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 0025.5—2010
代替JR/T 0025.5—2005

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

China financial integrated circuit card specifications—
Part 5:Debit/credit application card specification

2010-04-30 发布　　2010-04-30 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13个部分：

——第1部分：电子钱包/电子存折应用卡片规范；

——第2部分：电子钱包/电子存折应用规范；

——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；

——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。

本部分为JR/T 0025的第5部分。

本部分代替JR/T 0025.5—2005《中国金融集成电路（IC）卡规范　第5部分：借记/贷记卡片规范》。

本部分与JR/T 0025.5—2005相比主要变化如下：

——标准名称进行修订，由《中国金融集成电路（IC）卡规范　第5部分：借记/贷记卡片规范》修订为《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》；

——重新起草标准的前言及引言；

——对“术语和定义”及“符号和缩略语”在正文中的出现的情况做了核对，对于没有出现的直接予以删除，对于出现的进行了修改和完善，并同步修改标准正文；

——对“规范性引用文件”在正文中的引用情况做了核对，对正文中引用到的文件根据标准编写要求进行重新编排和规范，将参考到的文件归集到参考文献，将没有引用也没有参考的文件予以剔除；

——根据技术的发展趋势及主流标准的应用情况，对本部分进行了补充完善；

——根据中国银行卡产业的实际发展需要，保证标准的适用性，针对原标准在使用过程中发现的问题进行修订。

本部分的附录A、附录B、附录C、附录D、附录E和附录F是规范性附录。

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、交通银行、招商银行、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、中国印钞造币总公司、银行卡检测中心、国家电子计算机质量监督检验中心。

本部分主要起草人：姜云兵、杜宁、徐晋耀、李春欢、刘志刚、张永峰、张艳、聂舒、韩小西、张栋、回春野、吴蕃、史大鹏、边红丽、黄贵玲、李曙光、刘启滨、赵雷、詹旭波、徐文伟、黄发国、贾树辉、马小琼、赵宏鑫、林铁行、袁红斌、周兆确、向前、苏国经、周继军、赵亚东。

本部分于2005年3月首次发布，2010年4月第一次修订。

引　言

本部分为JR/T 0025的第5部分，与JR/T 0025的第4部分、第6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5部分：借记/贷记卡片规范

1 范围

JR/T 0025的本部分从卡片的角度描述了借记/贷记交易流程，包括卡片内部的处理细节、卡片所使用的数据元、卡片所支持的指令集等。

本部分适用于由银行发行或受理的金融借记/贷记IC卡。其使用对象主要是与金融借记/贷记IC卡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的本部分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 4880.1 语种名称代码 第1部分:2字母代码(GB/T 4880.1—2005,ISO/IEC 639-1:2002,MOD)

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 17552 识别卡 金融交易卡(GB/T 17552—1998,ISO/IEC 7813:1995,IDT)

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 0025.6 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 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 7816-4 识别卡 带触点的集成电路卡 第4部分：行业间交换用命令

ISO/IEC 8859-1～ISO/IEC 8859-10 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JR/T 0025的本部分。

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

路径 path

没有分隔的文件标识符的连接。

3.11

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，或者用于支付系统应用目的的目录定义文件（DDF）被选择后，IC 卡中所确立的逻辑条件集合。

3.12

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。

3.13

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。

3.14

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）。

3.15

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

下列缩略语和符号适用于JR/T 0025的本部分。

AAC 应用认证密文（Application Authentication Cryptogram）

AAR 应用授权参考（Application Authorization Referral）

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）
APDU	应用协议数据单元（Application Protocol Data Unit）
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）
CLA	命令报文的类别字节（Class Byte of the Command Message）
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）
ICC	集成电路卡（Integrated Circuit Card）
M	必备（Mandatory）
MAC	报文鉴别码（Message Authentication Code）
MDK	主密钥（Master DEA Key）
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）
UDK	子密钥（Unique DEA Key）

5 概述

本章概述了JR/T 0025借记/贷记交易。交易流程图画出了交易中各功能的执行顺序。本章最后描述了卡片和终端支持的功能和命令要求。

5.1 功能概述

下面是JR/T 0025借记/贷记交易处理中用到的功能。有些必备功能中的某些步骤是可选。没有标注必备的功能是可选，是否执行要由卡片或终端中的参数决定。

5.1.1 应用选择（必备）

面对一张JR/T 0025借记/贷记卡片，终端要决定哪些是卡片和终端都支持的应用。终端显示所有两方都支持的应用，由持卡人选择哪一个应用用于支付。如果这些应用不能在终端显示出来，终端选择由发卡行在卡片个人化时指定的优先级最高的应用。

5.1.2 应用初始化/读应用数据（必备）

在选择了JR/T 0025借记/贷记应用以后，终端要求卡片明确应用支持的数据和功能。根据应用的不同情况（国内或国外）卡片确定的数据或者支持的功能可能不同。终端读出卡片指定的数据，使用支持功能列表决定要执行的处理流程。

5.1.3 脱机数据认证（可选）

根据终端与卡片的支持情况，由终端决定是否使用脱机静态或动态数据认证进行卡片脱机认证。

静态数据认证（SDA）验证卡片中的重要数据在发卡后是否被篡改。终端使用卡片中的发卡行公钥验证卡片中的静态（不变）数据，发卡行公钥保存在卡片中的发卡行公钥证书中。数字签名包括一个重要数据哈希结果，使用发卡行私钥签名加密。还原出的哈希值与实际应用数据所产生的哈希值匹配证实了数据并未被修改。

动态数据认证（DDA）验证卡片中的重要数据在发卡后是否被篡改，同时验证卡片是否为伪卡。DDA有两种形式：标准DDA和复合动态数据认证/应用密文生成（CDA）。这两种方式中，终端使用类似SDA的方法验证卡片中的静态数据。

标准DDA为终端请求卡片使用来自卡片和终端的动态数据和IC卡私钥生成一个动态签名密文。终端使用从卡片中恢复出来的IC卡公钥对动态签名密文解密。恢复的数据和原始数据匹配验证了此卡片不是从一张合法卡片通过复制数据而生成的伪卡。

CDA、动态签名密文生成和卡片行为分析处理阶段的生成卡片应用密文组合在一起以确保应用密文来自有效的卡片。

5.1.4 处理限制（必备）

终端执行交易处理限制判断交易是否允许进行。终端检查卡片的有效期是否达到，卡是否失效，卡片和终端的应用版本是否匹配，应用用途控制（AUC）限制是否生效。发卡行可以使用AUC限制卡片的应用，包括：国内、国外、现金、商品、服务或返现。

5.1.5 持卡人验证（可选）

持卡人验证可以用来确保持卡人是合法而且卡片没有遗失或被盗。终端使用卡片中的持卡人验证方法（CVM）列表数据决定验证的执行方法。CVM列表建立了持卡人验证方法优先级别，根据终端能力和交易特性提示用户采用特定的持卡人验证方法。如果持卡人验证方法是脱机PIN，终端提示持卡人输入PIN并传送持卡人输入的PIN到卡片中，卡片比较输入的PIN和卡片中的PIN值。CVM也可能指定联机PIN、签名或不需要持卡人验证。

5.1.6 终端风险管理（必备）

终端风险管理检查交易是否超过了最低限额，账号是否在终端异常文件中，连续脱机交易次数是否超过了限制次数，是否新卡，以及商户是否强制进行联机，有些交易可能被随机的选择联机处理。

终端风险管理也包括可选的频度检查，终端使用卡片中的数据进行检查。在终端行为分析过程中要考虑终端频度检查的结果。

5.1.7 终端行为分析（必备）

终端行为分析根据脱机数据认证、交易处理限制和终端风险管理结果，持卡人验证结果和卡片和终端里设置的规则来决定交易应该接受脱机，送去联机授权或拒绝。卡片规则在由卡片送给终端的发卡行行为代码（IAC）数据域中设置。支付系统的规则在终端行为代码（TAC）中设置。在决定了交易的处理结果后，终端向卡片请求一个应用密文。应用密文的类型取决于交易的处理结果，见表1应用密文类型。终端请求中指明交易是否执行复合CDA。

表1 应用密文类型

	密文类型
批准交易	TC
联机交易	ARQC
拒绝交易	AAC

5.1.8 卡片行为分析（必备）

收到终端发来的应用密文请求后，卡片执行卡片行为分析。卡片可以执行卡片风险管理，以决定是否改变由终端做出的交易处理结果。可以包括的检查有前次没完成的联机交易，前次交易中发卡行认证失败或脱机数据认证失败，频度检查的交易次数和金额总量是否达到限制数。卡片可以将终端请求的脱机接受改成联机授权或脱机拒绝。卡片不能推翻终端做出的拒绝交易的决定。

检查完成后，卡片使用应用数据和卡片中的一个对称密钥生成应用密文，返回给终端。对于脱机接受的交易，TC和用来生成TC的数据通过清算报文传送，用于未来持卡人争议或退单处理。当一个持卡人质疑一笔交易的时候TC可以作为一个交易“证据”用来证明商户或收单行没有修改交易数据。对于脱机拒绝交易，密文类型为AAC。对于请求联机授权的交易，密文类型为ARQC。

当卡片作出接受交易的结论（卡片返回TC）后，卡片会记录交易明细。

5.1.9 联机处理（可选）

如果卡片和终端决定交易需要一个联机授权，而且终端具有联机能力，则终端传送一个联机授权报文给发卡行。这个报文包括ARQC密文、生成ARQC的数据和脱机处理结果指示器。在联机处理阶段，发卡行使用一个名为卡片认证方法（CAM）的处理过程验证ARQC来鉴别卡片。发卡行可以在它的授权决定中考虑CAM和脱机处理的结果。

传送回终端的授权响应报文包括发卡行生成的授权响应密文（ARPC）（由ARQC，授权响应码和卡片对称密钥生成）。这个响应也可能包括称为发卡行脚本的二次发卡（post-issuance）更新。

如果授权响应包含ARPC而且卡支持发卡行认证，卡片通过验证ARPC执行发卡行认证，验证响应来自真实的发卡行（或其代理）。一旦发卡行认证成功，卡片可以重新设置卡片中一些和风险控制相关的参数。这样阻止了通过模拟联机处理和伪造接受交易来重新设置计数器和指示器攻击卡片的安全特性。如果发卡行认证失败，卡片的后续交易将联机进行授权直到发卡行认证成功。发卡行可以选择当发卡行认证失败时设置卡片拒绝交易。

5.1.10 交易结束（必备）

卡片和终端执行最后的交易结束处理。发卡行接受的交易可能因为发卡行认证结果和卡片中的发卡行编码参数而被修改为拒绝。卡片使用交易处理结果、发卡行认证结果和发卡行编码规则决定是否重新设置基于卡片的计数器和指示器（位）。卡片接受交易生成TC，拒绝交易生成AAC。

如果终端在授权报文后传送一个清算报文，TC要在清算报文中。

当卡片作出接受交易的结论（卡片返回TC）后，卡片会记录交易明细。

5.1.11 发卡行脚本处理（可选）

如果发卡行在授权响应报文中包括了更新脚本，终端传递这些脚本命令给卡片。在处理更新之前，卡片执行安全验证确保脚本来自认证过的发卡行而且在传输过程中没有被修改。支持的脚本命令允许更新脱机处理参数、锁定和解锁应用、锁卡、重新设置脱机PIN尝试计数器以及修改脱机PIN值。

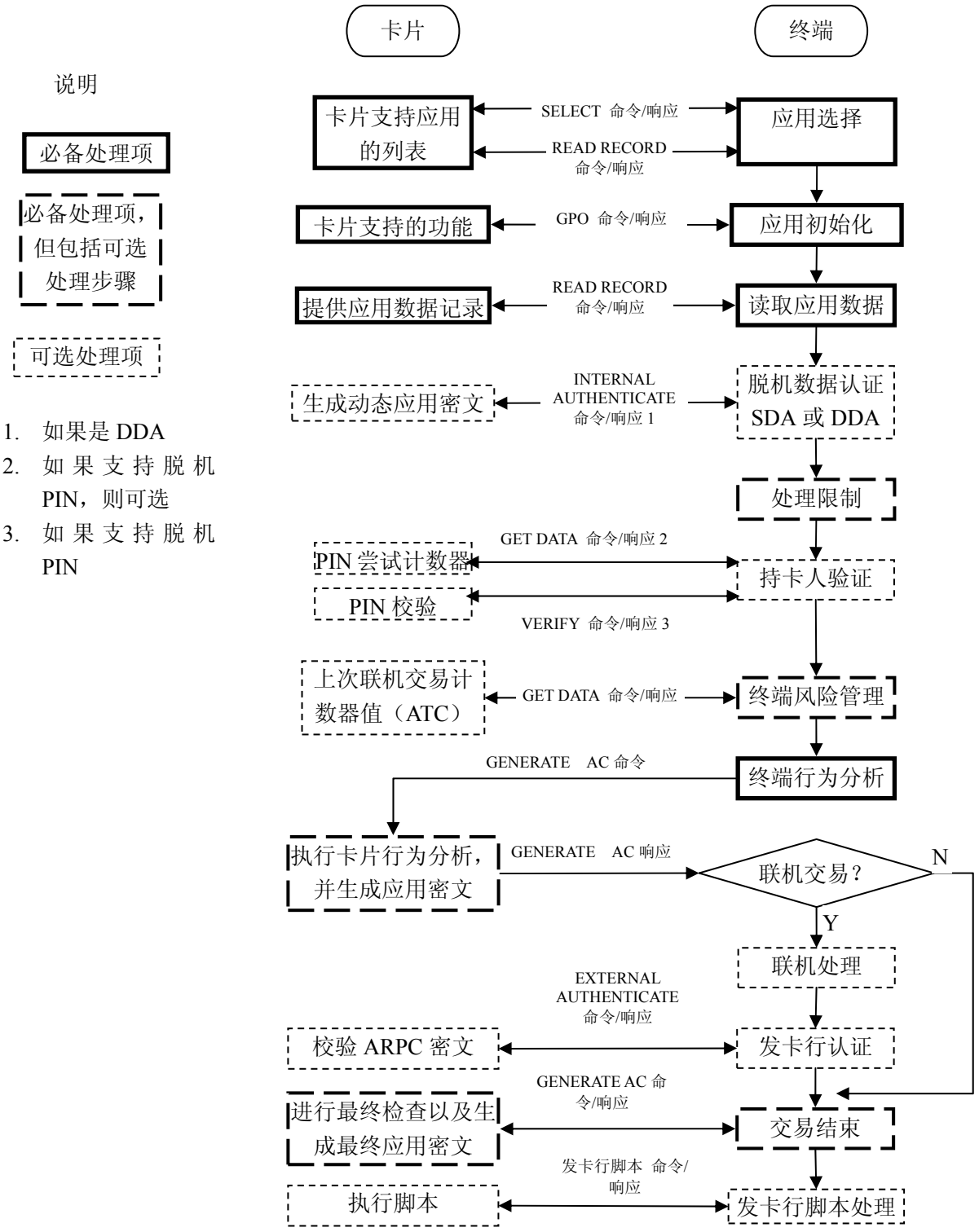


图1　交易流程实例

5.2　必备与可选功能

5.2.1　卡片功能需求

JR/T 0025借记/贷记卡片应支持表2中列出的必备功能。可选功能由发卡行或者市场需求来决定。如果相关条件满足，有条件的功能也要支持。

表2　卡片功能需求

功能	卡片支持
应用选择	必备（EMV）
● 目录选择方式	可选（EMV）
● 直接选择方式	必备（EMV）
应用初始化	必备（EMV）
读应用记录	必备（EMV）
脱机数据认证	可选（EMV）
● SDA	可选（EMV）有条件——如果支持 DDA（JR/T 0025 借记/贷记）
● 标准 DDA	可选（EMV）有条件——如果支持 CDA（JR/T 0025 借记/贷记）
● 复合 DDA/应用密文生成	可选（EMV）
处理限制	必备（EMV）
● 应用版本号检查	必备（EMV）
● 应用用途控制检查	可选（EMV）
● 生效日期检查	可选（EMV）
● 失效日期检查	必备（EMV）
持卡人验证	可选（EMV）
● 单独的 CVM	可选（EMV）
终端风险管理	可选（EMV）必备（JR/T 0025 借记/贷记）
● 终端异常文件检查	n/a（卡片没有处理）
● 商户强制联机	n/a（卡片没有处理）
● 最低限额检查	n/a（卡片没有处理）
● 交易日志	n/a（卡片没有处理）
● 随机选择	n/a（卡片没有处理）
● 频度检查	可选（EMV）
● 新卡检查	可选（JR/T 0025 借记/贷记）
终端行为分析	IAC 可选（EMV）IAC 需要（JR/T 0025 借记/贷记）
卡片行为分析	必备（EMV）
● 联机/脱机决定	必备（EMV）
● 卡片风险管理	可选（EMV）必备（JR/T 0025 借记/贷记）在卡片风险管理中有些步骤是可选的
● 通知报文	可选（EMV）
● 应用密文	提供算法选择（EMV） 提供多算法选择（JR/T 0025 借记/贷记）
联机处理	
● 联机能力	必备（EMV）
● 发卡行认证	可选（EMV）
交易结束	必备（EMV）
发卡行到卡片脚本处理	可选（EMV）
● 安全报文	给出两种脚本形式（EMV） 仅支持一种脚本形式（JR/T 0025 借记/贷记）

5.2.2　命令支持需求

卡片支持的命令在表3中描述。

表3　命令支持需求

命令	卡片支持
应用锁定 APPLICATION BLOCK	应用锁定功能可选，如果支持，推荐使用应用锁定命令（JR/T 0025 借记/贷记）
应用解锁 APPLICATION UNBLOCK	应用解锁功能可选，如果支持，推荐使用应用解锁命令（JR/T 0025 借记/贷记）
卡片锁定 CARD BLOCK	卡片锁定是推荐功能，可通过卡片锁定命令实现（JR/T 0025 借记/贷记）
外部认证 EXTERNAL AUTHENTICATE	有条件的——如果支持发卡行认证（EMV）
生成应用密文 GENERATE AC	必备（EMV）
取数据 GET DATA	可选（EMV） 必备（JR/T 0025 借记/贷记）
获取处理选项 GET PROCESSING OPTIONS	必备（EMV）
内部认证 INTERNAL AUTHENTICATE	有条件的——如果支持 DDA（EMV）
PIN 修改/解锁 PIN CHANGE / UNBLOCK	如果支持脱机 PIN。则 PIN 解锁功能必备，可使用 PIN 修改/解锁命令实现（JR/T 0025 借记/贷记） PIN 修改功能可选，如果使用则应在发卡行可控的环境下（JR/T 0025 借记/贷记）
设置数据 PUT DATA	可选（JR/T 0025 借记/贷记）
读记录 READ RECORD	必备（EMV）
选择 SELECT	必备（EMV）
修改记录 UPDATE RECORD	可选（JR/T 0025 借记/贷记）
验证 VERIFY	有条件的——如果支持脱机 PIN（EMV）

6　应用选择

应用选择处理决定了选择哪一个卡片和终端都支持的应用来完成交易。这一处理分为两个步骤：

步骤 1：终端建立终端和卡片都支持的应用列表；

步骤 2：从列表中确定一个应用来处理交易。

6.1　卡片数据

应用选择使用的卡片数据元和简单描述在表4中列出。附录A卡片和发卡行数据元表中有这些数据元以及他们使用的描述。

表4　应用选择——卡片数据

数据元	描述
应用标识符（AID）	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。它标识了在 GB/T 16649.5 中描述的应用

数据元	描述
	如果一张卡片中有超过一个应用使用相同的 AID，卡片 AID 应要有一个后缀。如果只有一个应用有这个 AID，则卡片 AID 不应该有后缀除非在卡片个人化以后另一个有同样 AID 的应用可能加到卡片中
应用定义文件（ADF）	应用基本文件（AEF）的入口文件，应用基本文件（AEF）包含应用数据元 FCI 模板 ● DF 名称 ● FCI 专有模板 应用标签 应用优先指示器（有条件。如果卡片包括多个支付账户，在磁条中有映射的账户优先级应为 1） PDOL（可选） 首选语言（可选） 发卡行代码表索引（可选。如果应用首选名称存在） 应用首选名称（可选） FCI 发卡行自定义数据（可选），如果卡片支持日志，则日志入口（9F4D）数据元在发卡行自定义数据中
应用基本文件（AEF）	应用基本文件，包括应用处理过程中使用的数据元
应用标签	用于应用选择。存在于 ADF 的 FCI 中（可选）和 ADF 目录入口中（必备）
应用首选名称	如果应用首选名称存在而且终端支持发卡行代码表索引入口，在应用选择的最后，是应用首选名称而不是应用标签显示给持卡人 应用首选名称应该和应用标签一样，不过也可以把它留给客户进行定制处理
应用优先指示器	表明一个目录中指定应用的优先级以及是否应要持卡人确认才能选择
目录定义文件（DDF）	定义其下目录结构的文件，DDF 的 FCI： FCI 模板 ● DF 名称 ● FCI 专有模板 目录文件的短文件标识符 SFI FCI 发卡行自定义数据（可选）
目录文件	一个文件，列出了目录下的 DDF 和 ADF。在选择后，使用读记录（READ RECORD）命令对它进行访问
文件控制信息（FCI）	选择（SELECT）命令的响应信息，选择不同类型的文件，响应信息不同
发卡行代码表索引	按 ISO/IEC 8859，指明在终端显示应用首选名称时使用的代码表
支付系统环境（PSE）	PSE 从名为“1PAY.SYS.DDF01”的 DDF 开始。此 DDF 的相关目录文件叫支付系统目录
支付系统目录	支付系统目录包括 ADF 和 DDF 的入口，入口格式见 JR/T 0025.3 的表 46 和表 47
处理选项数据对象列表（PDOL）	在应用初始化步骤，卡片需要的终端数据对象表，内容包括数据对象的标签和长度
短文件标识符（SFI）	短文件标识符是基本文件的指针 1-10 JR/T 0025 定义 11-20 支付系统定义 21-30 发卡行定义

6.2 终端数据

应用选择使用的终端数据在表5中描述。终端数据的描述见JR/T 0025.6。

表5　应用选择——终端数据

数据元	描述
AID	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。它标识了在 GB/T 16649.5 中描述的应用。见表 4 中的描述
应用选择指示器	表明终端是否支持部分 AID 选择
终端支持的应用列表	终端维护的一个表包括支持的应用和它们各自的 AID

6.3　命令

选择（SELECT）

选择命令见附录B中描述。

终端发送选择（SELECT）命令给卡片获取卡片支持的应用信息。应用信息包括发卡行参数，例如：选择应用的优先级别，应用名称，首选语言。命令中既可以包括支付系统环境目录名称（用于目录选择方式），一个目录名，或者一个被请求的AID（用于AID列表选择方式）。

命令的P1参数表明应用是按照名称方式选择的。P2参数表明在支持AID后缀的情况下是否有另外使用同样AID的应用被请求（当卡片支持多应用使用同样AID的时候）。

命令可以有下列SW1 SW2返回状态字：

——9000——选择（SELECT）命令成功返回；

——6A82——在命令包含支付系统环境名称情况下，卡片不支持目录选择方式；在命令包含 AID 的情况下，表示选择的文件没有找到或已经是相同 AID 的最后一个文件而 P2 参数指定还有下一个相同 AID 的应用可选；

