.1 概述

根据卡片风险管理的结果，卡片决定交易响应。卡片返回的密文可与终端请求密文类型不同：

——卡片可不考虑终端已批准脱机的决定而申请联机授权或拒绝脱机；

——卡片可不考虑终端申请联机授权的决定而拒绝交易。

表27给出了卡片对GENERATE AC命令的响应信息。

表27 卡片行为分析－卡片对 GENERATE AC 命令的响应

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

6.2.9.5.3.2 标准 GENERATE AC 的响应

卡片利用终端和卡片提供的数据生成一个基于对称算法的密文。JR/T 0025.5—2018附录D中详述了所要求的数据。密文生成过程中所需的对称密钥和算法应符合JR/T 0025.7—2018的规定。

卡片在GENERATE AC响应中将此密文返回给终端。这个响应中的密文类型表明了卡片对于此交易的处理决定（脱机批准、脱机拒绝、申请联机授权）。

6.2.9.5.3.3 CDA 的 GENERATE AC 响应

若终端在GENERATE AC命令中标明将执行CDA且卡片在GENERATE AC响应中返回的密文类型是TC或ARQC，则卡片用IC卡私钥将应用密文、密文信息数据以及其他的数据签名。在GENERATE AC响应中，卡片将这签名数据返回给终端。

6.2.9.6 前期相关处理

前期相关处理为读取应用数据。终端从卡片读取CDOL1。

6.2.9.7 后续相关处理

后续相关处理为交易结束（见6.2.12）。若要求联机处理但终端无法将交易联机发送，则卡片和终端执行其他的处理来决定是脱机批准或拒绝交易。

终端在执行另外的分析（类似于终端行为分析）中使用发卡行行为代码-缺省和终端行为代码-缺省来决定在最终GENERATE AC命令中要请求的密文类型（AAC或TC）。

卡片应执行下列的卡片风险管理检查，以决定最终的交易处理结果：

——对于全部连续脱机交易（上限）的频度检查；

——新卡；

——没有执行脱机 PIN 验证。

6.2.10 联机处理

6.2.10.1 概述

联机处理允许发卡行主机根据发卡行设置的主机风险管理参数判断交易是允许或拒绝。与传统的联机欺诈检查和信用检查相比，主机授权系统还需额外通过利用卡片产生的动态密文执行联机卡片授权，同时还需在决定授权时考虑脱机处理的结果。

发卡行返回的数据可以包括发卡行生成的密文和给卡片的更新数据，其中发卡行产生的密文用于卡片认证返回数据真实性。

6.2.10.2 卡片数据

终端所用到的卡片数据见表28。

表28 联机处理－终端使用的卡片数据

数据元	描述
GENERATE AC 命令返回数据	返回数据中包括： • 密文信息数据（若交易需要联机授权，则是 ARQC）； • AC； • ATC； • 发卡行应用数据。
AIP	终端在应用初始化处理时从卡片得到 AIP，其中一位指明卡片是否支持发卡行认证。

在发卡行授权过程中卡片内部使用的数据见表29。

表29 联机处理－卡片内部使用数据

数据元	描述
ARQC	由卡片在此交易的较早步骤产生。ARQC 和授权响应码将在 ARPC 确认处理中作为输入数据。
UDK	是 ARPC 确认处理中使用的对称密钥，与产生 ARQC 使用的是同一密钥。
CVR	若发卡行认证失败，相应位将置 1。
发卡行认证失败指示器	若发卡行认证失败，该位将置 1。

6.2.10.3 终端数据

根据发卡行认证状态，终端应改变的数据元见表30。

表30 联机处理－终端应改变数据元

数据元	描述
TVR	当发卡行认证失败时，其中相应位将置“1”。
TSI	当发卡行认证执行过后，其中相应位置“1”。

6.2.10.4 联机响应数据

表31是发卡行可能返回给收单行的响应数据，若存在，收单行应将数据传送给终端。

表31 联机处理－发卡行可能返回的响应数据

数据元	描述
发卡行认证数据	包括以下子项： • 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一些命令数据，用于更新卡片数据。

6.2.10.5 命令

联机处理过程使用EXTERNAL AUTHENTICATE命令。

若执行了发卡行认证，终端应使用从发卡行请求到的发卡行认证数据通过EXTERNAL AUTHENTICATE命令验证ARPC的正确性。通过命令的返回可知道认证是否通过。