——6A81——卡片锁定或命令不支持；

——6283——选择文件无效。

如果卡片包括一个PDOL，PDOL作为FCI的一部分包括在选择（SELECT）命令的响应信息中。在应用初始化处理中终端将PDOL中指定的数据送入卡片。

读记录（READ RECORD）

读记录（READ RECORD）命令见附录B中描述。

当使用目录选择方式时，读记录（READ RECORD）命令用来读取支付系统环境目录中的记录。只有在一个ADF或DDF选择以后使用。命令包括要读取文件的短文件标识符（SFI）和文件中的记录号。

卡片在响应信息中返回请求的记录内容。SW1 SW2可以有下列返回值：

——9000——成功执行；

——6A83——记录号不存在。

6.4　建立候选应用列表

终端使用两种方法建立卡片和终端都支持的应用列表。

——目录选择方式对于终端是必备要求，对于卡片是可选的。终端应优先选择此方式。终端从卡片中读取支付系统环境文件。此文件列出卡片支持的所有支付应用。终端将卡片列表和终端列表中都有的应用加入候选列表中；

——AID 列表选择方式是卡片和终端都必备要求的。终端为每一个终端支持的应用发送一个选择（SELECT）命令给卡片。如果卡片响应指出卡片支持此应用，终端加此应用到候选列表。

6.4.1　目录选择方式

从卡片角度来看，目录选择方式处理包括下列步骤：

步骤 1：卡片接收一个来自终端的选择（SELECT）命令，请求选择 PSE（文件名“1PAY.SYS.DDF01”）；

——如果卡片锁定或者选择（SELECT）命令不支持，卡片响应 SW1 SW2=“6A81”；

——如果卡片中没有 PSE，卡片响应选择（SELECT）命令指出文件不存在（SW1 SW2=“6A82”）；

——如果 PSE 锁定，卡片响应“6283”；

——如果 PSE 找到，卡片响应“9000”返回 PSE 的 FCI。

步骤 2：如果 PSE 找到，卡片接受终端发出的表明短文件标识和记录号的读记录（READ RECORD）命令，卡片对每一个读记录（READ RECORD）命令响应请求的记录内容和返回状态字 SW1 SW2=“9000”。当请求的记录不存在，卡片返回 SW1 SW2=“6A83”；

步骤 3：终端处理记录中的每一个入口。如果入口表明一个 DDF，终端发一个有此 DDF 名字的选择（SELECT）命令，卡片响应 DDF 的 FCI。FCI 包括一个目录文件的 SFI。

终端读取属于此 DDF 的目录文件中的所有记录，卡片对每个读记录（READ RECORD）命令返回请求的记录和状态字“9000”。当请求的记录不存在，卡片响应“6A83”，终端返回步骤 2 继续读 PSE 下的目录文件。

终端执行的步骤显示在图2所示：

步骤 1：从支付系统目录读记录 1；

步骤 2：检查 ADF 入口 1 或 2 中的 AID 是否和终端 AID 匹配。如果匹配，加入候选列表；

步骤 3：从支付系统目录读记录 2；

步骤 4：选择记录 2 中入口 1 指出的 DDF 目录；

步骤 5：读 DDF 目录文件中的记录 1；

步骤 6：检查记录 1 中 ADF 入口 1 或 2 中的 AID 是否和终端 AID 匹配。如果匹配，加入候选列表；

步骤 7：当卡片响应目录中没有其它记录时，返回前一个目录的处理入口和记录；

步骤 8：检查支付系统目录文件中记录 2 内入口 2 是否和终端 AID 匹配。如果匹配，加入候选列表；

步骤 9：当卡片响应支付系统目录中没有其它记录，建立候选列表结束。

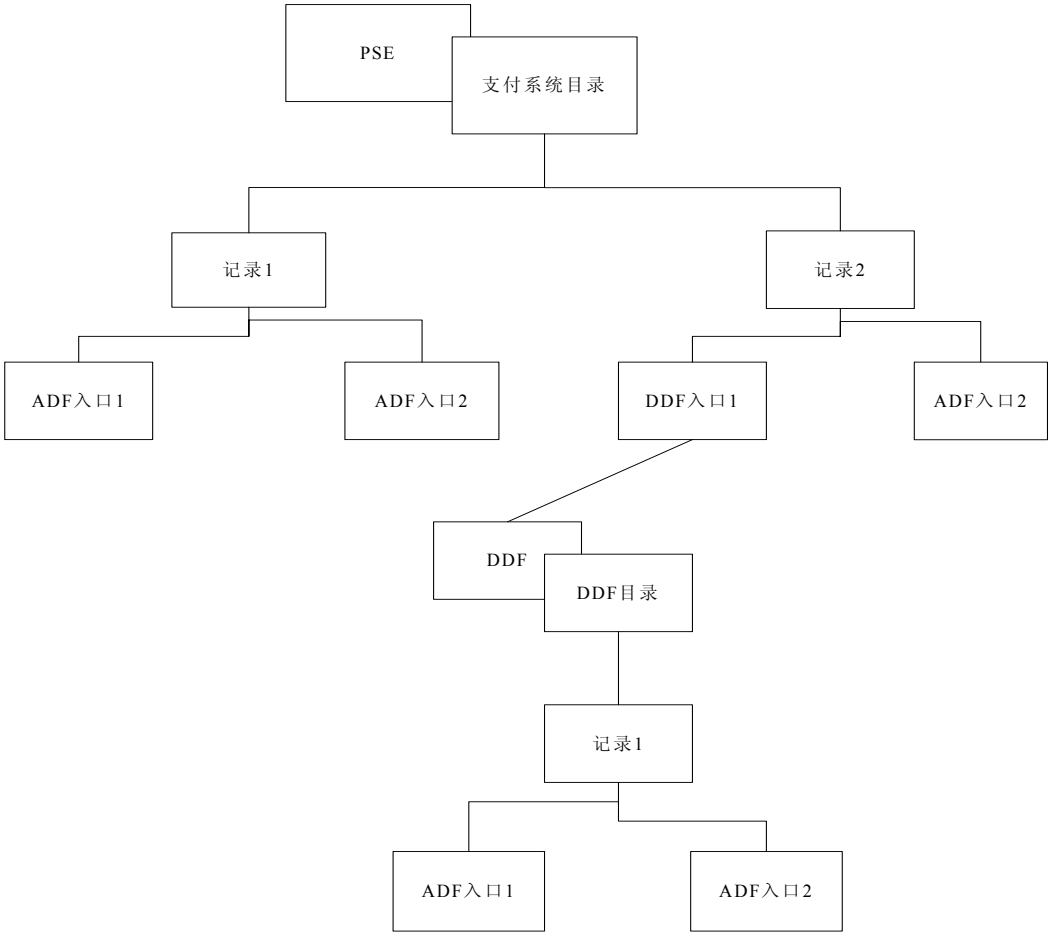


图2　卡片目录结构例子

6.4.2　AID 列表选择方式

从卡片的角度来看，AID列表选择方式包括下列步骤：

步骤 1：卡片收到终端发来选择（SELECT）命令，命令包括终端支持的应用列表中的 AID。卡片检查是否卡片中有匹配的 AID 应用（卡片 AID 长度可以长于终端 AID，但仍然认为匹配）。

AID匹配的例子在表6中显示。

表6　AID 匹配例子

终端 AID	终端应用	卡片 AID	卡片应用
A0000003330101	JR/T 0025 借记/贷记	A000000333010101	JR/T 0025 借记
A0000003330101	JR/T 0025 借记/贷记	A000000333010102	JR/T 0025 贷记

——如果 AID 匹配，卡片响应选择（SELECT）命令指明卡片支持此应用（SW1 SW2=“9000”）；

——如果卡片找不到匹配的 AID，卡片响应状态字 SW1 SW2=“6A82”指明应用没找到；

——如果卡片锁定或不支持选择（SELECT）命令，卡片响应状态字 SW1 SW2=“6A81”指明交易应被中止。

步骤 2：如果匹配的卡片 AID 长度比终端 AID 长，卡片在选择（SELECT）命令响应信息中返回完整的 AID 给终端。

——卡片接收终端发来的第 2 个选择（SELECT）命令，参数 P2 设置为“02”表明卡片要选择有同样 AID 的下一个应用；

——卡片选择下一个应用并在选择（SELECT）命令响应中提供这一应用给终端；

——当卡片不再有应用有此 AID，卡片响应“6A82”表明所有匹配的应用都已经选择。

6.5　确定和选择应用

如果候选列表中至少有一个双方都支持的应用，终端和持卡人决定选择哪个应用。终端发一个选择（SELECT）命令给卡片指出此应用确认用来处理交易。如果卡片决定此应用可以处理交易，响应“9000”。如果应用锁定，卡片响应“6283”。

6.6　流程图

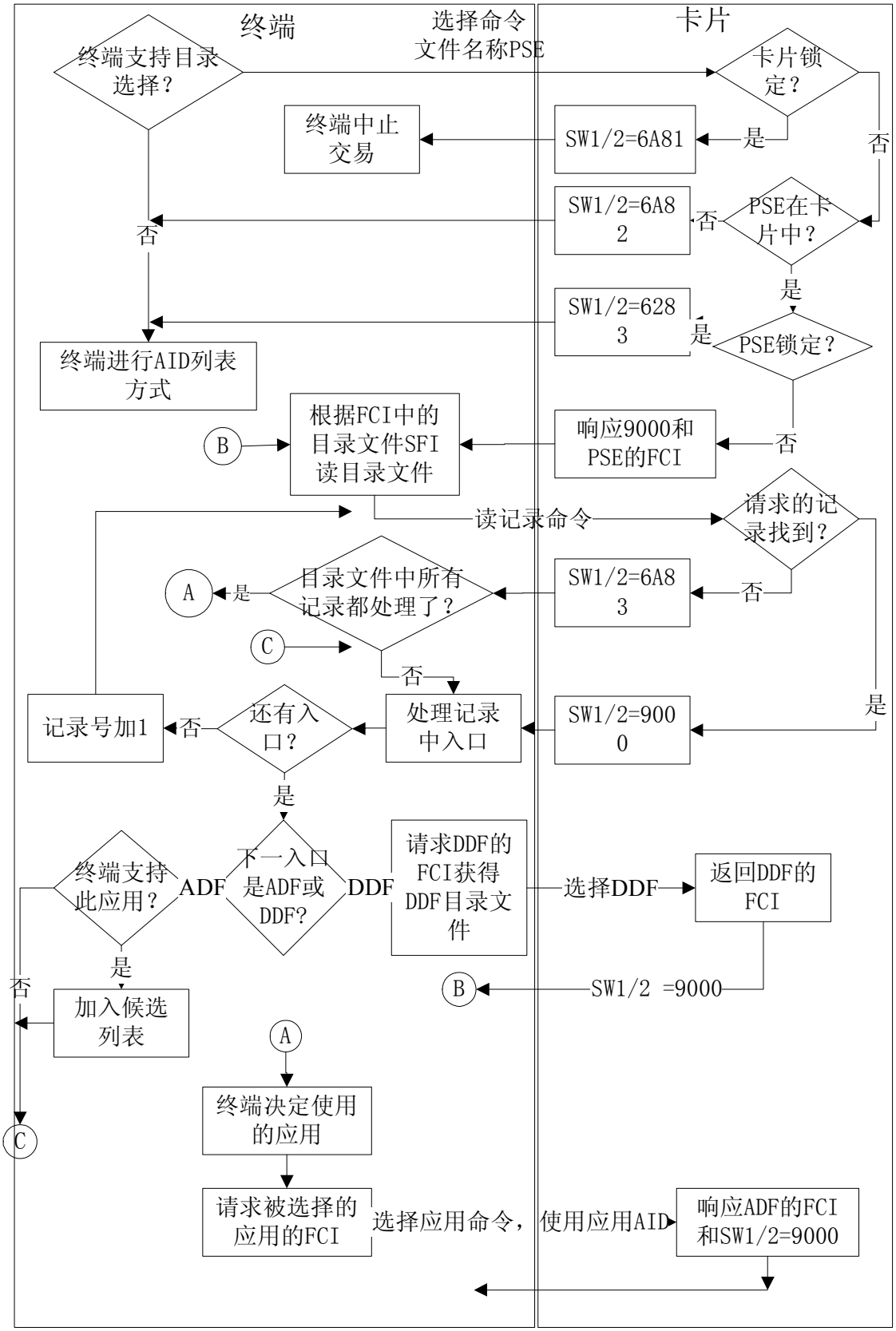


图3　使用目录方式进行应用选择

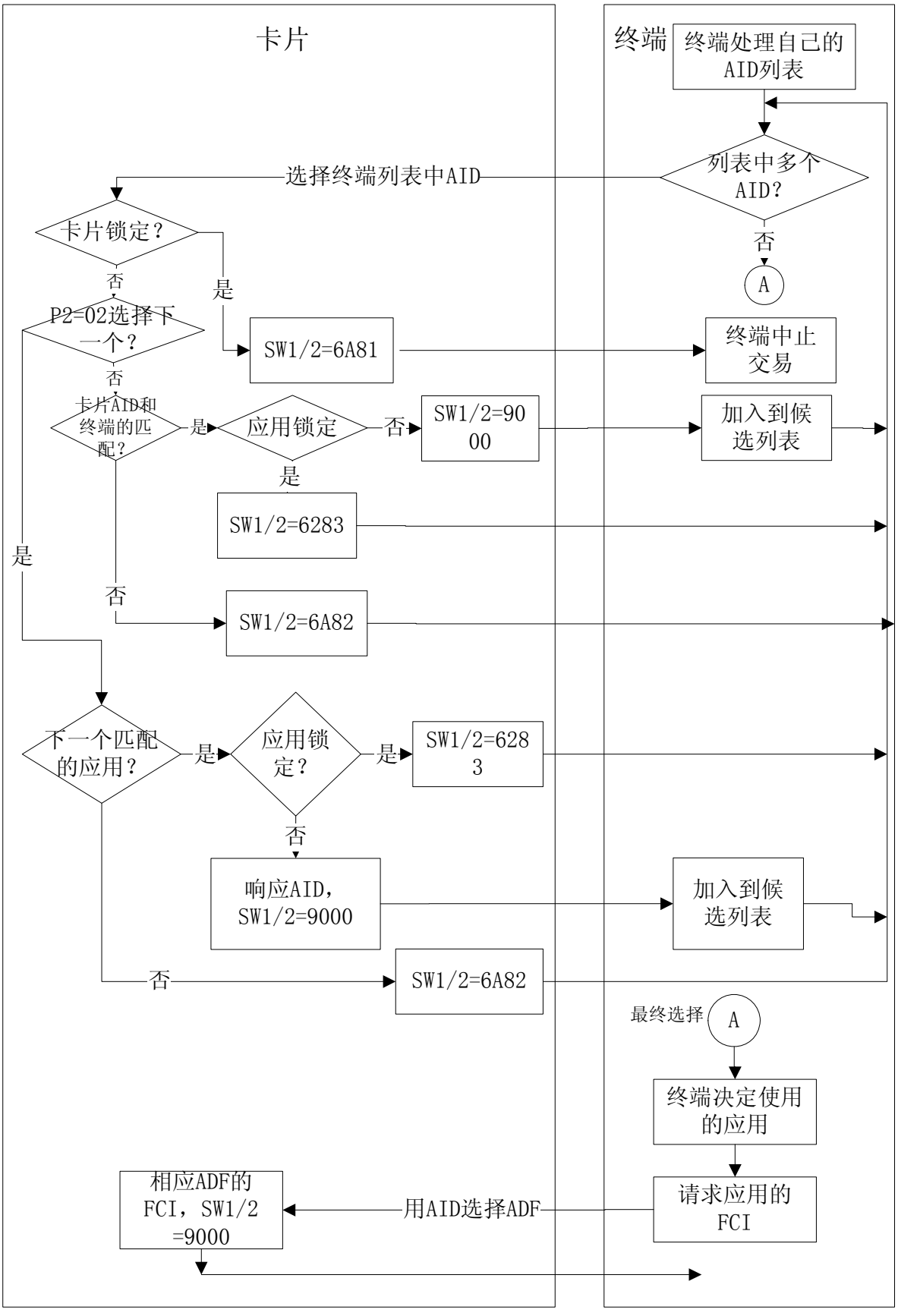


图4　使用 AID 列表选择方式进行应用选择

6.7 后续相关流程

应用初始化

终端发送获取处理选项（GPO）命令给卡片，如果在应用选择时选择（SELECT）命令的响应信息中包括PDOL，GPO命令中包括PDOL中指定的终端数据，例如交易日志记录里需要的终端数据。

如果某些限制不允许选择的应用做初始化，终端中止应用并返回应用选择步骤选择另一个应用。

7 应用初始化

在应用初始化处理中，终端通过发送获取处理选项（GPO）命令给卡片通知卡片交易处理开始。在命令中，终端提供给卡片在处理选项数据对象列表（PDOL）中请求的数据元。PDOL（一个数据元标签和长度的列表）是在应用选择处理中由卡片返回给终端的可选数据项。

卡片对GPO命令的响应信息包括：AIP和AFL。AIP列出了交易在处理过程中执行的功能；AFL列出交易需要读出的数据存放的短文件标识符、记录号、记录个数以及脱机数据认证需要的静态签名数据的存放位置。

7.1 卡片数据

应用初始化处理使用的卡片数据在表7中列出。

表7 应用初始化——卡片数据

数据元	描述
应用文件定位器（AFL）	说明终端作交易处理要读出的卡片数据存放的文件位置和记录范围。对每个要读出的文件，AFL 包括下列信息： ● 字节 1——短文件标识符（一个文件的数字标签） ● 字节 2——第 1 个要读出的记录号 ● 字节 3——最后一个要读出的记录号 ● 字节 4——存放用于脱机数据认证的数据的连续记录个数，字节 2 指出的是第 1 条要读的记录号
应用交互特征（AIP）	一个列表，说明此应用中卡片支持指定功能的能力（SDA、标准 DDA、CDA、终端风险管理、持卡人验证和发卡行认证） AIP 在个人化时应被写入卡中用来指明支持终端风险管理和持卡人验证
应用交易计数器（ATC）	应用个人化后，卡片应用交易计数器启动
卡片验证结果（CVR）	JR/T 0025 专用数据，表明从卡片角度来看本次和前次交易的脱机处理结果。数据存放在卡片中，作为发卡行应用数据的一部分联机上送
密文信息数据（CID）	指明卡片返回的密文类型和终端需要进行的后续处理行为。在应用初始化处理时被初始为全 0
处理选项数据对象列表（PDOL）	在应用初始化步骤，卡片在处理 GPO 命令时需要由终端提供的数据元的标识和长度列表

7.2 终端数据

在应用初始化处理中使用的终端数据在表8中列出。

表8 应用初始化——终端数据

数据元	描述
PDOL 中定义的其它数据	PDOL 中指定的来自终端的其它数据，例如交易日志记录里需要的终端数据

7.3 命令

获取处理选项（GPO）

终端使用获取处理选项（GPO）命令通知卡片交易开始。

命令中包含卡片在PDOL中列出的终端数据元的值部分，PDOL是卡片在应用选择阶段返回的可选数据。

卡片响应数据内容为AIP和AFL。AIP列出了交易在处理过程中执行的功能；AFL列出交易需要的数据存放的短文件标识符、记录号、记录个数以及脱机数据认证需要的静态签名数据的存放位置。

命令编码见附录B。

7.4 处理流程

卡片收到终端发送的获取处理选项（GPO）命令后，卡片：

步骤 1：如果卡片支持自定义限制检查并且处理选项命令中包括 PDOL 中指定的终端数据，卡片执行自定义的限制检查。如果限制检查不通过，卡片响应“使用条件不满足”（SW1 SW2=“6985”）提示终端将当前应用从候选列表中删除并返回应用选择步骤选择另一个应用；

步骤 2：决定要读取的文件记录，文件位置，建立 AFL。针对交易的不同情况可以返回不同 AFL 和 AIP；

步骤 3：如果自定义限制检查通过，卡片：

a) ATC 加 1，如果此时 ATC 达到 65535，则卡片应永久锁定应用；

b) 密文信息数据（CID）置零；

c) 卡片验证结果（CVR）置零（长度指示位除外）；

d) 卡片返回 AIP 和 AFL。

图5显示了应用初始化处理流程图。

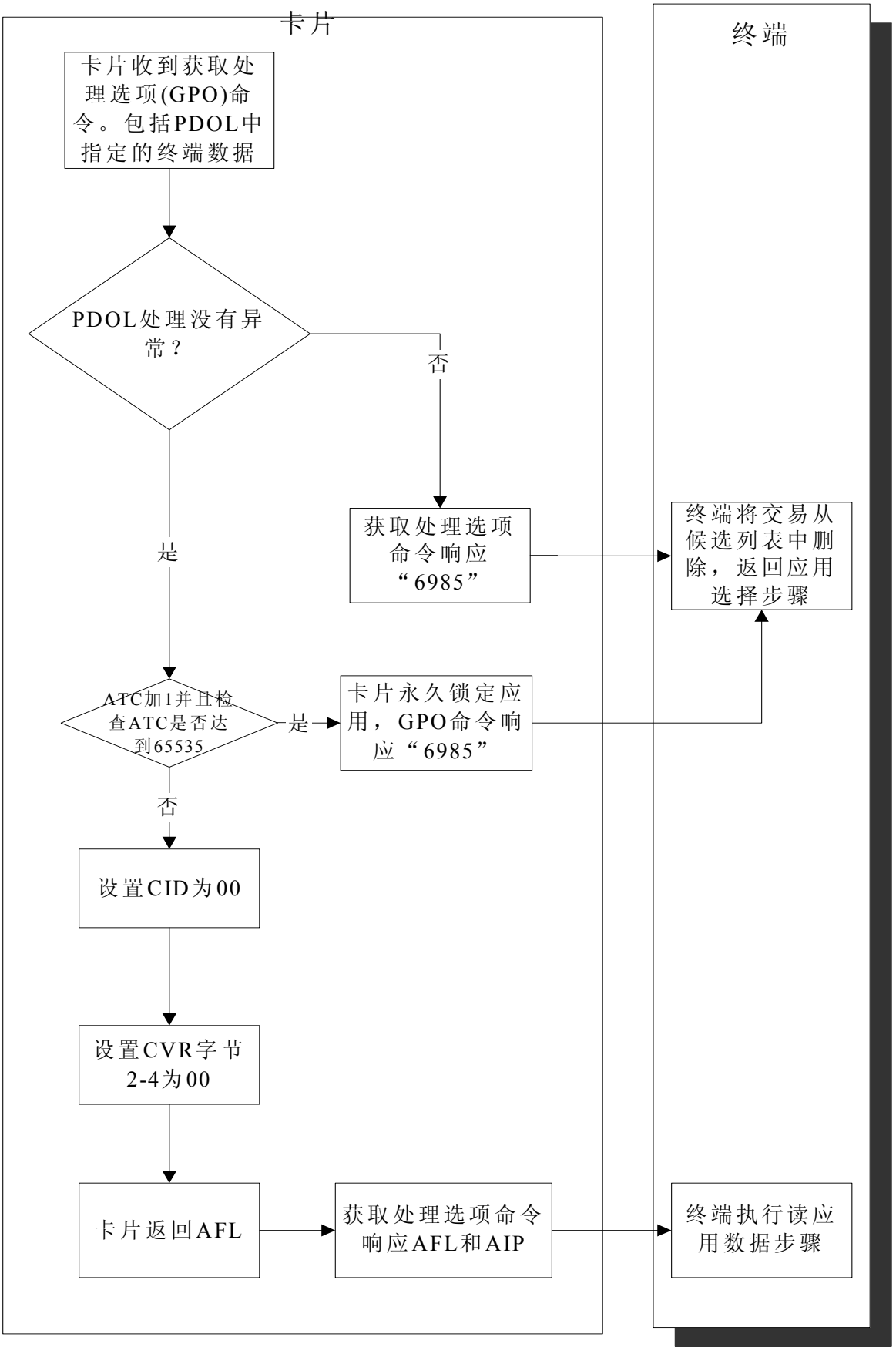

卡片
终端
卡片收到获取处理选项(GPO)命令。包括PDOL中指定的终端数据
PDOL处理没有异常？
否
是
获取处理选项命令响应“6985”
终端将交易从候选列表中删除，返回应用选择步骤
ATC加1并且检查ATC是否达到65535
是
卡片永久锁定应用，GPO命令响应“6985”
否
设置CID为00
设置CVR字节2-4为00
卡片返回AFL
获取处理选项命令响应AFL和AIP
终端执行读应用数据步骤