6.2.10.6 处理流程

6.2.10.6.1 概述

标准的联机处理包括联机请求、联机响应，若需要，可执行发卡行认证。若已经执行CDA，处理过程中还应包括动态数据的验证。联机处理流程见图15。

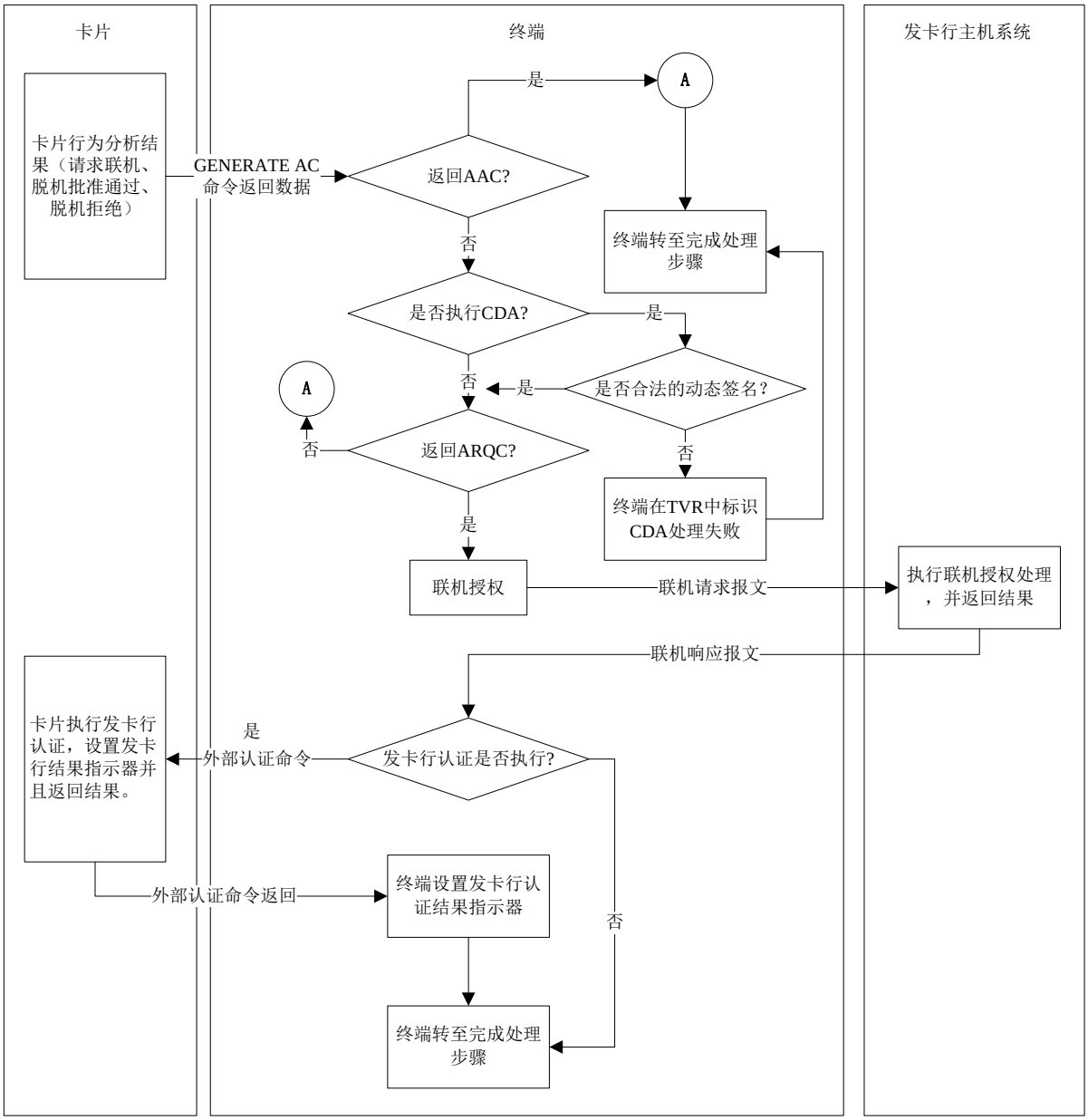

图 15　联机处理流程图

6.2.10.6.2　联机请求

联机请求处理根据是否已经执行CDA而有所不同。

——执行 CDA。若在 GENERATE AC 命令中标识执行的是 CDA 同时返回的密文是 ARQC 或 TC，终端将做以下处理：

- 终端用 IC 卡公钥验证动态密文；
- 若验证不正确，则 CDA 失败，并转至完成处理；
- 若验证正确，则进行标准联机处理。

——标准联机请求处理。若卡片在 GENERATE AC 向终端返回 ARQC，同时终端具备联机能力，则终端发出联机授权报文。若卡片没有返回 ARQC 或终端不具备联机能力，则转至完成处理步骤。

6.2.10.6.3　联机响应

联机请求报文成功发送给发卡行后，终端接受发卡行返回的响应报文，其中可以包括用于更改卡片信息的发卡行命令脚本或密文，也可以两者皆有，用于确认响应报文确实是从合法的发卡行返回的。若联机响应中包括发卡行认证数据，同时卡片支持发卡行认证，则执行发卡行认证。否则，转至完成处理步骤。

6.2.10.6.4 发卡行认证

终端向卡片发出EXTERNAL AUTHENTICATE命令用于执行发卡行认证，卡片用先前生成的ARQC、发卡行授权响应码以及存储在卡片特定安全区域的子密钥验证ARPC的合法性。

卡片和终端都应记录发卡行认证结果：

——卡片在 CVR 中设置发卡行认证结果以及发卡行认证失败标识，并且在 EXTERNAL AUTHENTICATE 命令响应报文中将结果返回给终端；

——终端在进行完成处理之前，在 TVR 中设置发卡行认证结果和 TSI。

6.2.10.7 前期相关处理

前期相关处理为卡片行为分析。若经过卡片分析后需要联机授权，则卡片返回的密文类型为ARQC。

6.2.10.8 后续相关处理

后续相关处理包括：

——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交易如何处理以及是否重置相关指示器和计数器；

——发卡行脚本处理：若联机处理范围报文中包括发卡行命令脚本，终端需要将这些命令脚本发给卡片执行。

6.2.11 发卡行脚本处理

6.2.11.1 概述

发卡行脚本处理使得发卡行不用二次发卡就可以改变卡片个人化数据。发卡行在认证响应时在返回报文中包括了有卡片指令的脚本，终端在安全条件满足的情况下将这些指令发送给卡片。

支持的脚本命令如下：

——更改卡片参数；

——应用锁定/解锁；

——卡片锁定；

——重置 PIN 计数器；

——修改脱机 PIN。

发卡行脚本处理可通过锁定被盗或恶意透支卡来防止信用和欺诈风险，另外也可根据持卡人的具体情况改变卡片参数。

6.2.11.2 脚本相关密钥

6.2.11.2.1 MAC 密钥

MAC密钥用来产生和验证命令脚本MAC。MAC是包含在命令脚本中的密文，用于确认数据没有被篡改，同时确认命令发出的发卡行是否合法（发卡行认证）。MAC处理过程中涉及三个密钥：

——MAC 主密钥（MAC MDK）由发卡行确定的唯一的双倍长对称密钥，用来产生卡片唯一的 MAC 认证密钥（MAC UDK）和交易 MAC 的过程密钥；

——卡片 MAC 子密钥（MAC UDK）在卡片个人化时由 MAC 主密钥分散后写入卡片的双倍长对称密钥。MAC UDK 用来在交易过程中产生 MAC 过程密钥；