图5　应用初始化流程图

7.5 前期相关处理

应用选择

在选择（SELECT）命令响应的FCI中卡片提供PDOL（如果存在）给终端。

7.6 后续相关处理

应用选择

如果卡片使用限制生效，交易返回应用选择阶段，此应用从候选列表中删除，选择另一个应用。

读应用数据

在获取处理选项（GPO）命令的响应数据中，卡片返回AFL给终端，终端使用AFL决定要从卡片中读取的应用数据和哪些数据用于脱机数据认证。

脱机数据认证

终端使用卡片在获取处理选项(GPO)命令的响应信息中的AIP决定卡片支持的脱机数据认证的类型。

持卡人验证

终端使用卡片在获取处理选项（GPO）命令的响应信息中的AIP决定卡片是否支持持卡人验证。

联机操作

终端使用卡片在获取处理选项（GPO）命令的响应信息中的AIP决定卡片是否支持发卡行认证。

8 读应用数据

在读应用数据处理中，终端读出卡片中处理交易和执行SDA或DDA的必要数据。

8.1 卡片数据

表9列出在读应用数据处理中使用，在前一步应用初始化处理中卡片返回的数据。

表9 读应用数据——卡片数据

数据元	描述
应用文件定位器（AFL）	在应用初始化处理中，卡片返回给终端的数据，包含了一组要求读取的记录入口，每一个入口包含： ● 文件的短文件标识符（SFI） ● 第 1 个和最后一个要读取记录的记录号 ● 用于保存 SDA 和 DDA 数据的记录个数。从文件中第 1 个开始读取的记录号开始计算

表10中列出读取卡片中应用基本文件记录的数据。

表10 读应用数据——卡片文件

数据元	描述
应用基本文件（AEF）	卡片数据文件，包括应用处理使用的数据。一个 AEF 包括一系列用记录号标识的记录。每个 AEF 用 SFI 唯一标识。终端使用读记录（READ RECORD）命令读取记录内容，命令中包括 SFI 和记录号
短文件标识符（SFI）	用来唯一标识应用数据文件。在 AFL 中列出，终端可以用来标识要读的文件

8.2 终端数据

卡片在此步骤中不使用终端数据。

8.3 命令

读记录（READ RECORD）

读记录（READ RECORD）命令编码见附录B。

卡片收到的命令中包括短文件标识符（SFI）和记录号。

卡片响应数据文件中的记录内容。

8.4 处理流程

卡片收到终端发送的读记录（READ RECORD）命令，返回终端请求的记录内容给终端。AFL中指定的每一条记录都是用一个读记录（READ RECORD）命令读出。

终端连续发读记录（READ RECORD）命令，直到AFL中指定的所有记录都读出。

用于脱机数据认证的记录数据是标识为‘70’的TLV编码格式。

使用读记录（READ RECORD）命令读出的数据见附录A.2。

8.5 前期相关处理

应用初始化

在应用初始化处理中，卡片返回AFL给终端指出终端要读出的数据记录。

8.6 后续相关处理

脱机数据认证

终端使用在读应用数据处理中建立的一个静态数据列表做SDA验证或DDA中使用的IC卡公钥验证。

9 脱机数据认证

脱机数据认证是终端使用公钥技术认证卡片中的数据的操作。脱机数据认证有两种类型：

——静态数据认证（SDA）；

——动态数据认证（DDA）。

SDA是终端认证卡片中静态（不变）数据。SDA可以确保卡片在个人化之后，发卡行选定的数据不会被篡改。

DDA包括标准DDA和复合DDA/应用密文生成（CDA）两种认证方式。在DDA的处理过程中，终端认证卡片中静态数据和卡片用交易唯一数据生成的密文。DDA可以确保卡片在个人化之后，发卡行选定的数据不会被篡改；DDA还可以防止伪卡（复制）。

脱机数据认证的结果是卡片和终端决定交易脱机、联机或拒绝的参考条件之一。联机授权系统在作出认证响应决定时同样可能要参考脱机数据认证结果。

具有脱机能力的终端应支持脱机数据认证，卡片是否支持是可选的。

9.1 密钥和证书

在JR/T 0025.7的5.1中描述。

9.2 决定脱机数据认证方法

终端使用卡片的应用交互特征（AIP）以及根据终端本身支持的脱机数据认证来决定是执行SDA，DDA还是CDA。

9.2.1 卡片数据

终端用来决定是否执行SDA或DDA的卡片数据在表11中列出。

表11 脱机数据认证——卡片数据

数据元	描述
应用交互特征（AIP）	包括指明： ● 卡片支持静态数据认证 SDA ● 卡片支持动态数据认证 DDA ● 卡片支持复合数据认证 CDA

9.2.2 处理流程

一次交易中只进行一种脱机数据认证。CDA优先级高于DDA，DDA的优先级高于SDA。如果卡片和终端一种脱机数据认证都不支持，脱机数据认证不执行。

如果终端测定卡片和终端都支持CDA，执行CDA；否则，如果都支持DDA，执行DDA；否则，如果都支持SDA，则执行SDA。

用于脱机数据认证的记录数据是标识为‘70’的TLV编码格式，对于文件的SFI分别在‘1-10’和‘11-30’的这两类文件，在脱机数据认证处理过程中的数据处理不同，见JR/T 0025.7的定义。

如果用于脱机数据认证的记录数据不是标识为‘70’的TLV编码格式，终端会认为脱机数据认证执行但是失败。终端将设置TSI中“脱机数据认证执行”位为1，同时设置TVR中相应的“SDA失败”或“DDA失败”或“CDA失败”位为1。

9.3 静态数据认证

在SDA处理中，终端使用公钥技术验证卡片中的关键数据自发卡后没有被改动。

9.3.1 卡片数据

终端在SDA处理中使用的卡片数据在表12中列出。

表12 SDA 中使用的卡片数据

数据元	描述
CA 公钥索引（PKI）	和发卡行公钥证书一起由 CA 提供。指明了终端里用于认证发卡行公钥证书的 CA 公钥
发卡行公钥证书	证书中包括了使用 CA 私钥签名的发卡行公钥
发卡行公钥指数	用于 RSA 算法中恢复签名静态应用数据。值为 3 或 65537
发卡行公钥余项	发卡行公钥没有包含在发卡行公钥证书中的部分（如果有）
AID 中的注册应用标识部分（RID）	和 CA 公钥索引一起用来标识终端中的公钥
签名的静态应用数据（SAD）	一个用来验证卡片静态数据的签名。在卡片个人化阶段，使用发卡行私钥签名的 SAD 保存在卡片中。推荐下列数据用来生成签名： ● 应用交互特征 AIP（如果支持 DDA） ● 应用生效日期 ● 应用失效日期 ● 应用主账号 ● 应用主账号序列号 ● 应用用途控制 AUC ● 持卡人验证方法（CVM）列表 ● IAC——缺省 ● IAC——拒绝 ● IAC——联机 ● 发卡行国家代码（“5F28”） 如果应用中签名的数据不是唯一，卡片应支持多个 SAD。举例来说，卡片给国内和国际交易分别设置 CVM 列表，而 CVM 列表是签名数据 如果发行后的卡片有修改签名数据的能力，则卡片应支持修改 SAD 的能力
SDA 标签列表	如果 AIP 也要签名，SDA 标签列表包括 AIP 的标签，如果支持 DDA 则建议将 AIP 做签名。除了 AIP 不能有其它数据标签

表13中是和SDA相关的卡片内部数据。

表13 和 SDA 相关的卡片数据

数据元	描述
卡片验证结果（CVR）	包括一个给后续交易参考的指示位，指示位在卡片行为分析时设置表明上次脱机拒绝交易的 SDA 失败
SDA 失败指示位	如果 SDA 失败并且交易脱机拒绝，在卡片行为分析过程中设置此位。根据发卡行认证的条件，在下一次联机交易的交易结束步骤中，此指示位复位

9.3.2 终端数据

在SDA过程中，卡片不需要终端数据。

9.3.3 命令

SDA操作没有使用命令。

9.3.4 处理流程

在SDA处理中，终端使用公钥验证技术恢复和验证发卡行公钥，并且验证卡片中的SAD。见JR/T 0025.7的5.2中的描述。概括的描述如下：

步骤 1：检索 CA 公钥

终端使用卡片中的PKI和RID确定使用哪一个CA公钥；

步骤 2：恢复发卡行公钥

终端使用CA公钥验证卡片中的发卡行证书并恢复证书中的发卡行公钥；

步骤 3：验证签名的静态应用数据

a) 恢复哈希结果；

b) 计算哈希；

c) 比较哈希结果。

如果所有的SDA步骤都成功，SDA通过。

9.4 动态数据认证

在DDA处理中，终端使用公钥技术验证卡片中关键数据自发卡后没有被改动，同时验证卡片是否是伪卡。

JR/T 0025支持两种DDA形式：标准DDA和CDA。在这两种方式里，终端验证卡片中的静态数据没有修改，同时验证卡片生成的动态密文。在标准DDA中，卡片在执行卡片行为分析之前，响应内部认证命令时使用卡片、终端和交易的动态数据生成动态签名。在CDA中，卡片在响应生成应用密文命令时生成动态签名，签名中包括应用密文、密文信息数据以及和标准DDA一样的终端、卡片和交易的动态数据。

9.4.1 卡片数据

除了SAD，SDA使用的所有数据DDA中都使用，表14中列出的数据仅用于DDA。

表14 脱机数据认证——DDA 卡片数据

数据元	描述
动态数据认证数据对象列表（DDOL）	指定在内部认证（INTERNAL AUTHENTICATE）命令中，卡片要求终端送入卡片的终端数据标签和长度列表。至少 DDOL 中要有终端不可预知数据的标签（“9F37”）
IC 卡动态数据	发卡行指定的包括在签名的动态应用数据中。JR/T 0025 里规定：1 字节为 IC 卡动态数长度；2，3 字节为 ATC
IC 卡动态数	IC 卡动态数据的一部分，卡片生成的随时间变化的数。JR/T 0025 建议为 ATC
IC 卡公钥证书	包含发卡行私钥签名的 IC 卡公钥，在卡片个人化时放入卡中。证书中有使用发卡行私钥作签名加密的静态应用数据
IC 卡公钥指数	用来恢复签名的动态应用数据，值为 3 或 65537
IC 卡公钥余项	没有包含在 IC 卡公钥证书内的 IC 卡公钥部分（如果存在）
签名的动态应用数据	卡片收到内部认证（INTERNAL AUTHENTICATE）命令生成的签名

在DDA处理中，卡片内部使用的数据元在表15中列出。

表15 脱机数据认证——DDA 处理中卡片内部数据元

数据元	描述
卡片验证结果（CVR）	包括和 DDA 相关的下列指示位： 上次交易脱机动态数据认证失败并且交易脱机拒绝 脱机数据认证执行

数据元	描述
IC 卡私钥	用来给动态应用数据签名加密的密钥
DDA 失败指示位	指示上次脱机拒绝交易的 DDA 认证失败。根据发卡行认证的条件，在下一次联机交易的交易结束步骤中，此指示位复位

9.4.2 终端数据

表16列出DDA处理中卡片使用的来自终端的数据。

表16 脱机数据认证——终端数据

数据元	描述
DDOL 中列出的不可预知数据和其它数据元	在内部认证（INTERNAL AUTHENTICATION）命令中的数据
缺省 DDOL	如果卡片中没有 DDOL，使用终端中缺省 DDOL

9.4.3 命令

9.4.3.1 内部认证命令

在标准DDA处理过程中，终端发送内部认证（INTERNAL AUTHENTICATE）命令。命令包括了DDOL或缺省DDOL中指明的终端动态数据。

为了确保内部认证（INTERNAL AUTHENTICATE）命令返回数据在256字节限制内，签名的动态应用数据加上可选的TLV格式编码的长度应该限制在JR/T 0025.7中定义的范围内。

当卡片收到内部认证（INTERNAL AUTHENTICATE）命令，使用IC卡私钥生成签名的动态应用数据。在内部认证（INTERNAL AUTHENTICATE）命令的返回中包含此动态签名。

具体的命令编码格式在附录B。

9.4.3.2 生成应用密文命令

终端在卡片行为分析处理步骤中发送第1次生成应用密文（GENERATE AC）命令，下面条件满足时，交易执行CDA：

当生成应用密文命令中参数P1的第5位为“1”,表明终端请求执行CDA且卡片AIP数据表明也支持CDA，当卡片返回一个TC或ARQC时，TC或ARQC要包括在DDA密文中。具体的描述在安全规范部分。

编码格式见附录B。

9.4.4 处理流程

在DDA处理步骤中，终端使用公钥技术验证卡片中的发卡行公钥证书、IC卡公钥证书和签名的动态应用数据（动态签名）。

在DDA处理过程中，卡片的唯一操作是生成动态签名。

DDA处理的描述见JR/T 0025.7的5.3。下面是一个概括性的描述。

9.4.4.1 标准动态数据认证

标准DDA的处理有以下步骤：

步骤 1：检索 CA 公钥

终端使用卡片中的PKI和RID确定使用哪一个CA公钥；

步骤 2：恢复发卡行公钥

终端使用CA公钥验证卡片中的发卡行证书并恢复证书中的发卡行公钥；

步骤 3：恢复 IC 卡公钥

终端使用发卡行公钥验证卡片中的IC卡公钥证书并恢复证书中的IC卡公钥和静态数据哈希结果。IC卡公钥证书确保IC卡公钥的合法性。终端用卡片中的实际数据元重新计算哈希值检查是否和恢复的哈希值匹配；

步骤 4：生成动态签名（仅用于标准 DDA）

终端发送内部认证命令请求一个动态签名。命令中包括了DDOL中指定的数据。

收到内部认证命令后，卡片：

a) 设置CVR中脱机动态数据认证执行位为“1”；

b) 连接内部认证命令中的终端数据和在IC卡动态数据中指定的卡片数据。见JR/T 0025.7部分5.3.5；

c) 用上一步连接的数据做哈希；

d) 将哈希包括在签名的动态应用数据中；

e) 使用IC卡私钥给签名的动态应用数据做签名；

f) 在内部认证命令的响应信息中返回签名的动态应用数据。

步骤5：动态签名验证（仅用于标准DDA）

终端执行下列步骤验证动态签名：

——使用IC卡公钥解密动态签名恢复数据元哈希值；

——使用动态数据元重新计算哈希；

——比较两个哈希是否匹配。

如果所有上述步骤成功，标准DDA通过。

9.4.4.2 复合动态数据认证/应用密文生成

CDA处理包括下列步骤：

——终端在读取应用数据后终端行为分析之前，执行标准DDA中步骤1到3；

——CDA剩下的卡片步骤是生成一个包括应用密文的动态签名。这一步在卡片收到生成应用密文命令时执行。只有当交易符合CDA的执行条件，而且应用密文类型是TC或ARQC时发生；

——CDA剩下的终端步骤是验证卡片生成动态签名。这一步在联机处理过程中执行。如果验证失败，交易拒绝。

9.5 前期相关处理

读应用数据

终端从卡片中读数据。如果卡片支持SDA，数据中包括发卡行公钥证书，其它和密钥相关的数据和签名的静态应用数据（SAD）。如果卡片支持DDA，那数据中也要有DDOL，IC卡公钥证书和其它和密钥相关数据。

9.6 后续相关处理

终端行为分析

终端使用SDA或DDA的结果和卡片与终端的参数决定交易是拒绝、上送联机或接受脱机交易。

卡片行为分析

如果交易符合CDA执行要求，卡片在响应终端之前，将ARQC或TC放到签名的动态应用数据中用IC卡私钥签名。

如果动态数据认证失败指示位是“1”，卡片设置CVR中上次交易动态数据认证失败，交易拒绝位为“1”。如果静态数据认证失败指示位是“1”，卡片设置CVR中一个类似的位。

如果当前交易拒绝而且终端送来的TVR中的动态数据认证失败指示位为“1”，卡片设置卡片中动态数据认证失败指示位为“1”。SDA也有类似处理。

联机操作

如果执行了CDA而且卡片返回的应用密文是ARQC或TC，终端在卡片响应生成应用密文命令后恢复并验证签名数据。

结束

当交易联机处理而且发卡行认证：

——执行并通过；

——支持但可选并且没有执行，或；

——不支持。

卡片中静态数据认证失败和动态数据认证失败指示位设为“0”。

如果交易拒绝而且终端送入的TVR中“CDA失败”位为“1”，卡片设置动态数据认证失败指示器为“1”。

10 处理限制

终端使用终端和卡片数据执行处理限制功能。包括检查应用版本、生效和失效日期等。

10.1 卡片数据

在处理限制过程中使用的卡片数据在表17中列出。

表17 处理限制——卡片数据

数据元	描述
应用生效日期	应用可以有效使用的开始日期
应用失效日期	应用使用的截止日期
应用版本号	此数据元（卡片标签“9F08”）表明卡片中应用的版本。在终端执行应用版本检查时使用
应用用途控制（AUC）	可选数据元。指明发卡行设置的卡片应用限制，包括国内、国际、交易种类、使用的终端设备等
发卡行国家代码	JR/T 0025 定义数据（5F28）指明卡片发行者的国家。在终端执行应用用途控制检查时使用

10.2 终端数据

在处理限制过程中使用的终端数据在表18中列出。

表18 处理限制——终端数据

数据元	描述
应用版本号	终端标签“9F09”表明终端中应用的版本号
交易类型	此数据元表明应用类型。在终端执行应用用途控制检查时使用
终端国家代码	此数据元表明终端所处国家。在终端执行应用用途控制检查时使用
交易日期	交易发生时的终端当地日期。在终端执行生效和失效日期检查时使用

10.3 处理流程

在处理限制过程中卡片不执行任何操作。下面描述了终端在处理限制过程中如何使用卡片数据。

10.3.1 应用版本号检查

终端比较卡片和终端中的应用版本号是否一样。

10.3.2 应用用途控制检查

在应用用途控制处理中，终端检查交易发生地的不同情况，决定交易是否继续进行。如果在读应用数据步骤中终端读取到应用用途控制（AUC）和发卡行国家代码数据，终端检查下列应用限制：

步骤 1：国内和国际检查

国内

终端比较发卡行国家代码和终端国家代码。如果相同，认为是国内交易。如果是国内交易，AUC中对应的国内交易类型指示位应为“1”表明请求的服务允许进行。

示例：如果是一个现金交易，AUC 中“国内现金交易有效”指示位应为“1”。

国际

如果国家代码不同，认为是国际交易。如果是国际交易，AUC中对应的国际交易类型指示位应为“1”表明请求的服务允许进行。

示例：如果是一个现金交易，AUC 中“国际现金交易有效”指示位应为“1”。

步骤 2：ATM 检查

如果终端设备为ATM，AUC中ATM有效位应为“1”。如果终端设备不是ATM，AUC中“除ATM外的终端有效”位应为“1”。

如果上述任何终端执行的检查失败，终端在TVR中标明“卡片产品不允许请求的服务”。

表19是AUC的编码格式，如果指示位的值为“1”说明支持此用途。

表19　应用用途控制（AUC）

字节	b8	b7	b6	b5	b4	b3	b2	b1	用途
1	1	x	x	x	x	x	x	x	国内现金交易有效
1	x	1	x	x	x	x	x	x	国际现金交易有效
1	x	x	1	x	x	x	x	x	国内商品有效
1	x	x	x	1	x	x	x	x	国际商品有效
1	x	x	x	x	1	x	x	x	国内服务有效
1	x	x	x	x	x	1	x	x	国际服务有效
1	x	x	x	x	x	x	1	x	ATM 有效
1	x	x	x	x	x	x	x	1	除 ATM 外的终端有效
2	1	x	x	x	x	x	x	x	允许国内返现
2	x	1	x	x	x	x	x	x	允许国际返现

10.3.3　应用生效日期检查

当卡片应用数据中包括应用生效日期时，终端执行应用生效日期检查。检查确保应用是有效的。如果应用生效日期大于交易日期，终端要在TVR中标明应用还未生效。

10.3.4　应用失效日期检查

应用失效日期检查是必备的。检查确保应用没有过期。如果应用失效日期小于交易日期，终端要在TVR中标明应用已经过期。

10.4　前期相关处理

读应用数据

终端使用读记录（READ RECORD）命令取得卡片中记录数据。这些数据包括发卡行国家代码，应用版本号，应用失效日期和可选的AUC和应用生效日期。

10.5　后续相关处理

终端行为分析

在终端行为分析阶段，终端检查发卡行行为代码（IAC）和终端行为代码（TAC）决定交易结果。

11　持卡人验证

持卡人验证用于确保持卡人身份合法以及卡片没有丢失。

在持卡人验证处理中，终端决定要使用的持卡人验证方法（CVM）并执行选定的持卡人验证。CVM处理允许增加其它持卡人验证方法，例如生物识别等。如果使用脱机PIN方式，卡片要验证卡片内部的脱机PIN。脱机PIN验证结果包括在联机授权信息中，发卡行作授权决定的时候要考虑其验证结果。

终端使用卡片中的CVM列表规则选择持卡人验证方式。选择原则包括交易类型（现金或消费），交易金额，终端能力等。CVM列表还给终端指明如果持卡人验证失败要如何处理。

11.1　卡片数据

表20描述了CVM列表处理过程中终端使用的卡片数据。

表20　CVM 列表处理——卡片数据

数据元	描述
应用货币代码	用来决定交易是否使用卡片中的指定货币。如果 CVM 列表存在而且 CVM 列表中金额 X 或金额 Y 不为零，卡片中应用货币代码数据要存在

应用交互特征（AIP）	标明卡片是否支持持卡人验证
持卡人验证方法列表（CVM List）	一个有优先顺序的持卡人验证方式列表。一张卡包括一个 CVM 列表，如果要实现不同的应用类型例如国内或国际使用不同的验证方式，卡片中要有多个 CVM 列表。一个 CVM 列表包括下列内容： ● 金额 X ● 金额 Y ● CVM 入口——CVM 列表可以包括多个入口，每个入口包括下列子集： **子集　　描述** CVM 代码　指出如果这个 CVM 失败，是执行下一 CVM 还是认为 CVM 失败 CVM 类型　CVM 的类型有： ● 脱机明文 PIN 验证 ● 联机加密 PIN 验证 ● 脱机明文 PIN 验证加签名 ● 签名 ● 无需 CVM（认为 CVM 通过） ● CVM 处理失败（认为 CVM 失败） ● 出示证件 CVM 条件　此 CVM 的使用条件，包括： ● 总是执行 ● 如果是现金或返现交易 ● 如果不是现金或返现交易 ● 如果终端支持此 CVM ● 如果交易金额小于金额 X ● 如果交易金额大于金额 X ● 如果交易金额小于金额 Y ● 如果交易金额大于金额 Y 注： 后四个条件要求交易使用的是卡片指定货币（卡片应用货币）