——MAC 过程密钥交易中唯一的双倍长对称密钥，用来在交易时产生脚本命令的 MAC 码。

6.2.11.2.2 数据加密密钥

数据加密密钥用来加密脚本中的敏感数据，如脱机PIN等。数据加密涉及三个密钥：

——数据加密主密钥（ENC MDK）：发卡行唯一的双倍长对称密钥，用于产生卡片唯一数据加密密钥以及交易的数据加密过程密钥；

——卡片数据加密子密钥（ENC UDK）：卡片个人化时由 ENC MDK 分散得到后写入卡片的双倍长对称密钥，用来产生数据加密过程密钥；

——数据加密过程密钥：交易中唯一的双倍长对称密钥，由 ENC MDK 分散而得到，用于发卡行主机系统加密脚本中的敏感数据。

6.2.11.3 卡片数据

脚本处理过程中卡片涉及的计数器和指示器见表32。

表32 发卡行脚本处理－卡片使用的计数器和指示器

数据元	描述
ATC	自卡片个人化以后处理的交易计数器，在终端频度检查中用到。
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。
发卡行脚本命令计数器	记录第二次生成应用密文后卡片收到的有安全报文的指令的个数，在下次交易中的结束处理步骤中可能被复位。
发卡行脚本失败指示器	若脚本指令执行失败，指示位置“1”，失败的情况包括： • 安全报文错误； • 安全报文通过但是指令执行失败； • 需要安全报文但是不存在。 在下次交易中的结束处理步骤中可能被复位。

6.2.11.4 终端数据

发卡行脚本处理过程中终端用到的数据元见表33。

表33 发卡行脚本处理－终端使用的数据元

数据元	描述
发卡行脚本结果	记录卡片对发卡行脚本指令处理的结果，此结果要包括在清算报文和下次联机授权中。
TVR	TVR 中包括和脚本有关的两个指示位： • 最后一个生成应用密文之前，发卡行脚本失败； • 最后一个生成应用密文之后，发卡行脚本失败。 JR/T 0025—2018 只支持在最后一个生成应用密文命令之后，处理发卡行脚本。
TSI	TSI 中包括一个表明执行发卡行脚本处理标记。

6.2.11.5 联机响应数据

发卡行脚本处理过程中联机响应数据元见表34。

表34 发卡行脚本处理－联机响应数据元

数据元	描述
发卡行脚本命令	脚本中的每一个发卡行脚本指令都按照 BER-TLV 格式，用标签“86”开始。
发卡行脚本标识	发卡行用来唯一标识发卡行脚本。
发卡行脚本模板 2	JR/T 0025－2018 仅支持发卡行脚本模板 2。标签“72”标识模板 2，模板中包括在第二次生成应用密文指令后，传送给卡片的发卡行专有脚本数据。

6.2.11.6 命令

6.2.11.6.1 应用锁定（APPLICATION BLOCK）

该命令将锁定当前选择的应用。若应用在交易过程中被锁定，卡片和终端将继续处理交易直到交易完成。在应用锁定之后，卡片将拒绝被锁的应用完成任何金融交易。终端可以选择被锁的应用，用于对该应用解锁。