下面是一个发卡行如何定义CVM的例子：

例子

CVM列表

一个发卡行以下列方式验证持卡人：

——所有 ATM 交易和返现交易使用联机 PIN；

——如果终端支持脱机 PIN，所有 POS 交易使用脱机 PIN；

——如果终端不支持脱机 PIN，POS 交易使用签名；

——如果终端不支持脱机 PIN 或签名，不需要签名。

CVM列表内容见表21。

表21　CVM 列表例子

入口	值/含义	注释
金额 X	0	CVM 列表中不检查金额
金额 Y	0	CVM 列表中不检查金额
CVM 入口 1		ATM 交易使用此 CVM 入口
CVM 条件	01-如果现金或返现	
CVM 类型	000010b-联机加密 PIN 验证	

入口	值/含义	注释
CVM 代码	1b-如果失败持卡人验证失败	
CVM 入口 2		POS 交易使用此入口 如果终端支持脱机明文 PIN 核对，执行此 CVM
CVM 条件	03-如果终端支持	
CVM 类型	000001b-脱机明文 PIN 验证	
CVM 代码	1b-如果失败持卡人验证失败	
CVM 入口 3		如果终端不支持脱机明文 PIN 核对，执行此入口 如果终端支持收集签名，执行此 CVM
CVM 条件	03-如果终端支持	
CVM 类型	011110b-签名	
CVM 代码	0b-如果失败执行下一个 CVM	
CVM 入口 4		如果终端不支持脱机明文 PIN 核对和签名，执行此入口 CVM 不可能失败
CVM 条件	00-总是	
CVM 类型	011111b-无需 CVM	
CVM 代码	1b-如果失败持卡人验证失败	

卡片使用的卡片数据在表22中描述。

表22　脱机 PIN 处理——卡片数据

PIN 尝试限制数	发卡行指定的 PIN 连续错误的最大次数
PIN 尝试计数器	指明 PIN 的剩余尝试次数。卡片使用取数据（GET DATA）命令返回 PIN 尝试计数器（可选）。在验证命令中返回给终端 当 PIN 验证不成功，计数器减一，直到验证成功或发重置计数器的脚本命令，计数器复位成最大尝试次数。当卡片支持脱机 PIN 验证时，此计数器应存在卡片中。这一数据不一定可读。当发卡行希望终端在持卡人最后一次输入 PIN 前获得提示信息，此数据应可以由取数据（GET DATA）命令读出。否则此数据不应由终端通过取数据（GET DATA）命令读取
脱机 PIN	卡片脱机 PIN 被安全的保存在卡片中
卡片验证结果（CVR）	包括下列内容的指示位： ● 脱机 PIN 认证已执行 ● 脱机 PIN 认证失败 ● 超过 PIN 尝试次数 ● 因为超过 PIN 尝试次数应用锁定
持卡人证件号	用于证件验证
持卡人证件类型	用于标识证件类型

11.2　终端数据

表23列出了终端使用的数据。

表23　PIN 处理——终端数据

数据元	描述
交易 PIN	持卡人输入的 PIN

11.3　命令

脱机PIN处理中使用下列命令：

——取数据（GET DATA）—终端用来从卡片中取得 PIN 尝试计数器的值，可选。

如果卡片不支持用取数据（GET DATA）命令返回PIN尝试计数器，卡片返回“6A88”；

——验证（VERIFY）——用于脱机明文 PIN 校验。

如果卡片支持脱机PIN处理就要支持验证（VERIFY）命令；

命令的响应状态字SW1 SW2可能有如下返回值：

- “9000”验证成功；
- “63Cx”PIN 不匹配，“x”表明剩余的次数；
- “6984”当在上次交易中尝试次数限制数已经超过，本次交易第 1 次处理验证（VERIFY）命令时返回；
- “6983”当在本次交易中尝试次数限制数超过，卡片再次收到验证（VERIFY）命令时返回。

11.4 处理流程

下面描述了在处理CVM列表中不同CVM时的卡片规则。

11.4.1 CVM 列表处理

除了在读应用数据处理过程中提供给终端CVM列表外，卡片不作操作。

11.4.2 脱机明文 PIN 处理

当一个PIN传送给卡片后，卡片的处理：

步骤 1：检查 PIN 尝试计数器

在终端决定要输入一个脱机PIN以后，终端可以发送一个取数据（GET DATA）命令获取PIN尝试计数器值。

a) 如果卡片支持使用取数据命令返回 PIN 尝试计数器，卡片：

——如果 PIN 尝试计数器为“0”，设置 CVR 中“PIN 尝试限制数超过”位为“1”；

——在取数据（GET DATA）命令的响应信息中返回 PIN 尝试计数器。如果为“0”，终端不再允许持卡人输入 PIN。

b) 如果卡片不支持使用取数据（GET DATA）命令返回 PIN 尝试计数器，卡片要返回“6A88”。

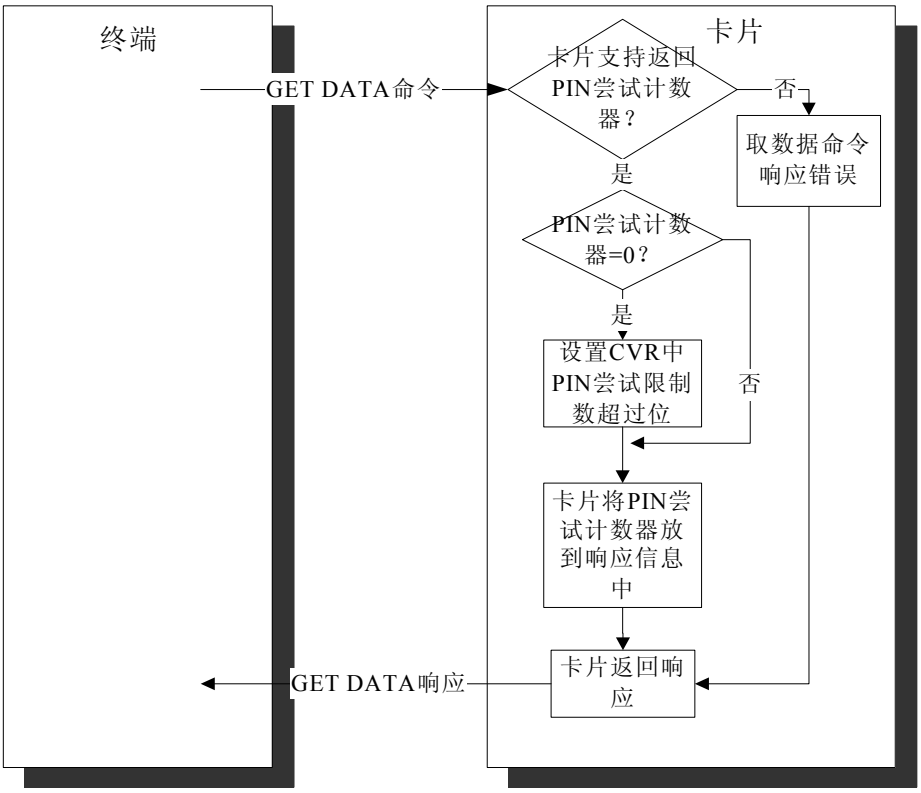


图6 检查 PIN 尝试计数器

步骤 2：接收验证（VERIFY）命令

持卡人输入交易PIN以后，终端发送一个包含此被输入的交易PIN的验证（VERIFY）命令。当卡片收到验证（VERIFY）命令，卡片要设置CVR中“脱机PIN验证执行”位为“1”。

步骤 3：PIN 验证

卡片执行下列PIN验证步骤：

a) PIN 尝试限制数已经超过，卡片应该采取以下措施：

——设置 CVR 中“PIN 尝试限制数超过”位为“1”；

——设置 CVR 中“脱机 PIN 验证失败”位为“1”；

——如果 PIN 尝试限制数是在上次交易中超过的，返回 SW1 SW2=“6984”；

——如果 PIN 尝试限制数是在本次交易中超过的，返回 SW1 SW2=“6983”。

b) PIN 匹配

如果PIN尝试功能没有锁定，卡片进行PIN验证。如果匹配，卡片：

——将 PIN 尝试计数器设置为最大值（PIN 尝试限制数）；

——设置 CVR 中“脱机 PIN 验证失败”位为“0”；

——验证（VERIFY）命令响应“9000”。

c) PIN 不匹配

如果交易PIN和卡片内脱机PIN不匹配，卡片：

——PIN 尝试计数器减 1；

——设置 CVR 中“脱机 PIN 验证失败”位为“1”。

卡片判断PIN尝试限制数是否超过

——没有 PIN 尝试机会；

如果PIN尝试计数器为“0”，卡片：

- 设置 CVR 中“PIN 尝试限制数超过”位为“1”；
- 如果有应用缺省行为（ADA）数据，而且 ADA 中“PIN 尝试限制数在本次交易中超过，应用锁定”位为“1”，设置 CVR 中“因为 PIN 尝试次数超过卡片锁应用”位为“1”并且锁应用。卡片将允许当前交易执行到结束步骤。这里描述的应用锁定不会使应用或卡片永久无效；
- 验证（VERIFY）命令响应“63C0”。

——还有尝试机会

如果PIN尝试计数器不为零，卡片响应验证（VERIFY）命令“63Cx”，x表示剩余的尝试次数。

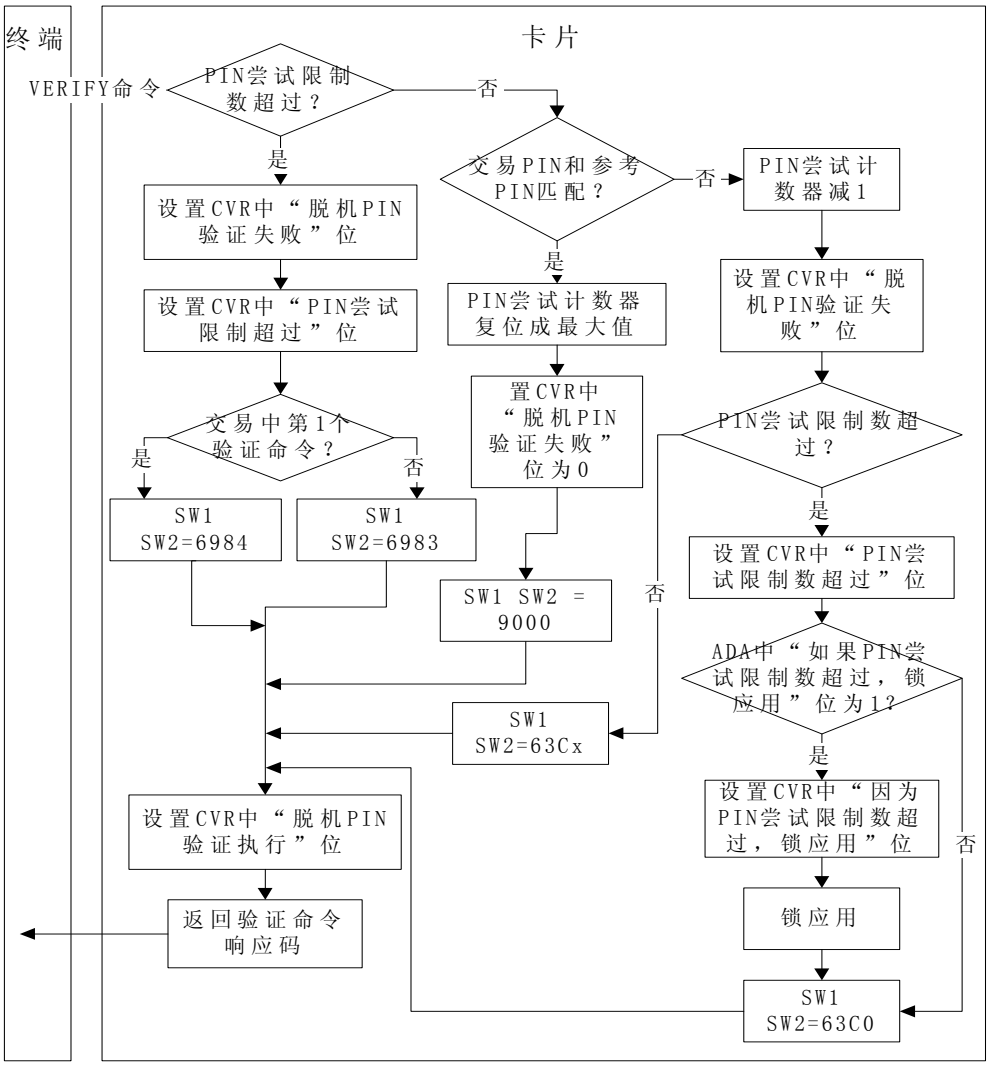


图7　脱机明文 PIN 处理

步骤 4：下一步处理

如果PIN核对失败而且PIN还有尝试次数，终端会提示持卡人再次输入交易PIN，并发送另一个验证（VERIFY）命令。

如果在PIN尝试次数减为零之前PIN验证成功，卡片：

a)　PIN 尝试计数器重置为最大值（PIN 尝试限制数）；

b)　设置 CVR 中“脱机 PIN 验证失败”位为“0”。

持卡人可以连续输入错误的PIN，直到尝试计数器为零。此时，终端不再给卡片发送验证（VERIFY）命令。

11.4.3　其它 CVM 处理

联机PIN或签名的持卡人验证处理过程中，卡片不执行操作。

11.5　前期相关处理

应用初始化

在获取处理选项（GPO）命令响应中返回的应用交互特征（AIP）中指明卡片是否支持持卡人验证。

读应用数据

终端读出持卡认证件号、持卡人证件类型、CVM列表和其它处理CVM列表需要的卡片数据。

11.6　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卡片和终端的参数决定交易是否拒绝、联机上送或接受交易。

卡片行为分析

卡片使用ADA中的参数决定当PIN尝试限制数超过是否生成通知。

卡片使用ADA参数决定当PIN尝试限制数在以前的交易中超过，交易是否拒绝或联机上送。

联机操作

CVM结果包括脱机PIN的验证结果，此数据包括在授权请求中，发卡行在作出授权决定的时候要考虑脱机PIN的验证结果。

如果CVM是联机PIN，联机请求中有加密的联机PIN。如果CVM是脱机PIN，联机授权请求中不包括此PIN值。

结束

如果终端尝试为一笔PIN尝试限制数超过的交易进行联机授权，而且尝试失败，卡片使用ADA参数决定交易是否拒绝或接受。

发卡行脚本操作

PIN修改/解锁命令用来重置PIN尝试计数器为最大值（PIN尝试限制数），也用来修改卡片中的脱机PIN值。

应用解锁命令可以用来解锁CVM处理过程中锁掉的应用。

12 终端风险管理

终端风险管理为大额交易提供了发卡行授权，确保芯片交易可以周期性的进行联机处理，防止过度欠款和在脱机环境中不易察觉的攻击。

发卡行需要支持终端风险管理。无论卡片是否支持，终端都需要支持终端风险管理。

12.1 卡片数据

终端在终端风险管理处理中使用的卡片数据在表24中列出。

表24 终端风险管理——卡片数据

数据元	描述
应用主账号（PAN）	此应用中的持卡人账号
应用交易计数器（ATC）	当卡片中建立应用时被初始化，由应用维护
上次联机应用交易计数器（ATC）寄存器	上次联机授权成功时的ATC值 如果卡片必备要求发卡行认证，在结束处理阶段，当发卡行认证执行并通过，设置寄存器的值 用于终端风险管理和新卡检查
连续脱机交易下限“9F14”	发卡行指定的，有联机能力的终端允许交易连续脱机的最大次数。终端频度检查中和终端新卡检查时使用
连续脱机交易上限“9F23”	发卡行指定的，终端允许交易连续脱机的限制数，如果联机授权没有执行，交易拒绝。终端频度检查中和终端新卡检查时使用

12.2 终端数据

终端风险管理中使用的终端数据在表25中列出。

表25 终端风险管理——终端数据

数据元	描述
授权金额	数字数据对象（标签“9F02”）存放当前交易的金额。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的数据
用于随机选择的目标百分数	用于随机选择交易联机的数据

终端最低限额	标明应用的终端最低限额。用于最低限额检查和交易随机选择联机处理
终端验证结果（TVR）	一组指示位，用来记录所有终端风险管理的处理结果
偏置随机选择的阈值	用于随机选择交易联机的数据
交易日志	终端上存储的被接受的交易的交易日志，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可能使用到这个日志
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标明终端风险管理已被执行

12.3 命令

取数据（GET DATA）命令

如果终端尚未获取上次联机ATC寄存器和应用交易计数器，则发送取数据（GET DATA）命令从卡片中读取。这些数据在终端频度检查和新卡检查时使用。

如果卡片支持终端频度检查或新卡检查，卡片要返回这些数据给终端。

如果卡片不支持终端频度检查或新卡检查，这些数据要存储为JR/T 0025专用数据元并不能返回给终端。此时卡片响应SW1 SW2=“6A88”。

有关取数据（GET DATA）命令，见附录B。

12.4 处理流程

在终端频度检查和新卡检查中，除了响应取数据命令，卡片不做操作。

下面描述了终端在终端风险管理处理过程中如何使用卡片数据。

12.4.1 终端异常文件检查

如果有终端异常文件，终端要检查卡片中的应用主账号（PAN）是否在其中。

12.4.2 商户强制交易联机

在有联机能力的终端上，商户可以指示终端进行联机交易。在此步骤中不需要卡片数据。

12.4.3 最低限额检查

进行最低限额检查，当交易金额超过终端最低限额，交易联机上送。此步骤中不需要卡片数据。

12.4.4 随机交易选择

有脱机和联机能力的终端要执行随机选择交易联机处理。此步骤不需要卡片数据。

12.4.5 频度检查

在连续脱机次数达到一个特定的次数后，频度检查允许发卡行请求交易联机处理。发卡行可以选择不支持终端频度检查，则在个人化时，连续脱机交易的上限和下限（标签“9F14”和标签“9F23”）数据不写入卡中。

在频度检查处理中，终端发送取数据（GET DATA）命令读取卡片中的上次联机ATC寄存器和ATC值。

卡片返回数据。

连续脱机交易的次数是ATC和上次联机ATC寄存器的差值。

注： 卡片在卡片行为分析处理时可以执行类似的处理。

12.4.6 新卡检查

如果终端执行新卡检查，终端检查上次联机ATC寄存器值是否为零（如果存在）。

终端发取数据（GET DATA）命令给卡片读出上次联机ATC寄存器值。

注： 卡片在卡片行为分析处理时可以执行类似的处理。

12.5 前期相关处理

读应用数据

下列数据从卡片中读出：

——应用主账号，用于终端异常文件检查；

——连续脱机交易上限/下限，用于终端频度检查（可选）。

12.6 后续相关处理

终端行为分析

根据卡片和终端的设置，如果出现下列情况，终端作出处理决定：

——卡片在终端异常文件中；

——商户强制交易联机；

——超过最低限额；

——交易被随机选择联机；

——频度检查中金额或计数器超过限制数；

——卡片是新卡。

13 终端行为分析

在终端行为分析过程中，终端对脱机处理结果使用发卡行在卡片中设置的规则和支付系统在终端中设置的规则来决定交易是接受、拒绝还是上送联机授权。终端行为分析包括下面两个步骤：

步骤 1：检查脱机处理结果——终端通过检查脱机处理结果，决定交易是联机上送、接受脱机或拒绝。这个处理过程中要考虑发卡行在卡片中定义的发卡行行为代码（IAC）以及终端中定义的终端行为代码（TAC）。

步骤 2：请求密文——终端请求卡片生成密文。

终端行为分析过程中做出的交易联机或接受并不是一个最终的结果。卡片进行卡片行为分析处理时，卡片可能会推翻终端的决定。但是卡片不能推翻终端做出的交易拒绝的决定。

13.1 卡片数据

在终端行为分析处理过程中，终端使用的卡片数据在表26中列出。

表26 终端行为分析——卡片数据

数据元	描述
卡片行为代码（IAC）	IAC 是三个数据元，每个数据元都和终端验证结果（TVR）中的每一位对应。这三个卡片行为代码是： IAC-拒绝 和对应的 TVR 中的条件如果满足，则交易拒绝 IAC-联机 和对应的 TVR 中的条件如果满足，则交易联机 IAC-缺省 当交易申请联机但无法执行时，对应的 TVR 中的条件如果满足，则交易拒绝

IAC数据建议作为静态脱机数据认证用数据。

表27列出的数据是终端在之前的步骤中得到，在请求密文时使用的。

表27 请求密文处理——卡片数据

数据元	描述
卡片风险管理数据对象列表 CDOL1	列出卡片在生成应用密文时需要终端提供的数据的标签和长度
交易证书数据对象列表 TDOL	列出生成交易证书（TC）哈希计算的数据对象（标签和长度）

13.2 终端数据

在终端行为分析处理过程中，终端使用的终端数据在表28中列出。

表28　检查脱机处理结果——终端数据

数据元	描述
终端行为代码（TAC）	TAC 有 3 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 收单行设置能够导致脱机拒绝的 TVR 条件位 ● TAC-联机 收单行设置能够导致交易联机的 TVR 条件位 ● TAC-缺省 收单行设置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

终端在请求应用密文时使用的终端数据元在表29中列出。

表29　请求密文处理——终端数据

数据元	描述
终端数据元	在 CDOL1 或 TDOL 中指定的终端数据，在生成应用密文（GENERATE AC）命令中使用
交易证书（TC）哈希结果	可选。作为输入数据使用生成应用密文（GENERATE AC）命令送入卡片

13.3　命令

生成应用密文（GENERATE AC）命令

终端使用生成应用密文（GENERATE AC）命令请求卡片生成一个应用密文。

命令中的P1参数标明了密文类型以及是否执行CDA。命令的数据部分包括卡片在CDOL1中要求的终端数据元。CDOL1是终端在读应用记录处理过程中从卡片中读出的。

卡片处理生成应用密文（GENERATE AC）命令并响应。

具体的命令编码见附录B。

13.4　处理流程

13.4.1　检查脱机处理结果

终端行为分析中检查脱机处理结果步骤是完全由终端执行的，终端使用卡片中的IAC和终端中的TAC。

卡片在此步骤中没有操作。

13.4.2　请求密文处理

在请求密文处理过程中，终端发送一个生成应用密文（GENERATE AC）命令给卡片请求卡片生成一个应用密文。命令中包含CDOL1中指定的终端数据元。

当卡片收到命令后，卡片进行卡片行为分析处理，见第14章。

13.5　前期相关处理

读应用数据

在读应用数据处理中，卡片返回应用数据记录给终端，这些数据包括IAC，CDOL1等。

13.6　后续相关处理

卡片行为分析

在卡片行为分析阶段，卡片执行风险管理确定是否同意终端作出的交易拒绝、交易接受或联机上送的决定。

14　卡片行为分析

卡片行为分析允许发卡行设置在卡片内部执行频度检查和其它风险管理。本部分描述JR/T 0025自定义的卡片风险管理，包括的检查有：

——上次交易行为；

——卡片是否新卡；

——脱机交易计数和累计脱机金额。

卡片行为分析结束后，卡片返回一个应用密文给终端。AAC表示交易拒绝，ARQC表示请求联机授权，TC表示脱机交易接受。如果卡片和终端都支持CDA，卡片返回的ARQC或TC要作为签名的动态应用数据的一部分。

14.1 卡片数据

表30列出了在卡片行为分析处理过程中使用的卡片数据。

表30 卡片行为分析——卡片数据

数据元	描述
应用密文	生成应用密文（GENERATE AC）命令的响应信息。 ● AAC 表示交易拒绝 ● TC 表示接受交易 ● ARQC 表示请求联机授权
应用货币代码	指明和应用有关的国内货币，是卡片指定货币
应用缺省行为（ADA）	发卡行定义的指示器，指定在一些特殊条件下的卡片行为。如果卡片中没有则缺省认为为零
应用交互特征（AIP）	包括表明卡片支持 CDA 和发卡行认证能力的指示器
卡片风险管理数据对象列表 1（CDOL1）	列出在第 1 个生成应用密文（GENERATE AC）命令中，卡片要求终端传送的数据对象（标签和长度）。下列在 CDOL1 中的数据用于卡片风险管理检查： ● 交易货币代码——连续国际脱机交易次数频度检查（基于货币），本地货币累计脱机交易金额频度检查，本地货币加第 2 货币累计脱机交易金额频度检查 ● 终端国家代码——连续国际脱机交易次数频度检查（基于国家） ● 授权金额——本地货币累计脱机交易金额频度检查，本地货币加第 2 货币累计脱机交易金额频度检查 ● 终端验证结果（TVR）——包括 SDA 和 DDA 是否失败的指示位 CDOL1 中包含的数据不能重复
卡片验证结果（CVR）	JR/T 0025 专有数据。表明当前和上次交易的脱机处理结果。此数据作为发卡行应用数据的一部分联机上送
密文信息数据（CID）	在生成应用密文（GENERATE AC）命令中返回给终端，CID 指出了卡片返回的密文的类型。CID 还包括了是否要生成通知的标识位，以及生成通知的原因的代码
连续脱机交易计数器（国际-货币）	JR/T 0025 专有数据。每次使用非卡片指定货币的脱机交易，计数器加 1
连续脱机交易限制次数（国际-货币）	JR/T 0025 专有数据。使用卡片非指定货币的脱机交易的限制次数，超过则请求联机处理
连续脱机交易计数器（国际-国家）	JR/T 0025 专有数据。每次发卡行国家代码和终端国家代码不同的脱机交易，计数器加 1
连续脱机交易限制次数（国际-国家）	JR/T 0025 专有数据。发卡行国家代码和终端国家代码不同的脱机交易的限制次数，超过请求联机处理
累计脱机交易金额	JR/T 0025 专有数据。记录自从上次联机处理以来，使用卡片指定货币的脱机交易总金额
累计脱机交易金额限制	JR/T 0025 专有数据。累计脱机交易金额的限制数。如果超过请求联机处理
累计脱机交易金额（双货币）	JR/T 0025 专有数据。记录自从上次联机处理以来，使用卡片指定货币和第 2 货

数据元	描述
	币的脱机交易总金额
累计脱机交易金额限额（双货币）	JR/T 0025 专有数据。累计脱机交易金额（双货币）的限制数。如果超过请求联机处理
货币转换因子	用来将第 2 应用货币转换成应用指定货币的汇率值。此数据元有四个字节，第 1 个高半字节表示小数点的位置，后面 7 个半字节表示汇率值
DDA 失败指示位	当上次交易 DDA 失败而且交易拒绝时设置的卡片内部应用指示位
发卡行认证失败指示位	当上次联机交易出现下面两种情况之一时设置的卡片内部应用指示位： ● 发卡行认证执行并失败 ● 发卡行认证必备但没执行
发卡行认证指示位	指明卡片支持的发卡行认证是必备还是可选的指示位
发卡行国家代码（“9F57”）	JR/T 0025 专有数据。表明发卡行的国家
发卡行脚本命令计数器	记录上次联机交易中，有安全报文的发卡行脚本命令的个数
发卡行脚本失败指示位	在上次联机交易中，发卡行脚本处理失败时设置
连续脱机交易下限（“9F58”）	JR/T 0025 专有数据。在申请联机授权之前，卡片允许的最大连续脱机交易限制数
卡片请求脱机拒绝指示位	当卡片风险管理检查决定交易拒绝时设置的卡片内部应用指示位
联机授权指示位	当申请联机的交易无法联机或联机授权被中止时设置的内部应用指示位
卡片请求联机指示位	当卡片风险管理检查决定交易要联机上送时设置的卡片内部应用指示位
PIN 尝试计数器	记录 PIN 剩余的尝试次数
第 2 应用货币代码	用于双货币频度检查。可以使用货币转换因子转换为本地货币（卡片指定货币）
SDA 失败指示位	当上次交易 SDA 失败而且交易拒绝时设置的卡片内部应用指示位
交易明细文件短文件标识符	当卡片作出接受交易的决定后，卡片内部自动记录交易明细，交易明细文件的短文件标识符标识此文件

14.2 终端数据

表31列出在卡片风险管理处理中使用的终端数据。

表31 卡片行为分析——终端数据

数据元	描述
授权金额	交易的金额
交易货币代码	表明交易的货币类型，在 CDOL1 中
终端国家代码	表明终端的国家，在 CDOL1 中
终端验证结果（TVR）	终端记录脱机处理结果的一系列指示位

14.3 命令

生成应用密文（GENERATE AC）命令

终端使用生成应用密文（GENERATE AC）命令请求卡片提供一个应用密文。

命令中的P1参数表明了密文类型以及是否执行CDA。命令的数据部分包括CDOL1中指定的终端数据。

命令的响应信息包括应用密文和密文信息数据。如果卡片执行CDA，而且密文类型为ARQC或TC，密文要作为签名的动态应用数据使用IC卡私钥签名。具体描述在JR/T 0025.7中。

14.4 处理流程

14.4.1 卡片收到密文请求

卡片收到终端发来的生成应用密文（GENERATE AC）命令。命令的数据部分包括CDOL1中卡片指定的终端数据。

表32列出了CDOL1中支持卡片风险管理需要的数据。

14.4.2 卡片风险管理

表32总结了所有卡片风险管理检查，并标明这些检查是否必备或可选，同时描述了检查的结果。

如果发卡行选择执行任意一个可选的卡片风险管理检查,发卡行需要确保执行检查的数据在卡片个人化时被写入卡中，同时确保在CDOL1中列出了需要的终端数据的标签和长度。

如果指定的终端数据无效（即在生成应用密文（GENERATE AC）命令中，数据部分用零占位）卡片将跳过去处理下一个卡片风险管理检查。如果卡片中没有应用缺省行为（ADA），卡片认为该值缺省全零。

表32 卡片风险管理检查

风险管理检查	执行条件	结果（如果条件满足）
联机授权没有完成（上次交易）	有条件——如果支持发卡行脚本命令或发卡行认证则执行	请求联机处理，设置 CVR 指示位
上次交易发卡行认证失败(或上次交易发卡行认证必备但是没有执行)	有条件——如果支持发卡行认证则执行	设置 CVR 指示位 检查 ADA 如果指明则请求联机处理
上次交易 SDA 失败	有条件——如果支持 SDA 则执行	设置 CVR 指示位
上次交易 DDA 失败	有条件——如果支持 DDA 则执行	设置 CVR 指示位
上次联机交易发卡行脚本处理	有条件——如果支持二次发卡（post-issuance）则执行	在 CVR 中保存脚本命令的个数 如果脚本处理失败(使用卡片内的发卡行脚本失败指示位),设置 CVR 指示位。 ADA 中的设置决定交易是否联机处理
连续脱机交易下限频度检查	可选	如果限制数超过，请求联机处理 设置 CVR 中指示位
连续国际脱机交易(基于货币)频度检查	可选	如果限制数超过，请求联机处理 设置 CVR 中指示位
连续国际脱机交易(基于国家)频度检查	可选	如果限制数超过，请求联机处理 设置 CVR 中指示位
使用指定货币的累计脱机交易金额频度检查	可选	如果限制数超过，请求联机处理 设置 CVR 中指示位
累计脱机交易金额(双货币)频度检查	可选	如果限制数超过，请求联机处理 设置 CVR 中指示位 如果使用的货币是第 2 货币,需要先进行货币转换
新卡检查	可选	如果以前没有请求过联机本次可以申请联机 设置 CVR 中指示位
脱机 PIN 验证没有执行(PIN 尝试限制数超过)	可选	设置CVR中如果本次交易脱机PIN验证没有执行而且 PIN 尝试限制数在之前已经超过指示位 ADA 中设置这种情况下交易拒绝或请求联机

14.4.3 卡片风险管理流程

卡片执行每一个卡片风险管理检查确定预设的情况是否发生,看是否有情况满足,然后执行下一个。如果有检查不被支持，卡片继续执行下一个检查。

14.4.3.1 联机授权没有完成检查

如果支持发卡行认证或发卡行脚本命令，需要执行此检查。检查在上次交易中，在卡片请求一个联机授权之后，在终端接收到联机响应进行处理之前或无法联机的终端处理之前，卡片是否离开了终端设备。卡片中的联机授权指示位在上次交易请求联机授权的时候置“1”。

如果指示位设置了，卡片将请求联机处理，直到交易联机并且下面中的一个条件满足：

——发卡行认证成功；

——发卡行认证可选并且没执行；

——不支持发卡行认证。

注： 这些指示位在结束阶段根据发卡行认证的状态和卡片参数被重新设置。

如果联机授权指示位设为“1”，卡片：

——设置卡片请求联机指示位置“1”；

——设置 CVR 中“上次联机交易没完成”位为“1”。

14.4.3.2 上次交易发卡行认证失败（或必备未执行）检查

如果卡片AIP中表明支持发卡行认证，则应执行此检查。如果上次交易发卡行认证（1）失败或（2）必备（发卡行认证指示位表示）但是没有执行，卡片请求联机处理。

如果发卡行认证失败指示位设为“1”，卡片：

——设置 CVR 中“上次联机交易发卡行认证失败”位为“1”；

——如果应用缺省行为（ADA）中“发卡行认证失败，下次交易联机上送”位为“1”，设置卡片请求联机指示位置“1”。

14.4.3.3 上次交易静态数据认证（SDA）失败检查

如果支持SDA，此检查必备执行。检查上次脱机拒绝的交易中SDA是否失败。

如果SDA失败指示位为“1”，卡片设置CVR中“上次交易SDA失败而且交易拒绝”位为“1”。

14.4.3.4 上次交易动态数据认证（DDA）失败检查

如果支持DDA，此检查强制执行。检查上次脱机拒绝的交易中DDA是否失败。

如果DDA失败指示位为“1”，卡片设置CVR中“上次交易DDA失败而且交易拒绝”位为“1”。

14.4.3.5 上次联机交易发卡行脚本处理检查

如果支持发卡行脚本处理，此检查强制执行。使用上次联机交易处理的发卡行脚本命令计数器和脚本处理失败指示位数据元。

卡片设置CVR中第4字节的第8-5位为发卡行脚本命令计数器的值。

如果发卡行脚本失败指示位为“1”，卡片设置CVR中“上次交易发卡行脚本处理失败”位为“1”。

如果发卡行脚本失败指示位为“1”，如果ADA中“如果上次交易发卡行脚本失败，交易联机上送”位是“1”，设置卡片请求联机指示位为“1”。

14.4.3.6 连续脱机交易下限频度检查

此检查可选。如果连续脱机交易次数超过此下限，卡片请求联机授权。

如果上次联机ATC寄存器和JR/T 0025专有数据：连续脱机交易下限（标签“9F58”）存在，卡片可以执行此检查。

如果ATC和上次联机ATC寄存器的差值大于连续脱机交易下限，卡片：

——设置 CVR 中“频度检查超过”位为“1”；

——设置卡片请求联机指示位为“1”。在卡片风险管理结束时，卡片返回联机请求。

14.4.3.7 连续国际脱机交易（基于货币）限制数频度检查

此检查可选。如果连续脱机交易计数器（国际-货币）超过连续脱机交易限制数（国际-货币），卡片请求联机授权。此检查定义的国际脱机交易是终端发送的交易货币代码和卡片中的应用货币代码不同的交易。

如果数据应用货币代码、连续脱机交易计数器（国际-货币）、连续脱机交易限制次数（国际-货币）存在，卡片执行此检查。

卡片比较交易货币代码和应用货币代码，如果不等，而且连续脱机交易计数器（国际-货币）加1的值大于连续脱机交易限制次数（国际-货币），卡片：

——设置 CVR 中“频度检查超过”位为“1”；

——设置卡片请求联机指示位为“1”。

14.4.3.8 连续国际脱机交易（基于国家）限制数频度检查

此检查可选。如果连续脱机交易计数器（国际-国家）超过连续脱机交易限制数（国际-国家），卡片请求联机授权。此检查定义的国际脱机交易是终端送进的终端国家代码和卡片中的发卡行国家代码不同的交易。

如果数据发卡行国家代码、连续脱机交易计数器（国际-国家）、连续脱机交易限制次数（国际-国家）存在，卡片执行此检查。

如果下面两个条件都满足：

——终端国家代码和发卡行国家代码不同；

——连续脱机交易计数器（国际-国家）加 1 的值大于连续脱机交易限制次数（国际-国家）。

卡片：

——设置 CVR 中“频度检查超过”位为“1”；

——设置卡片请求联机指示位为“1”。

14.4.3.9 使用指定货币的脱机交易累计金额频度检查

此检查可选。如果使用应用指定货币的累计脱机交易金额超过累计脱机交易金额限制，卡片请求联机授权。

如果数据应用货币代码、累计脱机交易金额、累计脱机交易金额限制存在，卡片执行此检查。

如果下面两个条件都满足：

——交易货币代码等于应用货币代码；

——累计脱机交易金额加本次授权金额大于累计脱机交易金额限制。

卡片：

——设置 CVR 中“频度检查超过”位为“1”；

——设置卡片请求联机指示位为“1”。

14.4.3.10 交易累计金额（双货币）频度检查

此检查可选。如果使用应用指定货币和第2应用货币并接受脱机的累计脱机交易金额超过累计脱机交易金额限制（双货币），卡片请求联机授权。

如果数据应用货币代码、第2应用货币代码、货币转换因子、累计脱机交易金额（双货币）、累计脱机交易金额限制（双货币）存在，卡片执行此检查。

——如果交易货币代码等于应用货币代码，累计脱机交易金额（双货币）加本次授权金额和累计脱机交易金额限制（双货币）进行比较；

——如果交易货币代码等于第 2 应用货币代码，使用货币转换因子将授权金额转换为近似的应用货币代码金额。累计脱机交易金额（双货币）加这个近似的授权金额和累计脱机交易金额限制（双货币）进行比较；

——如果比较的结果是大于了限制数，卡片应该采取以下措施：

- 设置 CVR 中“频度检查超过”位为“1”；
- 设置卡片请求联机指示位为“1”。

14.4.3.11 新卡检查

此检查可选。如果卡片是新卡，交易请求联机。新卡是指从来没有联机接受过的卡片。

如果数据上次联机ATC寄存器、应用缺省行为存在，卡片执行此检查。

如果上次联机ATC寄存器值为零，卡片应该采取以下措施：

——设置 CVR 中“新卡”位为“1”；

——如果 ADA 中“如果新卡，交易联机”位为“1”，设置卡片请求联机指示位为“1”。

注： 如果卡片要求发卡行认证必备执行，除非发卡行认证成功，否则上次联机ATC寄存器值一直为零。

14.4.3.12 脱机 PIN 验证没有执行（PIN 尝试限制数超过）检查

当卡片支持脱机PIN验证，此检查可选。如果PIN尝试限制数在上次交易中就已超过，交易请求联机或拒绝交易。

如果执行此检查，卡片中要有应用缺省行为（ADA）数据。

如果下列所有条件成立：

——卡片支持脱机 PIN 验证；

——卡片没有收到过验证命令；

——PIN 尝试计数器已经为零。

卡片要执行下列操作：

——设置 CVR 中“PIN 尝试限制数超过”位为“1”；

——如果 ADA 中“如果上次交易 PIN 尝试限制数超过，交易拒绝”位为“1”，设置卡片请求拒绝指示位为“1”；

——如果 ADA 中“如果上次交易 PIN 尝试限制数超过，交易联机”位为“1”，设置卡片请求联机指示位为“1”；

——如果 ADA 中“如果上次交易 PIN 尝试限制数超过，交易拒绝并锁应用”位为“1”，拒绝交易并锁应用。

14.5 卡片提供响应密文

根据卡片风险管理的结果，卡片响应生成应用密文（GENERATE AC）命令。卡片的响应可能会修改终端在生成应用密文（GENERATE AC）命令中参数P1指定的密文类型。修改要遵循下列原则：