6.2.11.6.2 应用解锁（APPLICATION UNBLOCK）

该命令将已被锁定的应用解锁。对于发卡行，应用解锁最好在专用设备上进行。

6.2.11.6.3 卡片锁定（CARD BLOCK）

卡片锁定将使卡片上所有的应用永久锁定。

6.2.11.6.4 PIN 修改/解锁（PIN CHANGE/UNBOLCK）

该命令可以让发卡行在PIN解锁（重置PIN重试计数器）的同时更改卡片PIN。PIN修改/解锁应在满足发卡行安全要求的环境下进行。

6.2.11.6.5 设置数据（PUT DATA）

该命令用于更新卡片中由发卡行设置的管理参数，如连续脱机交易次数上限、连续脱机交易次数下限、连续脱机国际交易限制、累计脱机交易总额上限等。

6.2.11.6.6 修改记录（UPDATE RECORD）

该命令用来修改文件中一条记录的内容。

6.2.11.7 处理流程

6.2.11.7.1 概述

发卡行脚本处理包括发卡行脚本、命令执行、安全报文三方面。发卡行脚本处理流程见图16。

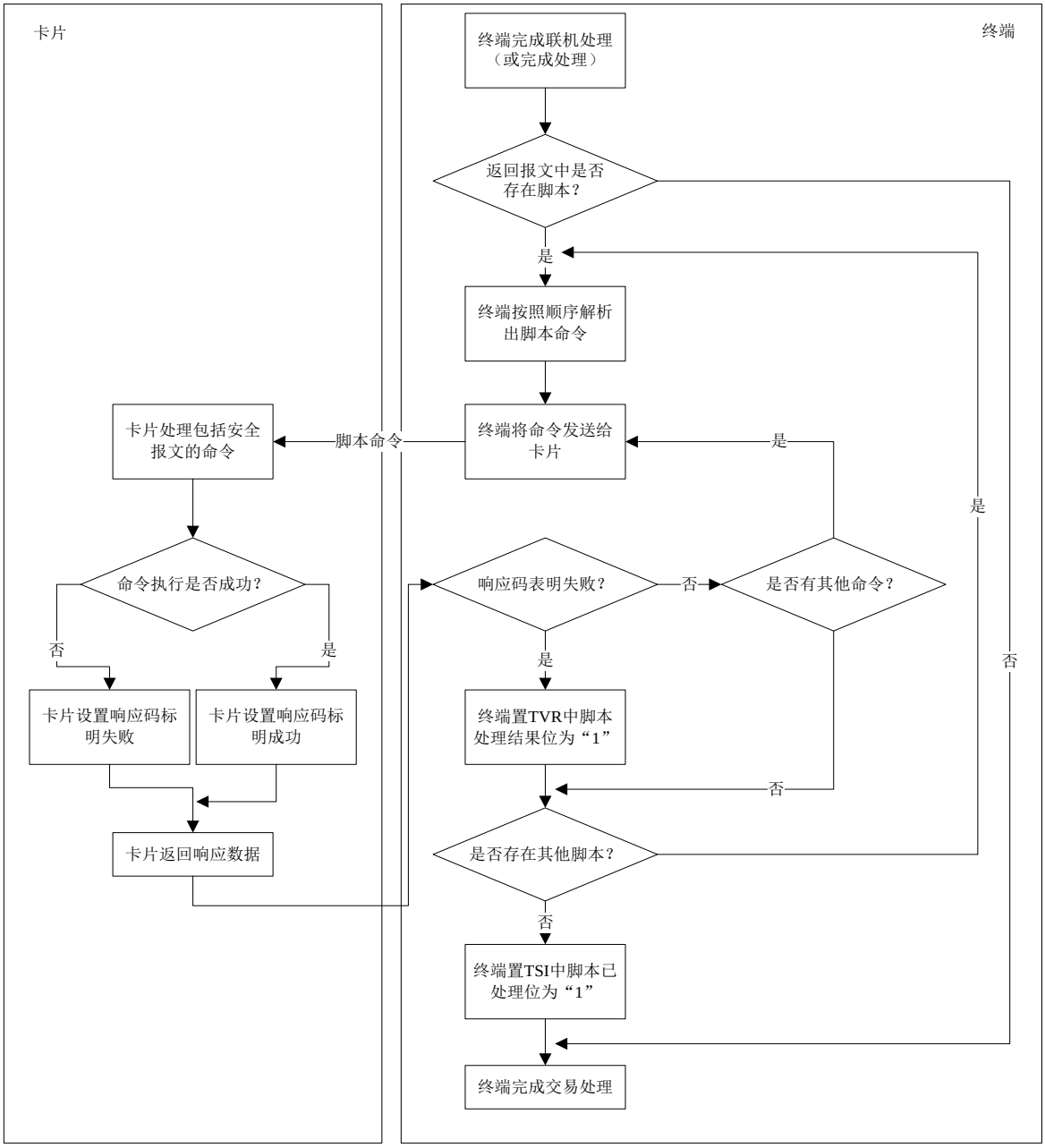

图 16　发卡行脚本处理流程图

6.2.11.7.2　发卡行脚本

发卡行通过返回报文将发卡行脚本发送给收单方。

发卡行返回报文中若包括标识“72”，表明在最终的GENERATE AC后需执行发卡行脚本。

6.2.11.7.3　命令执行

被推荐的发卡行脚本命令用来处理先前说明的那些功能。只有命令支持安全报文且安全报文能成功执行的前提下，卡片才执行被请求的命令来更新包含在卡里的数据。

在处理发卡行脚本命令之前，发卡行应先成功执行一些发卡行认证方式。由于安全报文是一种发卡行认证方式，通过为命令成功地执行安全报文也可满足此要求。卡片发卡行承担着发卡行脚本命令组织。若一个不同于发卡行的实体发起命令，也会发起同样的请求。