——卡片可以把终端做出的接受交易决定改为交易联机上送或交易拒绝；

——卡片可以把终端做出的交易联机决定改为交易拒绝。

表33列出了修改原则。

表33 卡片响应第 1 个生成应用密文命令

		卡片响应		
		AAC	ARQC	TC
终端请求	AAC	拒绝	–	–
	ARQC	拒绝	联机上送	–
	TC	拒绝	联机上送	接受

卡片中的卡片请求脱机拒绝指示位为“1”表明卡片决定交易拒绝。卡片中的卡片请求联机指示位为“1”表明卡片决定交易联机上送。

卡片设置CVR中第1个生成应用密文响应TC，AAC或ARQC指示位，卡片还设置CVR中“还没有请求第2个生成应用密文”指示位。

卡片使用终端提供的数据和卡片内部数据生成一个基于对称密钥算法的密文，需要的具体数据和算法在附录D中描述。

14.5.1 卡片脱机拒绝交易

当交易被脱机拒绝，卡片用AAC响应生成应用密文（GENERATE AC）命令，在响应之前，卡片：

步骤 1：检查应用缺省行为（ADA）：

——在 ADA 中“如果交易脱机拒绝，生成通知”位为“1”，设置 CID 中需要通知位为“1”；

——如果 PIN 尝试限制数超过，而且 ADA 中标明需要通知：

- 设置 CID 中“需要通知”位为“1”；

- 如果 CID 中的原因代码不是“服务不允许”，设置为“PIN 尝试限制数超过”。

注： 在CID中，“服务不被允许”原因代码比其它原因代码优先。

步骤 2：检查在生成应用密文（GENERATE AC）命令中提供的数据 TVR

——如果 SDA 失败位为“1”，设置卡片中 SDA 失败指示位为“1”；

——如果 DDA 失败位为“1”或者 CDA 失败位为“1”，设置卡片中 DDA 失败指示位为“1”。

步骤 3：计数器加 1：

——如果终端国家代码和发卡行国家代码不同，连续脱机交易计数器（国际-国家）加 1；

——如果交易货币代码和应用货币代码不同，连续脱机交易计数器（国际-货币）加 1。

14.5.2 卡片请求联机操作

当交易联机上送做授权，卡片用ARQC响应生成应用密文（GENERATE AC）命令。在响应之前，卡片设置卡片内联机授权指示位为“1”。

注： 此时下面的计数器不增加：连续脱机交易计数器（国际-货币），连续脱机交易计数器（国际-国家），累计脱机交易金额，累计脱机交易金额（双货币）。

14.5.3 卡片脱机接受交易

当脱机接受交易，卡片使用TC响应生成应用密文（GENERATE AC）命令。在响应之前，卡片内相关计数器加1：

——如果终端国家代码不等于发卡行国家代码，连续脱机交易计数器（国际-国家）加 1；

——如果交易货币代码等于应用货币代码：

- 累计脱机交易金额累加授权金额；
- 累计脱机交易金额（双货币）累加授权金额。

——如果交易货币代码不等于应用货币代码，连续脱机交易计数器（国际-货币）加 1；

——如果交易货币代码等于第 2 应用货币代码，使用货币转换因子将授权金额转换为指定应用货币的近似授权金额后累加到累计脱机交易金额（双货币）；

——卡片记录交易明细，明细的内容在交易初始化阶段，通过获取处理选项（GPO）命令传送到卡片中。关于卡片交易明细的内容见本部分 18 章。

14.5.4 复合动态数据认证/生成应用密文请求

当终端发送的生成应用密文命令中的 P1 参数中 CDA 位为“1”且卡片 AIP 标明卡片支持 CDA 时，卡片执行 CDA。

卡片：

步骤 1：按照上面的描述执行卡片风险管理，生成应用密文；

步骤 2：如果卡片响应 AAC，没有特殊处理；

步骤 3：如果卡片响应 ARQC 或 TC，卡片响应的应用密文作为签名动态应用数据用 IC 卡私钥签名，步骤如下：

a）设置 CVR 中“DDA 执行”位为“1”。此步骤在步骤 1 生成应用密文之前执行；

b）使用应用密文生成一个动态签名密文，详见 JR/T 0025.7 中的 5.3.6。归纳为下面 4 个步骤：

——按照 JR/T 0025.7 中的 5.3.6 中描述的方法组织数据；

——用上述数据做一个哈希计算；

——将哈希包括到签名的动态应用数据中；

——使用 IC 卡私钥对签名的动态应用数据作签名。

c）在生成应用密文（GENERATE AC）命令响应中包括签名的动态应用数据。

14.6 流程图

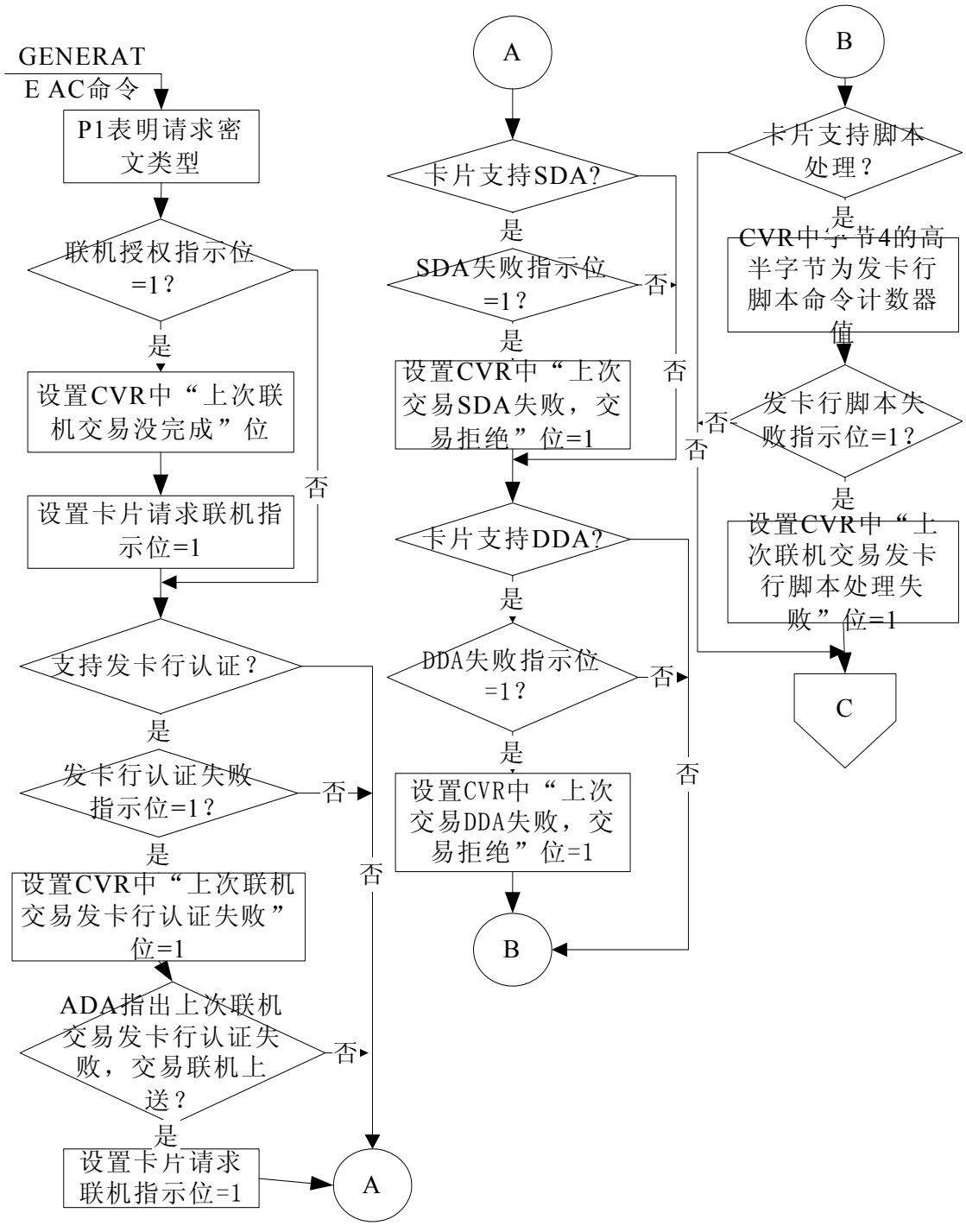


图8 卡片行为分析处理流程图（1）

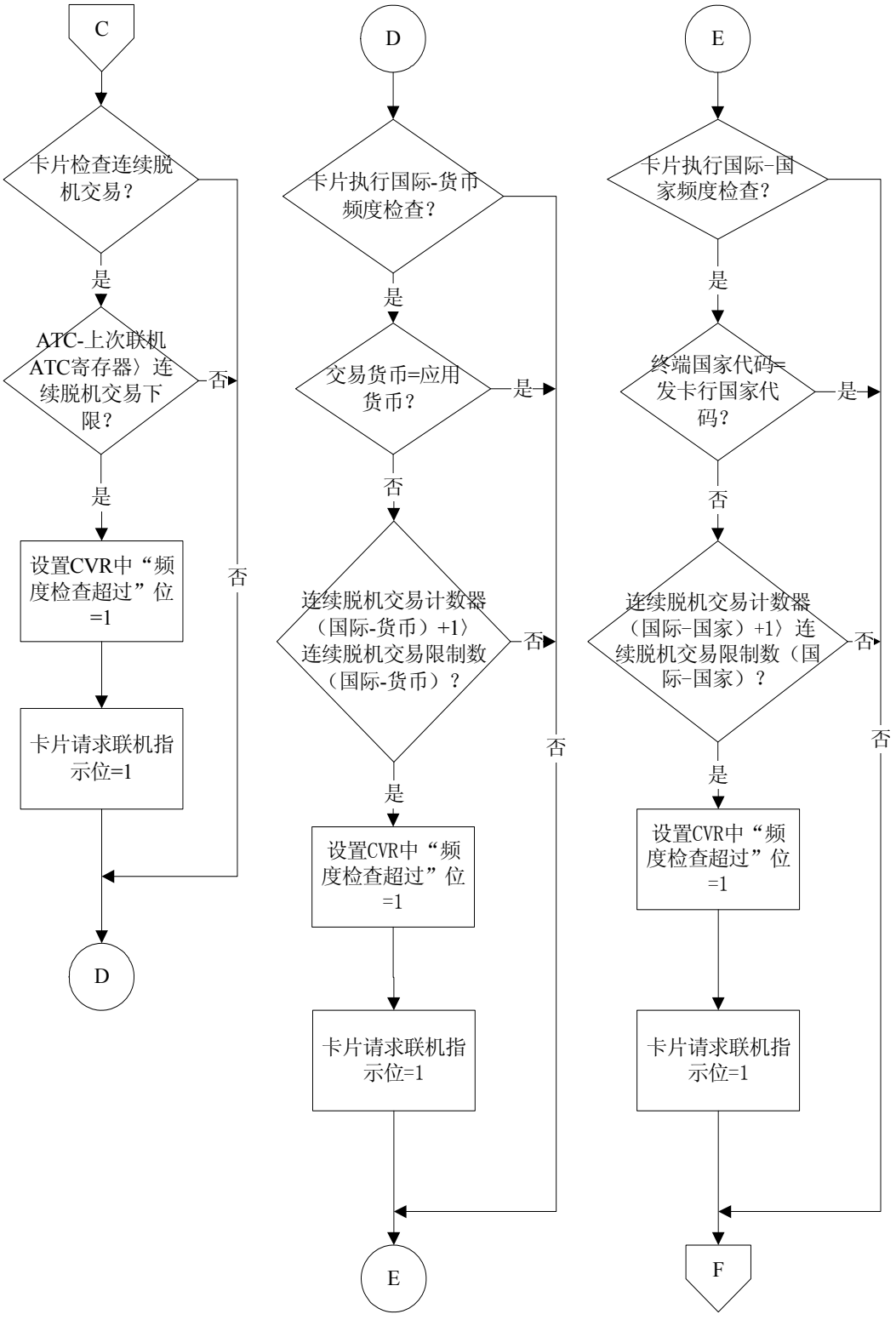


图9　卡片行为分析处理流程图（2）

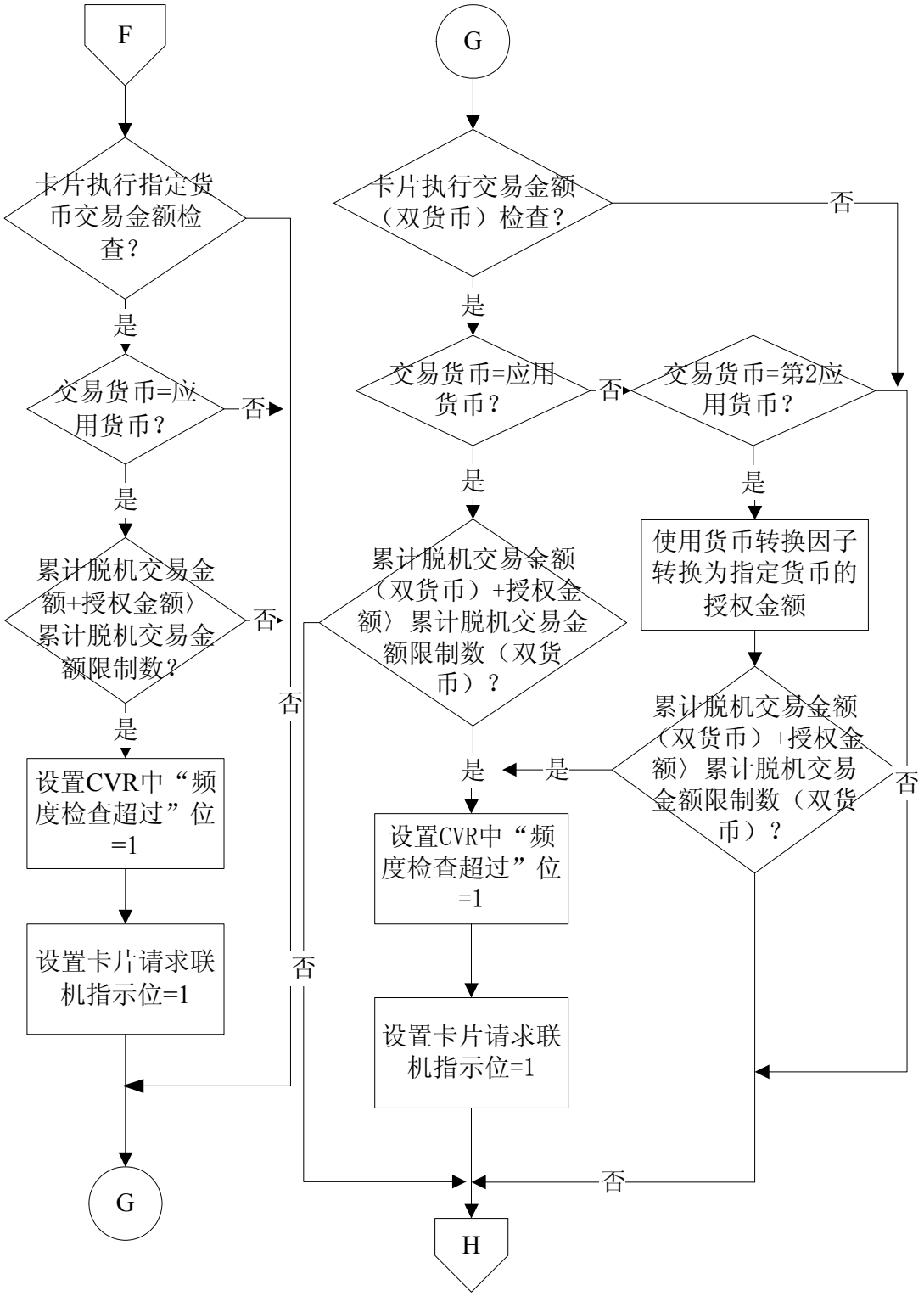


图10　卡片行为分析处理流程图（3）

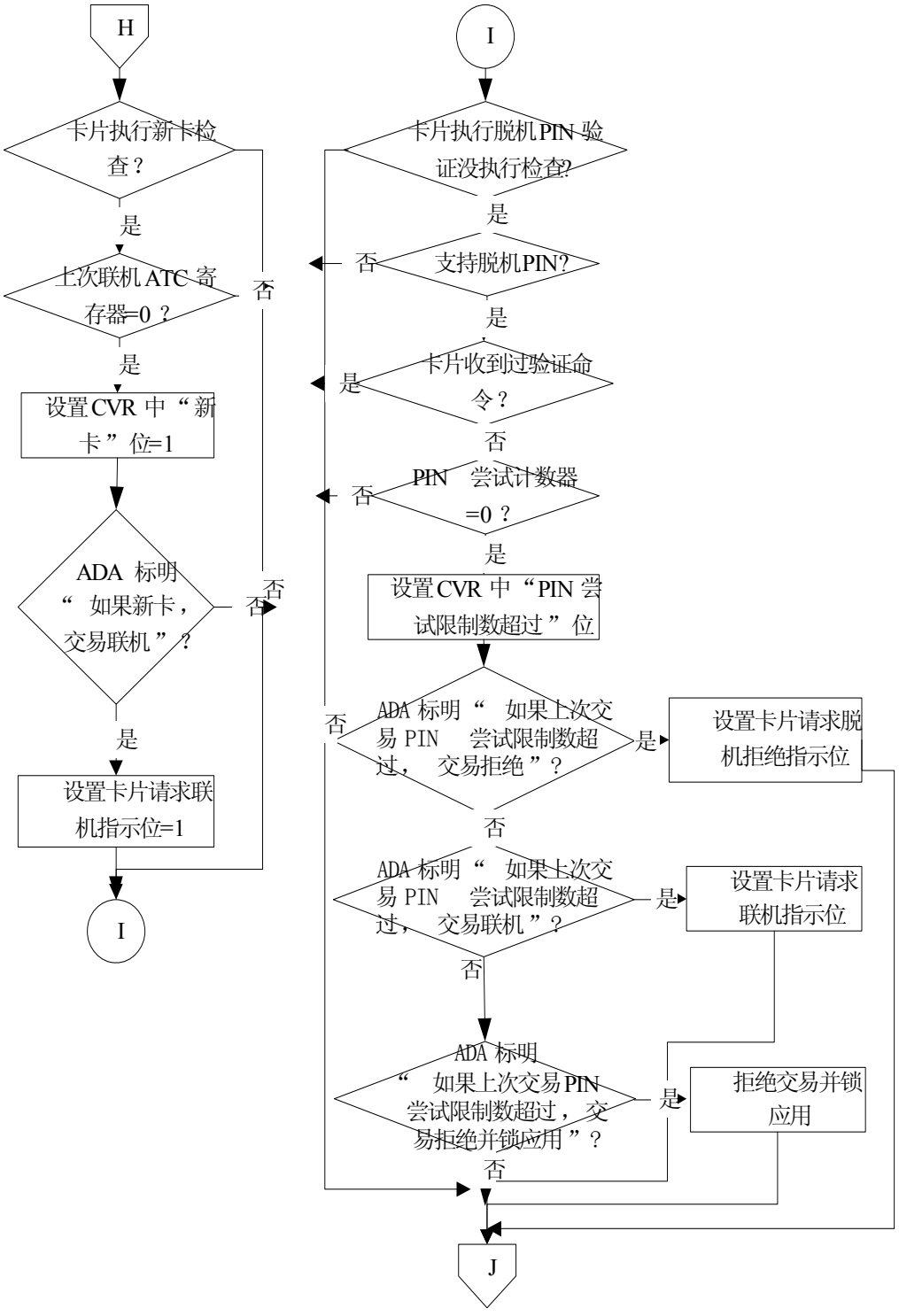


图11　卡片行为分析处理流程图（4）

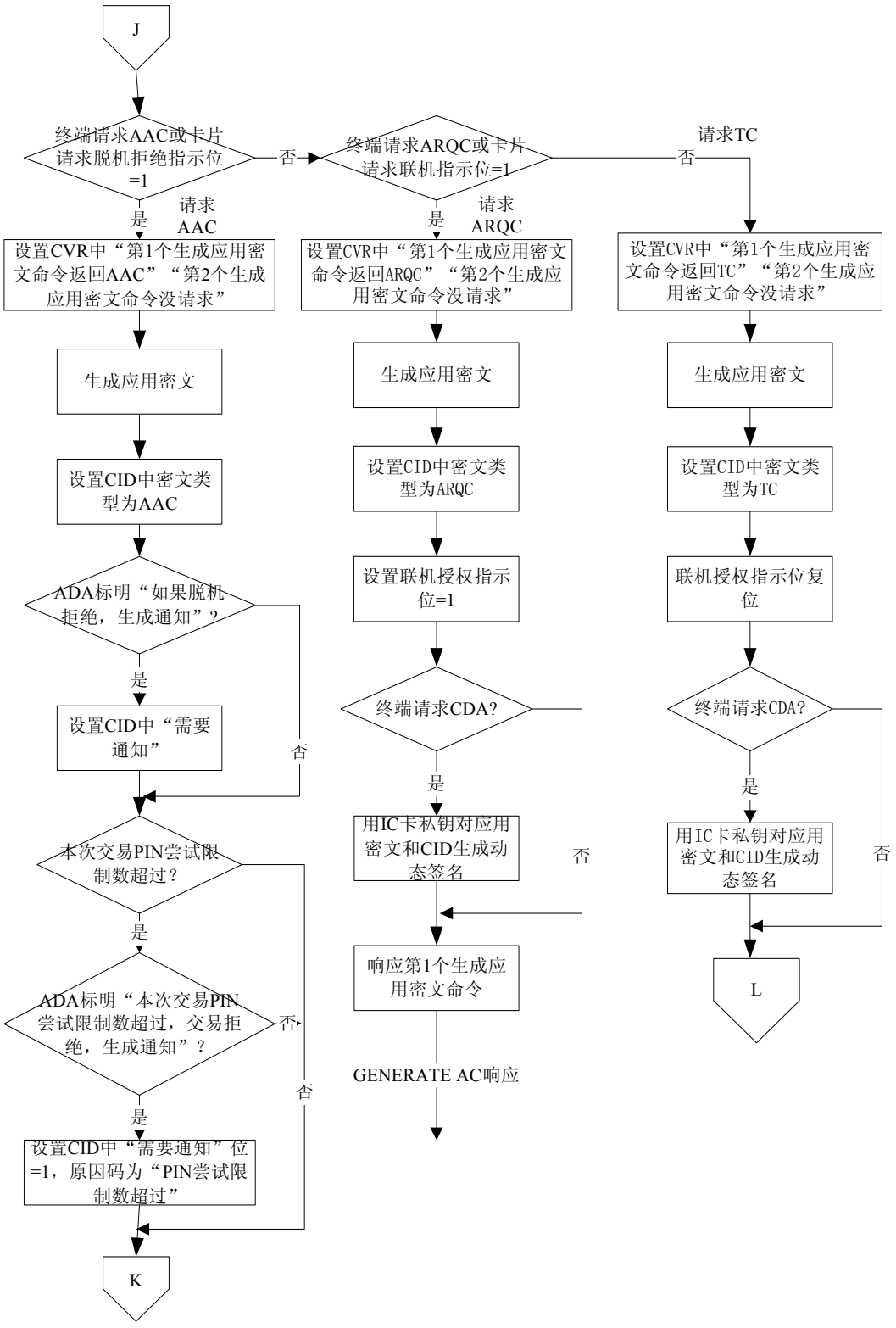


图12　卡片行为分析处理流程图（5）

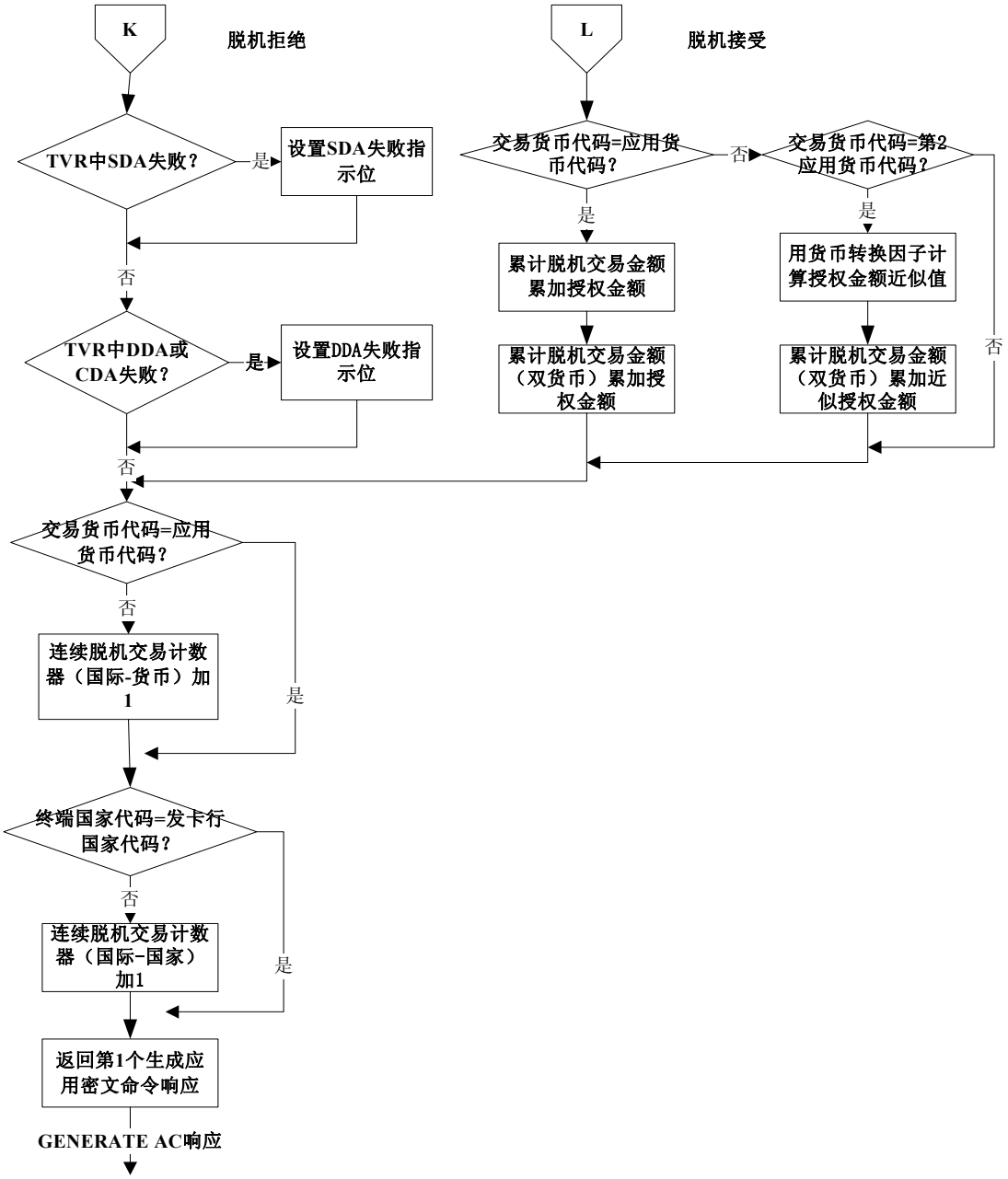


图13　卡片行为分析处理流程图（6）

14.7　前期相关处理

读应用数据

终端从卡片中读取CDOL1数据，和交易明细文件短文件标识符（SFI）。

卡片行为分析

终端发送第1个生成应用密文（GENERATE AC）命令给卡片请求密文。命令包括CDOL1中指定的终端数据，这些数据用来生成应用密文和进行卡片风险管理。

14.8 后续相关处理

联机处理

终端根据生成应用密文（GENERATE AC）命令返回的密文类型决定是否执行联机授权。

结束

如果请求交易联机授权但是终端没有联机能力，卡片执行另外的风险管理。

根据发卡行认证的状态和发卡行认证的卡片设置，卡片中的一些计数器和指示位会被复位。

15 联机处理

联机处理允许发卡行使用发卡行主机系统中的风险管理参数对交易进行检查，作出批准或拒绝交易的决定。除了执行传统的联机检查以外，主机授权系统可以使用由卡片生成的动态密文执行联机卡片认证，并且在作出授权决定时可以考虑交易脱机处理的结果。

发卡行的响应可以包括给卡片的二次发卡更新和一个发卡行生成的密文。卡片验证密文确保响应来自一个有效的发卡行。此验证叫发卡行认证。

本章描述卡片联机处理功能。

15.1 卡片数据

表34列出了在联机处理过程中终端使用的卡片数据。

表34 生成应用密文响应——卡片数据

数据元	描述
密文信息数据	包括表示密文类型的指示位
应用交易计数器（ATC）	卡片建立应用时初始化的交易计数器
应用密文	卡片返回联机密文 ARQC
发卡行应用数据	发卡行应用数据是 JR/T 0025 必备数据，用来把 JR/T 0025 定义的数据传送给终端，然后被放到联机请求报文或清算报文中。此数据中包括的数据元有： ● 长度指针 ● 分散密钥索引 ● 密文版本信息 ● 卡片验证结果（CVR） ● 算法标识 ● 发卡行自定义数据（可选）

表35列出了在收到联机请求后，终端使用的卡片数据。

表35 决定发卡行认证——卡片数据

数据元	描述
应用交互特征（AIP）	AIP 数据在应用初始化步骤由卡片送给终端。如果卡片支持发卡行认证，AIP 中“发卡行认证”位为“1”

表36列出了在发卡行认证处理中卡片用到的数据。

表36 联机处理，发卡行认证——卡片数据

数据元	描述
授权请求密文	卡片在卡片行为分析处理时生成的应用密文，用来验证授权响应密文（ARPC）
卡片验证结果	CVR 包括了下列和发卡行认证相关的标记： ● 发卡行认证执行并失败 ● 上次联机交易发卡行认证失败 ● 联机交易后发卡行认证没有执行
发卡行认证失败指示位	如果发卡行认证失败，卡片设置此指示位

应用密文（AC）密钥	卡片认证 ARPC 使用的对称密钥

15.2 联机响应数据

从发卡行到终端的联机响应信息中包括的数据在表37列出。终端用外部认证命令将此数据送入卡片中用于发卡行认证。除了下面的数据，联机响应中可以包括发卡行脚本数据。

表37 联机处理——终端数据

数据元	描述
发卡行认证数据	在外部认证（EXTERNAL AUTHENTICATE）命令的数据域中的数据。包括内容： 授权响应密文（8 字节）——发卡行主机（或代理）生成 授权响应码（2 字节）——用来计算 ARPC 的数据

15.3 命令

外部认证（EXTERNAL AUTHENTICATE）命令

如果执行发卡行认证，终端发送外部认证命令给卡片。

外部认证命令里包括发卡行认证数据。

外部认证命令的响应码说明发卡行认证数据验证是否通过。如果验证通过，SW1 SW2=“9000”，如果失败，返回“6300”。

一次交易中，卡片允许处理一次外部认证命令，后续的外部认证命令卡片一律返回“6985”。

命令编码见附录B。

15.4 处理流程

联机处理由联机请求处理，联机响应处理和发卡行认证三部分组成。卡片只在发卡行认证过程中有操作。

15.4.1 联机请求

当终端收到卡片返回的ARQC而且具有联机能力，终端发起一个联机请求。联机请求中包括终端之前从卡片取得的数据。在此步骤中，卡片不进行操作。

15.4.2 联机响应

在联机响应处理中，卡片不进行操作。

15.4.3 发卡行认证

如果卡片中的AIP数据表明卡片支持发卡行认证，而且终端收到的联机响应中包括发卡行认证数据，终端发送一个外部认证命令给卡片。

当卡片收到外部认证命令，卡片执行发卡行认证，步骤如下：

步骤 1：如果在当前交易里，收到过外部认证命令：

——设置发卡行认证失败指示位为“1”；

——返回状态字 SW1 SW2=“6985”。

步骤 2：将发卡行认证数据中的授权响应码分离出来保存，将来在交易结束阶段使用；

步骤 3：使用第 1 次生成应用密文（GENERATE AC）命令响应时生成的 ARQC 和授权响应码生成一个授权响应密文（ARPC）。附录 D 中描述密文生成用的密钥和算法；

步骤 4：新生成的 ARPC 和外部认证命令里送进来的 ARPC 进行比较，如果相同，发卡行认证成功。

如果发卡行认证成功，卡片：

步骤 1：设置发卡行认证失败指示位为“0”；

步骤 2：外部认证命令响应“9000”。

如果发卡行认证失败，卡片：

步骤 1：设置发卡行认证失败指示位为“1”；

步骤 2：设置 CVR 中“发卡行认证执行但失败”位为“1”；

步骤 3：外部认证命令响应“6300”。

卡片要确保当交易结束，卡片从终端中取出后，发卡行认证失败指示位继续设置为“1”。在下一个交易中，卡片行为分析过程中要检查此指示位来决定交易是否要联机上送。

在交易结束过程中，卡片在处理第2个生成应用密文（GENERATE AC）命令时，要检查发卡行认证是否执行以及是否成功。

15.5 流程图

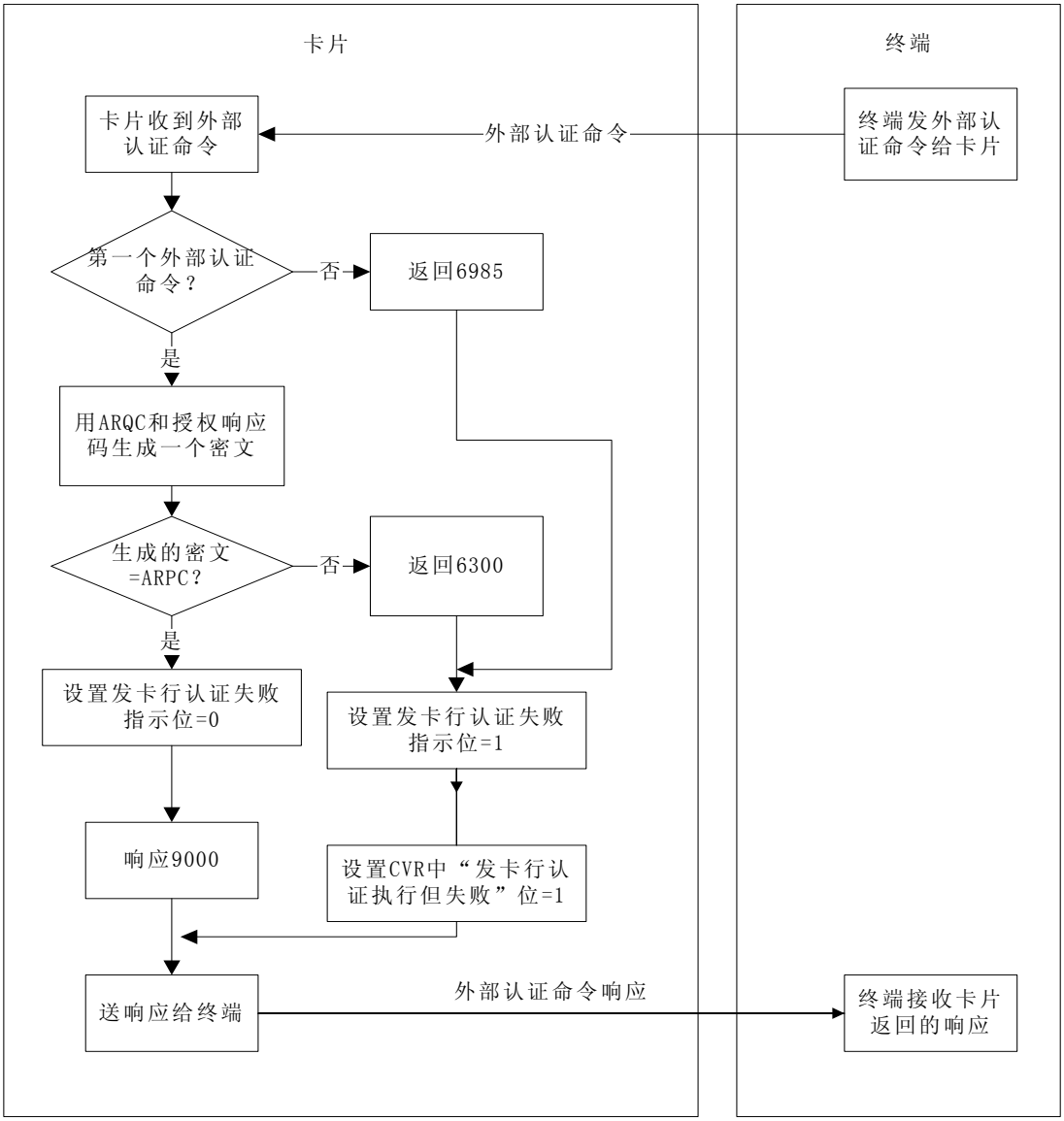


图14 联机处理流程图

15.6 前期相关处理

应用初始化

卡片在获取处理选项（GPO）命令中返回AIP给终端，AIP中标明卡片是否支持发卡行认证。

卡片行为分析

第1条生成应用密文（GENERATE AC）命令里，卡片响应应用密文。

15.7 后续相关处理

交易结束

在交易结束处理中，卡片使用发卡行认证结果决定交易的最终结果以及对一些计数器和指示位进行复位。

发卡行到卡片脚本处理

终端将在联机响应中包括的所有发卡行脚本命令发送到卡片。

卡片行为分析（后续交易）

如果联机授权指示位指出：上次交易联机处理没有完成，卡片将请求本次交易进行联机授权。

16 交易结束

终端和卡片执行交易结束步骤决定交易处理结果。包括下列步骤：

——如果请求了联机处理但是终端不支持联机或者联机授权没有完成，终端和卡片执行另外的风险管理决定交易是接受还是拒绝；

——卡片可以根据发卡行认证的结果以及卡片内部的一些设置将一个发卡行作出的联机接受交易改为拒绝；

——一些计数器和指示位要被设置用来记录交易过程中发生的各种情况；

——联机授权结束后，根据授权结果和卡片内部的一些设置，一些计数器和指示位复位。

16.1 卡片数据

表38列出卡片在交易结束处理过程中使用的数据。

表38 交易结束——卡片数据

数据元	描述
应用货币代码（9F51）	指明和应用有关的国内货币
应用缺省行为（ADA）	发卡行定义的指示器，指定在一些特殊条件下的卡片行为
应用交互特征（AIP）	包括表明卡片支持发卡行认证能力的指示位
连续脱机交易计数器（国际-货币）	JR/T 0025 专有数据。记录自从上次联机授权以来，使用非指定货币的脱机交易的次数
连续脱机交易计数器（国际-国家）	JR/T 0025 专有数据。记录自从上次联机授权以来，终端国家代码和发卡行国家代码不同的脱机交易的次数。此检查使用发卡行国家代码决定交易是国内还是国际
累计脱机交易金额	JR/T 0025 专有数据。记录自从上次联机处理以来，使用应用指定货币的脱机交易总金额
累计脱机交易金额（双货币）	JR/T 0025 专有数据。记录自从上次联机处理以来，使用应用指定货币（应用货币代码）和第 2 应用货币的脱机交易总金额。如果是第 2 应用货币，在累加之前要先使用货币转换因子将授权金额进行转换
累计脱机交易金额上限	JR/T 0025 专有数据。累计脱机交易金额和累计脱机交易金额（双货币）的最大累计值限制数
货币转换因子	用来将第 2 应用货币转换成应用指定货币的汇率值。第 2 应用货币金额乘以转换因子转换为应用指定货币金额
DDA 失败指示位	标明本次或上次交易 DDA 失败
发卡行认证失败指示位	标明本次或上次交易发卡行认证失败，在后续交易的卡片行为分析步骤中使用
发卡行认证指示位	标明发卡行认证是必备还是可选 如果发卡行认证是必备的，卡片应收到并成功处理一个 ARPC（即通过发卡行认证）来对上次联机 ATC 寄存器和脱机计数器进行复位
发卡行国家代码（9F57）	JR/T 0025 专有数据。表明发卡行的国家

数据元	描述
发卡行脚本命令计数器	记录上次联机交易中，有安全报文的发卡行脚本命令的个数
发卡行脚本失败指示位	在上次联机交易中，发卡行脚本处理失败时设置
上次联机 ATC 寄存器	上次联机授权并满足发卡行验证需要的交易的 ATC 值
联机授权指示位	当申请联机的交易无法联机或联机授权被中止时设置的内部应用指示位
第 2 应用货币代码	用于双货币频度检查。可以使用货币转换因子转换为应用货币
SDA 失败指示位	标明本次或上次交易 SDA 失败
连续脱机交易上限	JR/T 0025 专有数据，如果交易无法联机，接受交易脱机的最大连续脱机交易次数

表39列出了在交易结束处理中卡片使用的以及生成应用密文的响应数据。

表39　生成应用密文命令响应

数据元	描述
密文信息数据	包括下列指示位： 密文类型 ● 拒绝 AAC ● 接受 TC ● 联机上送 ARQC 其它状态信息
应用交易计数器（ATC）	当应用建立的时候初始化的交易次数计数器
应用密文（AC）	密文的值。如果卡片执行 CDA，而且密文信息数据表明密文是 TC 或 ARQC，则应用密文和其它数据包含在非对称数字签名中
发卡行应用数据 ● 卡片验证结果（CVR）	包含用来上送给发卡行的自定义应用数据，包括 CVR ● JR/T 0025 专有数据。表明当前和上次交易的脱机处理结果

表40列出了在交易结束处理过程中终端使用的卡片数据。

表40　交易结束——终端使用的卡片数据

数据元	描述
卡片风险管理数据对象列表 2（CDOL2）	列出在第 2 个生成应用密文（GENERATE AC）命令中，卡片要求终端传送的数据对象（标签和长度）。除了密文算法中要求的数据标签外，下面列出的数据应在 CDOL2 中用于交易结束处理： ● 授权金额（如果支持使用金额的频度检查） ● 授权响应码 ● 终端验证结果（TVR） ● 交易货币代码（如果支持使用货币代码的检查） ● 终端国家代码（如果支持使用国家代码的检查） CDOL 中的数据元不能重复

16.2　终端数据

表41列出了在交易结束处理过程中卡片使用的终端数据。

表41　交易结束——终端数据

数据元	描述
授权金额	当前交易金额
授权响应码	表明交易处理结果，提交给卡片 ● Y1=脱机接受 ● Z1=脱机拒绝

	● Y3=不能联机（脱机接受） ● Z3=不能联机（脱机拒绝）
终端验证结果（TVR）	用来记录脱机处理结果，例如 SDA 执行情况等
终端国家代码	标明终端所在国家
交易货币代码	标明本次交易使用的货币

16.3 命令

生成应用密文（GENERATE AC）命令

终端发第2个生成应用密文（GENERATE AC）命令给卡片请求第2个应用密文。

命令的数据域包括CDOL2中指定的终端数据，包括授权响应码。

命令的P1参数表明终端请求的应用密文类型。

命令的响应信息中包括密文信息数据，说明卡片的授权结果，应用交易计数器（ATC），应用密文和发卡行应用数据。发卡行应用数据中包括记录处理结果的CVR。

第2次发生成应用密文（GENERATE AC）命令，见附录B。

16.4 处理流程

只有在卡片行为分析后，卡片返回ARQC申请联机授权的情况下卡片执行结束操作。

在卡片行为分析的最后，卡片：

——请求脱机接受或拒绝。此时卡片的处理就已经结束，不再执行交易结束步骤；

——请求联机授权。这时卡片要执行交易结束步骤。

图15是结束处理的过程图。

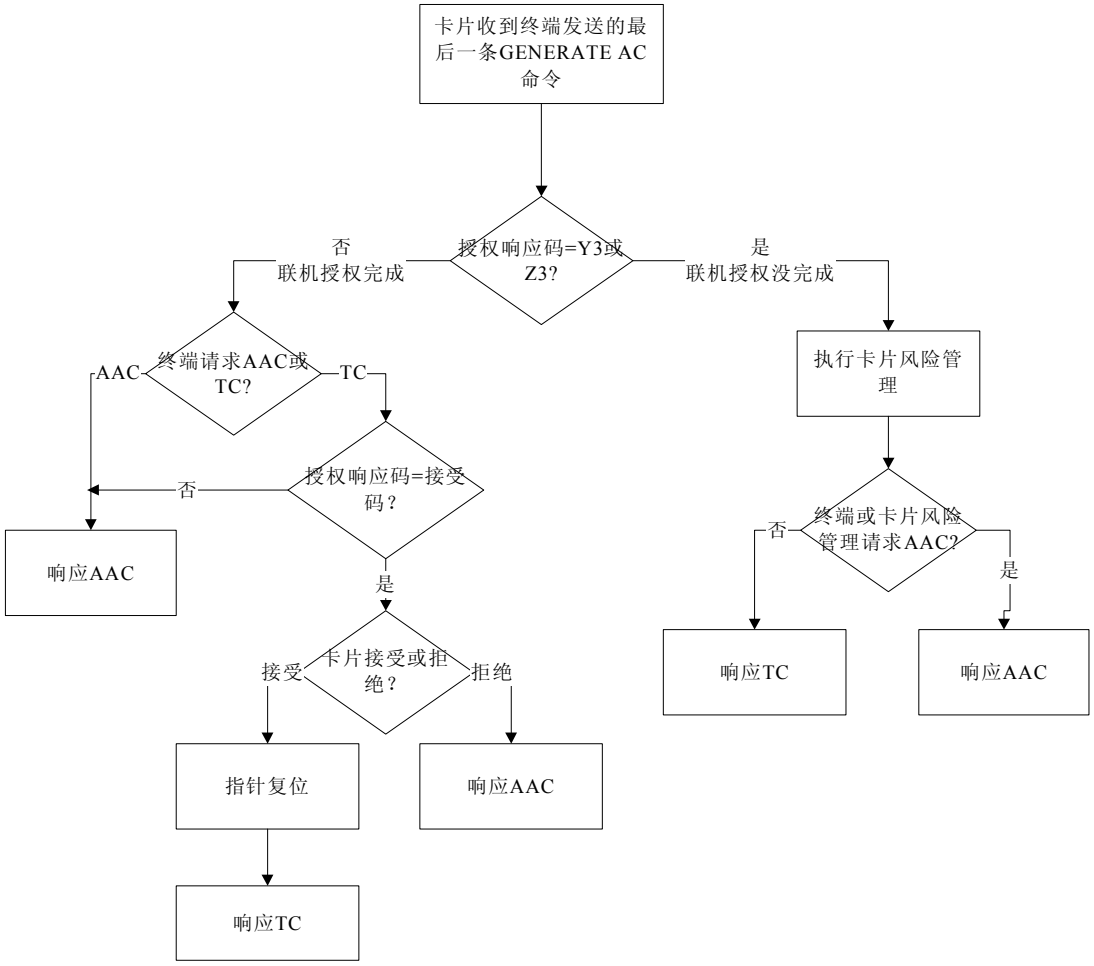


图15 交易结束处理流程图

16.5 收到生成应用密文命令

卡片在收到第2次生成应用密文（GENERATE AC）命令后，进行交易结束处理。根据命令中的授权响应码类型，结束操作分为两条线路执行：联机授权的交易见16.6和请求联机，但是联机授权没有完成的交易见16.7。

16.6 联机授权的交易

当交易进行了联机授权（授权响应码不是Y3或Z3），卡片作如下处理：

——如果发卡行认证执行，检查在外部认证命令中送来的授权响应码：

- 授权响应码为 00，10 或 11 表明发卡行接受交易；
- 授权响应码为 01 或 02 表明发卡行请求参考；
- 其它值表明发卡行拒绝，卡片按照终端请求交易拒绝进行处理。

——检查第 2 个生成应用密文（GENERATE AC）命令中的 P1 参数：

- 如果 P1 表明请求 TC（接受交易）而且授权响应码表明发卡行接受或推荐，执行交易接受处理。见 16.6.2 中的描述；
- 如果 P1 表明请求 AAC（拒绝交易）或者授权响应码表明发卡行拒绝，执行交易拒绝处理。见 16.6.1 中的描述。

16.6.1 联机授权后请求 AAC（拒绝）

当第2个生成应用密文（GENERATE AC）命令中请求生成AAC或者授权响应码表明交易发卡行拒绝，卡片要响应AAC，在响应之前，卡片：

——设置 CVR 中“第 2 个生成应用密文（GENERATE AC）命令返回 AAC 位”为“1”；

——如果 AIP 中标明支持发卡行认证但是没有执行，设置 CVR 中“联机授权后，发卡行认证没有执行”位为“1”；

——如果发卡行认证必备（由发卡行认证指示器标明）但是没有执行，设置发卡行认证失败指示位为“1”；

——如果发卡行认证：不支持，或者可选而且没有执行，或者执行并成功。下列指示位归零：

- 联机授权指示位；
- SDA 失败指示位；
- DDA 失败指示位；
- 发卡行脚本命令计数器；
- 发卡行脚本失败指示位。

——下列指示位不变：

- 上次联机 ATC 寄存器；
- 累计脱机交易金额；
- 累计脱机交易金额（双货币）；
- 连续脱机交易计数器（国际-货币）；
- 连续脱机交易计数器（国际-国家）。

——生成应用密文；

——设置密文信息数据中密文类型为 AAC；

——响应第 2 个生成应用密文（GENERATE AC）命令。

16.6.2 联机授权后请求 TC（接受）

当第2个生成应用密文（GENERATE AC）命令中终端请求TC而且授权响应码表示发卡行接受或推荐，卡片执行下列步骤：

——如果 AIP 中标明支持发卡行认证但是没有执行，设置 CVR 中“联机授权后，发卡行认证没有执行”位为“1”；

卡片可以根据发卡行认证的设置情况决定是接受交易还是拒绝交易。

卡片接受

如果下面条件满足一条，卡片接受交易：

——发卡行认证成功；

——AIP 中标明发卡行认证不支持；

——发卡行认证可选而且没有执行；

——发卡行认证失败，但是 ADA 中“如果发卡行认证失败，交易拒绝位”为“0”；

——发卡行认证必备但是没有执行，但是 ADA 中“如果发卡行认证必备但没有 ARPC 收到，交易拒绝位”为“0”。

执行卡片接受交易的后续步骤，见16.6.2.1。

卡片拒绝

如果下面条件满足一条，卡片拒绝交易：

——发卡行认证失败，ADA 中“如果发卡行认证失败，交易拒绝位”为“1”；

——发卡行认证必备但是没有执行，但是 ADA 中“如果发卡行认证必备但没有 ARPC 收到，交易拒绝位”为“1”。

执行卡片拒绝交易的后续步骤，见16.6.2.2。

16.6.2.1 收到 TC 请求后卡片接受交易

当卡片接受交易，卡片：

步骤 1：设置 CVR 中“第 2 个生成应用密文（GENERATE AC）命令返回 TC”位为“1”；

步骤 2：设置 CID 中密文类型为 TC；

步骤 3：根据发卡行认证的状态复位计数器；

a）如果发卡行认证失败，或者必备但是没有执行，卡片：

——下列计数器值不变：

- 上次联机 ATC 寄存器；
- 累计脱机交易金额；
- 累计脱机交易金额（双货币）；
- 连续脱机交易计数器（国际-货币）；
- 连续脱机交易计数器（国际-国家）；
- 联机授权指示位；
- SDA 失败指示位；
- DDA 失败指示位；
- 发卡行脚本命令计数器；
- 发卡行脚本失败指示位。

——如果发卡行认证必备但是没有执行：

- 设置发卡行认证失败指示位为“1”；
- 设置 CVR 中“联机授权以后，发卡行认证没有执行位”为“1”。

b）如果发卡行认证成功，或者可选而且没有执行，或者不支持，卡片：

——如果 AIP 标明支持发卡行认证但是卡片没有收到外部认证命令，设置 CVR 中“联机授权以后，发卡行认证没有执行位”为“1”；

——下列计数器和指示位复位：

- 联机授权指示位；
- SDA 失败指示位；
- DDA 失败指示位；
- 发卡行脚本命令计数器；
- 发卡行脚本失败指示位；

- 累计脱机交易金额；
- 累计脱机交易金额（双货币）；
- 连续脱机交易计数器（国际-货币）；
- 连续脱机交易计数器（国际-国家）。

——修改上次联机 ATC 寄存器的值为当前交易 ATC。

步骤 4：生成应用密文；

步骤 5：卡片记录交易明细，明细的内容在交易初始化阶段，通过获取处理选项（GPO）命令传送到卡片中。关于卡片交易明细的内容见第 18 章；

步骤 6：响应第 2 个生成应用密文（GENERATE AC）命令。

16.6.2.2 收到 TC 请求后卡片拒绝交易

当卡片收到接受交易请求后决定拒绝交易，卡片：

——设置 CVR 中“第 2 个生成应用密文（GENERATE AC）命令返回 AAC”位为“1”；

——如果支持发卡行认证而且是必备的，设置发卡行认证失败指示位为“1”；

——设置 CID 中的应用密文类型为 AAC；

——如果 ADA 中“如果因为发卡行认证失败或没有执行造成交易拒绝，生成通知”位为“1”，设置 CID 中“需要通知”位为“1”；

——下列计数器值不变：

- 累计脱机交易金额；
- 累计脱机交易金额（双货币）；
- 连续脱机交易计数器（国际-货币）；
- 连续脱机交易计数器（国际-国家）；
- 上次联机 ATC 寄存器；
- SDA 失败指示位；
- DDA 失败指示位；
- 发卡行脚本命令计数器；
- 发卡行脚本失败指示位。

卡片：

——生成应用密文（GENERATE AC）；

——响应第 2 个生成应用密文（GENERATE AC）命令。

16.7 请求联机操作，但是联机授权没有完成

当发送的第2个生成应用密文（GENERATE AC）命令中的授权响应码表明请求联机处理但是没有完成时（Y3或Z3），卡片：

——执行可选的卡片风险管理见 16.7.1 中描述；

——响应终端见 16.7.2 中描述。

16.7.1 卡片风险管理

卡片风险管理执行的检查是可选的，包括检查连续脱机交易的次数是否超过了连续脱机交易上限，连续脱机累计金额是否超过限制数，卡片是否新卡和PIN尝试限制数是否在上次交易中超过。

当联机授权没有完成，即使在第2个生成应用密文（GENERATE AC）命令中终端请求拒绝（AAC）或在之前的风险管理中卡片决定拒绝，卡片仍然要执行所有支持的卡片风险管理步骤。因为卡片执行所有的检查，执行检查的顺序不需要按照下面所描述的顺序。