6.2.11.7.4 安全报文

安全报文目的是确保数据机密性、消息完整性以及发卡行认证。数据机密性确保保密数据在从发卡行到卡的传送中保持其秘密。消息完整性确保命令和命令数据在传送时没有被改变。发卡行认证确保命令来自有效发卡行。使用MAC来达到消息完整性以及发卡行认证。使用对明文命令数据（若有出现）的加密来达到数据机密性。

6.2.11.8 前期相关操作

前期相关处理为联机处理（见6.2.10）。联机处理响应报文中可能包括需要在发卡行脚本处理过程中处理的发卡行脚本。

6.2.11.9 后续相关操作

后期相关处理包括：

——卡片行为分析（下一交易）。在下一交易的卡片行为分析时，卡片中的 CVR 子域将根据卡片中保存的上次交易发卡行脚本失败指示器和发卡行命令脚本计数器设置脚本运行结果。发卡行将在下次清算记录和联机授权时收到 CVR；

——交易结束（下一交易）。当下列任何一种情况发生时，卡片将重置发卡行脚本失败指示器和发卡行命令脚本计数器为“0”：

- 发卡行认证成功；
- 发卡行认证为可选项，并且没有执行；
- 不支持发卡行认证。

当联机授权没有完成或发卡行认证条件不满足时，发卡行脚本失败指示器和发卡行命令脚本计数器应不被重置。

6.2.12 交易结束

6.2.12.1 概述

终端和卡片执行完成来结束交易处理，主要包括以下动作：

——若要求联机处理，但终端并不支持联机处理或联机授权无法完成，则终端和卡片通过其他的分析决定交易是否可脱机完成或拒绝；

——若终端执行 CDA 失败，则终端按照以下方式处理：

- 若卡片请求 ARQC，则终端在第二次发送 GENERATE AC 命令时请求 AAC；
- 若卡片请求 TC 并且 CDA 执行失败，终端拒绝交易并返回响应码。

——发卡行的联机确认结果有可能会因为发卡行认证结果和卡片的一些选项而变成拒绝交易；

——交易处理过程中指示器和计数器会反映发生情况；

——联机授权后，指示器和计数器可能会根据发卡行认证结果和卡片选项重置。

终端可执行其他一些附加的功能以完成整个交易，例如打印凭条、记录交易数据等与JR/T 0025.6－2018不冲突的功能。

6.2.12.2 卡片数据

完成处理时卡片内部使用到的部分数据元见表35，其他数据元见JR/T 0025.5—2018。

表35 交易结束－卡片使用数据元

数据元	描述
ADA	发卡行定义的指示位，指定在一些特殊条件下的卡片行为。
CDOL2	列出在第二个生成应用密文指令中，卡片要求终端传送的数据对象（标签和长度）。下列在 CDOL2 中的数据用于卡片风险管理检查： • 交易货币代码； • 终端国家代码； • 授权金额； • 授权响应码； • TVR。

卡片对GENERATE AC命令的响应数据见表36。

表36 交易结束－GENERATE AC 命令卡片响应数据

数据元	描述
AC	由卡片产生的密文。
ATC	卡片记录交易次数的计数器。
密文信息数据	包括下列指示位： • 密文类型（拒绝 AAC、接受 TC 或联机上送 ARQC）； • 其他状态信息。
发卡行应用数据	发卡行定义的应用数据，包括 CVR。
CVR	标明当前和上次交易的脱机处理结果。

6.2.12.3 终端数据

在完成处理过程中终端使用到的数据元见表37。

表37 交易结束－终端使用数据元

数据元	描述
授权响应码	标明交易处理结果，提交给卡片。
TVR	用来记录脱机处理结果，例如 SDA 执行情况等。

6.2.12.4 命令

使用GENERATE AC命令。终端发出第二次GENERATE AC命令向卡片请求最终的应用密文，此处的GENERATE AC命令也可标识成需要执行CDA。

GENERATE AC命令包含卡片在CDOL2中详细描述的终端数据元，终端通过读取应用数据取得这些数据元。CDOL2数据包括发卡行联机返回的授权响应码或在联机授权无法完成的情况下由终端返回的授权响应码。

指令参数P1指明终端请求的加密类型见JR/T 0025.5—2018的表B.7。

GENERATE AC命令的响应信息包括卡片交易计数器、指明卡片授权决定的密文类型、应用密文和CVR指定的处理结果，发卡行自定义的数据也可被返回。

6.2.12.5 处理流程

交易结束处理流程见图17。

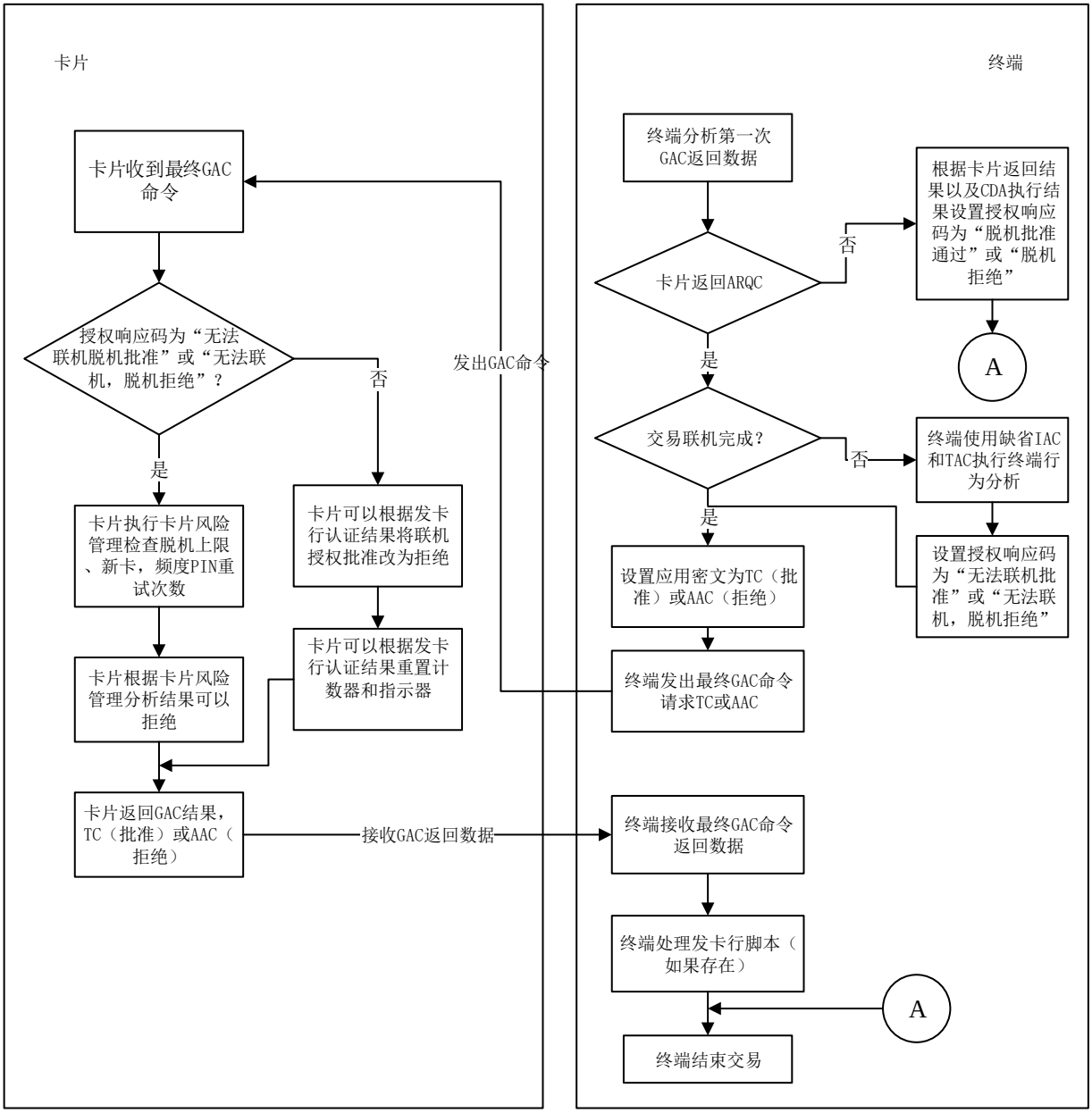

图 17 交易结束处理流程图

根据先前的交易处理中所发生的情况，完成处理期间终端可能处理不同的情况：

卡片行为分析结束后，卡片可能已经：

——请求脱机批准（TC）或拒绝交易（AAC）；

——请求联机授权（ARQC）。

在联机处理时，联机授权可能已经：

——成功完成；

——由于终端或通讯原因未完成。

当卡片行为分析执行第一个GENERATE AC命令返回TC或AAC时，则交易脱机接受或拒绝。

终端应根据第一个GENERATE AC命令响应返回的CID以及TVR中显示的CDA结果决定交易最终结果，见表38 。

表38 交易结束－终端处理结果（脱机）

第一次 GENERATE AC 返回结果	CDA 处理结果	最终交易结果
TC	CDA 不执行或成功	脱机批准通过
TC	CDA 失败	拒绝
ARQC	CDA 失败	在第二次 GENERATE AC 命令中请求 AAC
AAC	--	拒绝

当卡片行为分析执行，第一个GENERATE AC命令返回ARQC（要求联机）时：

a) 由于终端不支持或其他原因造成联机授权没有完成，终端向卡片发出第二个 GENERATE AC 命令请求产生 AAC 或 TC；

b) 当联机授权完成，根据联机授权结果，终端向卡片发出第二个 GENERATE AC 命令请求 TC（批准）或 AAC（拒绝）。终端根据表 39 所列情况处理交易。

表39 交易结束－终端处理结果（联机）

<table>
<tr><th colspan="2">联机授权结果</th><th>终端向卡片请求数据</th><th>卡片返回</th><th>最终交易结果</th></tr>
<tr><td colspan="2" rowspan="2">未完成</td><td>AAC</td><td>AAC</td><td>拒绝</td></tr>
<tr><td>TC</td><td>TC/AAC</td><td>批准/拒绝</td></tr>
<tr><td rowspan="2">完成</td><td>通过</td><td>TC</td><td>TC 或 AAC</td><td>除以下两种情况卡片返回 AAC（拒绝），其他情况卡片返回 TC（批准）：
● 发卡行认证失败，同时 ADA 中标识此种情况拒绝交易；
● 发卡行认证强制，但未执行，同时 ADA 中标识此种情况拒绝交易。</td></tr>
<tr><td>拒绝</td><td>AAC</td><td>AAC</td><td>拒绝</td></tr>
</table>

6.2.12.6 前期相关操作

前期相关操作为联机处理。若卡片收到终端发送的EXTERNAL AUTHENTICATE命令，则卡片开始进行发卡行认证处理，同时设置指示器为发卡行认证已执行并标识成功或失败。这些指示器将在完成处理期间被卡片用于卡片响应，并且决定哪些卡片计数器和指示器将被重置。

6.2.13 卡片交易明细记录

6.2.13.1 概述

卡片可以支持交易明细记录，对于支持交易明细的卡片，在SELECT命令的响应中应包含日志入口（Log Entry）数据元，同时应支持终端通过GET DATA命令从卡片获取日志格式（Log Format）数据元，对于需要访问交易明细记录的终端可通过发送READ RECORD命令到卡片，逐条读取交易记录。

支持记录明细的卡片应通过DOL向终端获取记录交易明细所需要的终端数据元。当交易结束时，若卡片批准交易通过并返回TC，卡片内部会记录此笔交易的交易明细供持卡人脱机查询。

交易明细是以循环记录结构保存在卡片的某一文件中。该文件的修改由卡片内部完成，终端只能对其进行读取操作。

6.2.13.2 交易明细数据元

交易明细中宜包含交易日期、交易时间、授权金额、其他金额、终端国家代码、交易货币代码、商户名称、交易类型、应用交易计数器等数据，具体格式见表40。

表40 卡片交易明细－数据格式

数据	格式	长度（字节）
交易日期	YYMMDD	3
交易时间	HHMMSS	3
授权金额	n12	6
其他金额	n12	6
终端国家代码	n3	2
交易货币代码	n3	2
商户名称	ans	20
交易类型	n2	1
ATC	b	2

7 安全、密钥和数字证书

借记/贷记应用过程中与安全相关的内容（包括但不限于脱机静态数据认证、脱机动态数据认证、AC生成和发卡行认证、安全报文）应符合JR/T 0025.7—2018的要求。