16.7.1.1 连续脱机交易上限频度检查

此检查可选。检查连续脱机交易次数是否超过了最大限制。

如果上次联机ATC寄存器和JR/T 0025专有数据：连续脱机交易上限（标签“9F59”）存在，卡片执行此检查。

如果ATC和上次联机ATC寄存器的差值大于连续脱机交易上限，卡片：

——设置 CVR 中“频度检查超过”位为“1”；

——设置卡片请求脱机拒绝指示位为“1”。在卡片风险管理后，卡片返回交易拒绝。

16.7.1.2 新卡检查

此检查可选。检查以前是否有过联机接受的交易。

如果卡片中上次联机ATC寄存器存在，卡片执行此检查。如果ADA不存在，卡片认为缺省为零。

如果上次联机ATC寄存器值为零，卡片：

——设置 CVR 中“新卡”位为“1”；

——如果 ADA 中“如果是新卡而且交易无法联机，交易拒绝”位为“1”，设置卡片请求脱机拒绝指示位为“1”。在卡片风险管理后，卡片返回交易拒绝。

16.7.1.3 PIN 尝试限制数超过检查

此项检查可选，检查PIN尝试限制数是否在之前的交易中就已经超过。

如果卡片中没有ADA数据，卡片认为ADA值缺省为零。

如果卡片支持脱机PIN验证，而且在本次交易中，卡片没有收到过验证命令，卡片：

——如果 PIN 尝试计数器已经为零，而且如果 ADA 中“如果上次交易 PIN 尝试限制数超过而且交易无法联机，交易拒绝”位为“1”：

- 设置卡片请求脱机拒绝指示位为“1”；
- 设置 CVR 中“PIN 尝试限制数超过”位为“1”。

16.7.1.4 累计脱机交易金额（上限）频度检查

此检查可选。检查使用指定货币的连续脱机交易累计金额是否超过了最大限制数。

如果累计脱机交易金额和累计脱机交易金额上限数据存在，卡片执行此检查。

如果累计脱机交易金额加本次授权金额大于累计脱机交易金额上限。

卡片：

——设置 CVR 中频度检查超过位为“1”；

——设置卡片请求脱机拒绝指示位为“1”。

16.7.1.5 累计脱机交易金额上限（双货币）频度检查

此检查可选。检查使用指定货币和第2应用货币的连续脱机交易累计金额是否超过了最大限制数。

如果累计脱机交易金额（双货币）和累计脱机交易金额上限数据存在，卡片执行此检查。

如果累计脱机交易金额加本次授权金额（如果使用第2应用货币要先使用货币转换因子转换）大于累计脱机交易金额上限。

卡片：

——设置 CVR 中频度检查超过位为“1”；

——设置卡片请求脱机拒绝指示位为“1”。

16.7.2 无法联机上送后的卡片响应

根据终端请求的应用密文类型和卡片风险管理的结果，卡片响应第2个生成应用密文（GENERATE AC）命令。

如果下面的条件满足一条，卡片拒绝交易：

——终端在生成应用密文命令中请求 AAC；

——卡片风险管理的结果是卡片请求脱机拒绝指示位设置为“1”。

交易拒绝处理在“16.7.2.1无法联机上送后，卡片拒绝交易”中描述。

如果下面的条件都满足，卡片接受交易：

——终端在生成应用密文命令中请求 TC；

——卡片风险管理的结果是卡片请求脱机拒绝指示位设置为“0”。

交易接受处理在16.7.2.2中描述。

16.7.2.1 无法联机上送后，卡片拒绝交易

本部分描述了当交易请求联机但是联机授权无法完成（授权响应码为Y3或Z3），卡片拒绝交易的处理过程。卡片：

——设置 CVR 中的下列指示位：

- 第 2 个生成应用密文（GENERATE AC）命令返回 AAC；
- 终端不能联机上送。

——如果 TVR 中“SDA 失败”位为“1”，设置 SDA 失败指示位为“1”；

——如果 TVR 中“DDA 失败”位为“1”，设置 DDA 失败指示位为“1”；

——如果 TVR 中“CDA 失败”位为“1”，设置 DDA 失败指示位为“1”；

——如果终端国家代码和发卡行国家代码不同，连续脱机交易计数器（国际-国家）加 1；

——如果交易货币代码和应用货币代码不同，连续脱机交易计数器（国际-货币）加 1；

——如果 ADA 中“如果交易拒绝，生成通知”位为“1”，设置 CID 中“需要通知”位为“1”；

——上次联机 ATC 寄存器值不变；

——生成应用密文；

——设置 CID 中应用密文类型；

——响应生成应用密文（GENERATE AC）命令。

16.7.2.2 无法联机上送后，卡片接受交易

本部分描述了当交易请求联机但是联机授权无法完成（授权响应码为Y3或Z3），卡片接受交易的处理过程。卡片：

——设置 CVR 中的下列指示位：

- 第 2 个生成应用密文命令返回 TC；
- 终端不能联机上送。

——如果终端国家代码和发卡行国家代码不同，连续脱机交易计数器（国际-国家）加 1；

——如果交易货币代码和应用货币代码相同；

- 累计脱机交易金额累加授权金额；
- 累计脱机交易金额（双货币）累加授权金额。

——如果交易货币代码和应用货币代码不同，连续脱机交易计数器（国际-货币）加 1；

——如果交易货币代码和第 2 应用货币代码相同，累计脱机交易金额（双货币）累加转换后的授权金额；

——上次联机 ATC 寄存器值不变；

——生成应用密文；

——设置 CID 中密文类型为 TC；

——卡片记录交易明细，明细的内容在交易初始化阶段，通过获取处理选项（GPO）命令传送到卡片中。关于卡片交易明细的内容见第 18 章中描述；

——响应生成应用密文命令。

16.8 复合动态数据认证/生成应用密文响应

当终端发送的生成应用密文命令中的P1参数中CDA位为“1”且卡片AIP标明卡片支持CDA时，卡片执行CDA。

卡片：

步骤 1：按照上面的描述，生成应用密文；

步骤 2：如果卡片响应 AAC，没有特殊处理；

步骤 3：如果卡片响应 TC，卡片响应的应用密文作为签名动态应用数据用 IC 卡私钥做签名，步骤如下：

a）设置 CVR 中“DDA 执行”位为“1”。此步骤在步骤 1 生成应用密文之前执行；

b）使用应用密文生成一个动态密文，详见 JR/T 0025.7 中的 5.3.6。归纳为下面 4 个步骤：

——按照 JR/T 0025.7 的 5.3.6 中描述组织数据。数据包括 IC 卡动态数据（包括 IC 卡动态数长度、IC 卡动态数、密文信息数据和应用密文等）；

——用上述数据做一个哈希计算；

——将哈希包括到签名的动态应用数据中；

——使用 IC 卡私钥对签名的动态应用数据作签名。

c）响应生成应用密文（GENERATE AC）命令信息中包括签名的动态应用数据。

16.9 流程图

图16－图20是卡片执行交易结束处理的流程图。

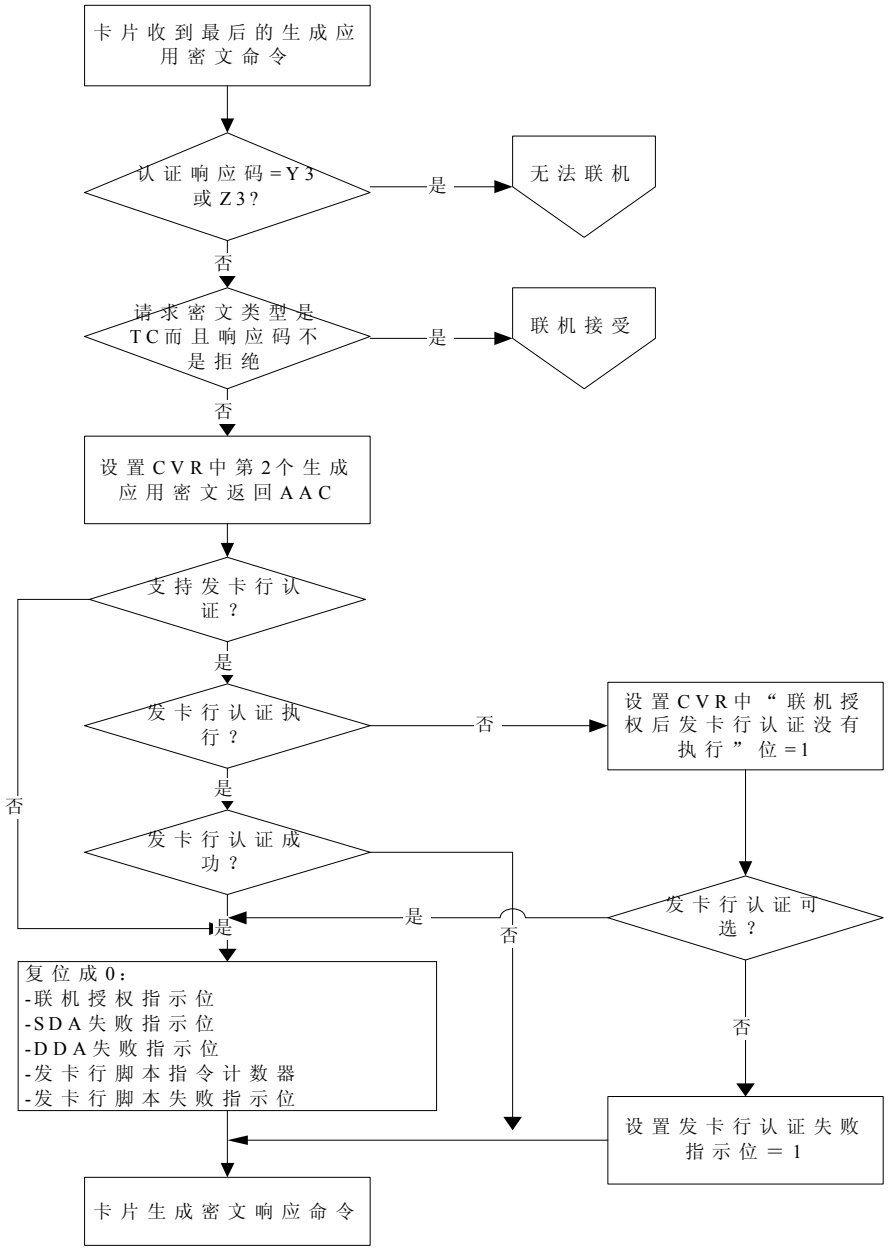


图16　交易流程图（1）

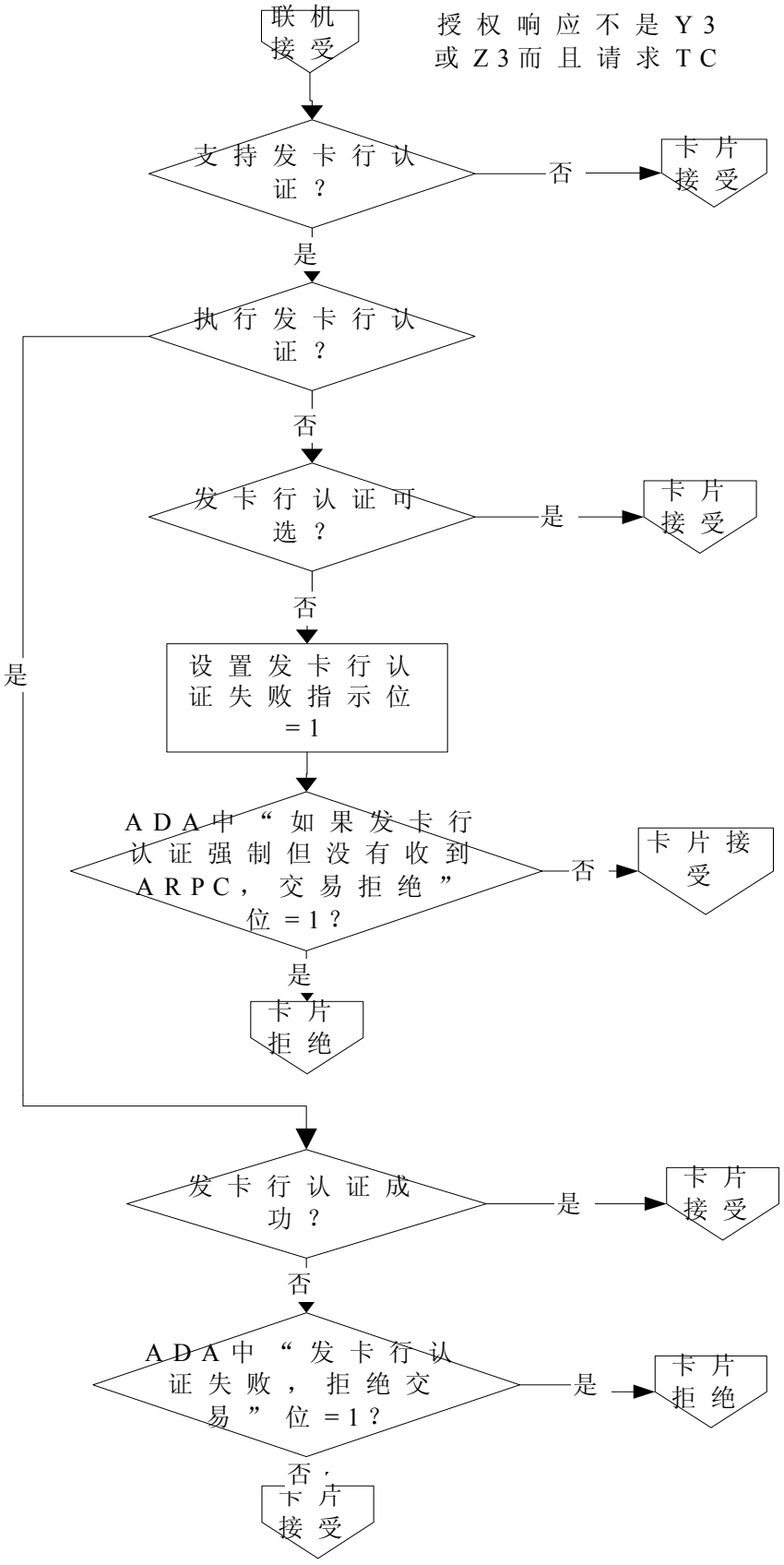

联机接受
授权响应不是Y3或Z3而且请求TC
支持发卡行认证？
否
卡片接受
是
执行发卡行认证？
否
发卡行认证可选？
是
卡片接受
否
设置发卡行认证失败指示位=1
是
ADA中“如果发卡行认证强制但没有收到ARPC，交易拒绝”位=1？
否
卡片接受
是
卡片拒绝
发卡行认证成功？
是
卡片接受
否
ADA中“发卡行认证失败，拒绝交易”位=1？
是
卡片拒绝
否，
卡片接受

图17　交易流程图（2）

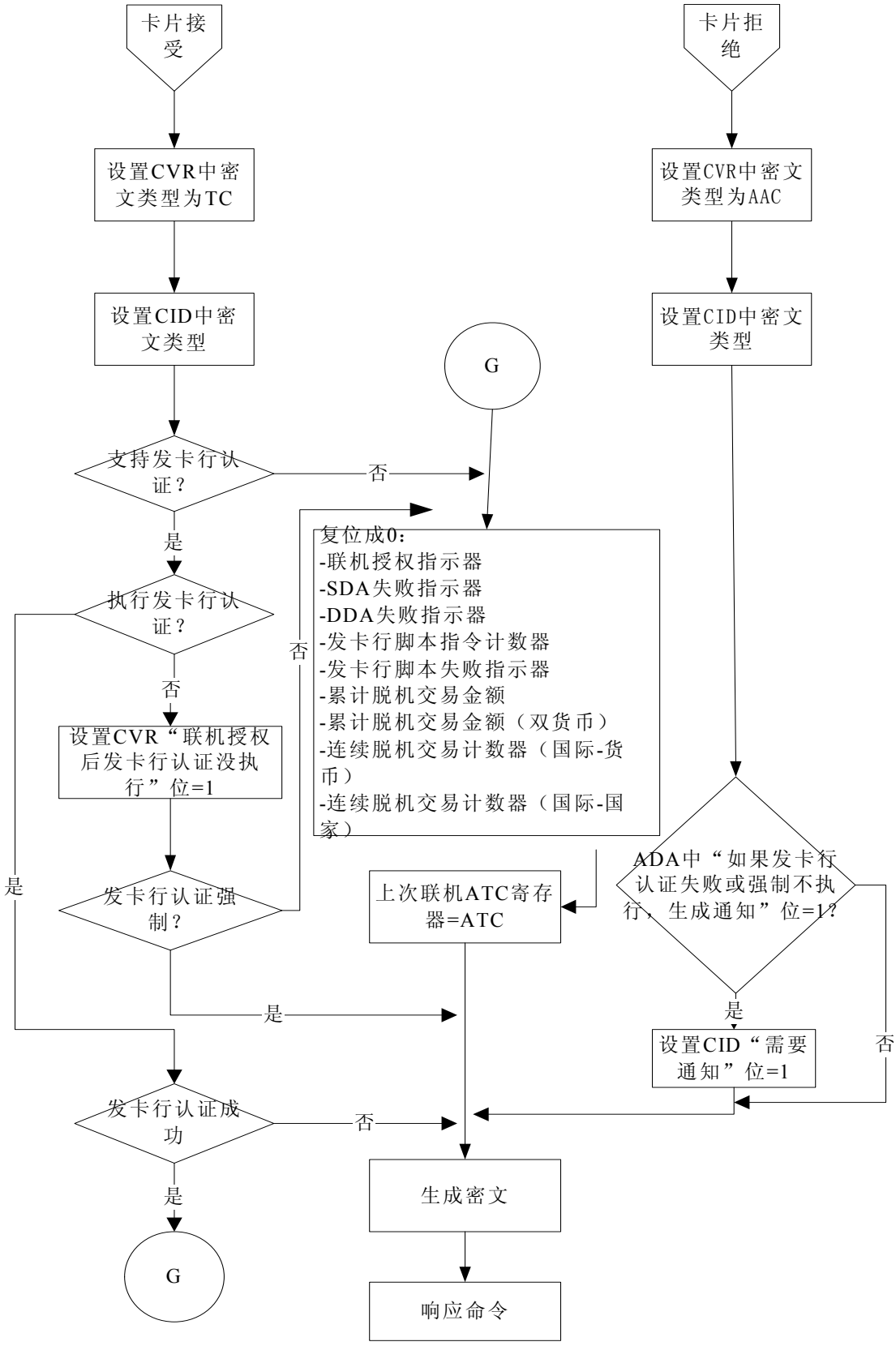

卡片接受
卡片拒绝
设置CVR中密文类型为TC
设置CVR中密文类型为AAC
设置CID中密文类型
设置CID中密文类型
G
支持发卡行认证？
否
是
复位成0：
-联机授权指示器
-SDA失败指示器
-DDA失败指示器
-发卡行脚本指令计数器
-发卡行脚本失败指示器
-累计脱机交易金额
-累计脱机交易金额（双货币）
-连续脱机交易计数器（国际-货币）
-连续脱机交易计数器（国际-国家）
执行发卡行认证？
否
设置CVR“联机授权后发卡行认证没执行”位=1
发卡行认证强制？
否
是
上次联机ATC寄存器=ATC
ADA中“如果发卡行认证失败或强制不执行，生成通知”位=1?
是
否
设置CID“需要通知”位=1
是
发卡行认证成功
否
是
生成密文
G
响应命令

图18　交易流程图（3）

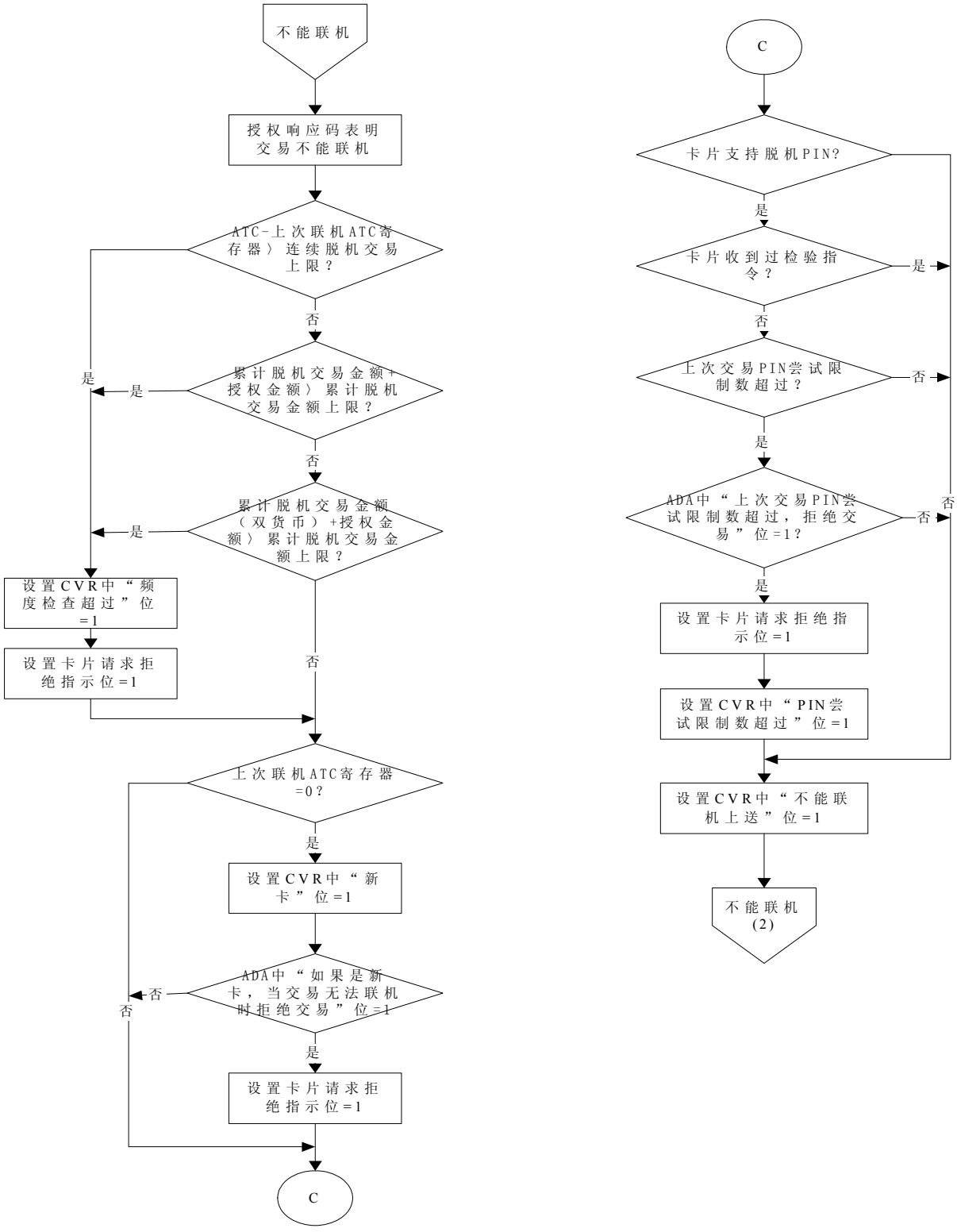

不能联机
授权响应码表明交易不能联机
ATC-上次联机ATC寄存器〉连续脱机交易上限？
否
是
是
累计脱机交易金额+授权金额〉累计脱机交易金额上限？
否
是
累计脱机交易金额（双货币）+授权金额〉累计脱机交易金额上限？
否
设置CVR中“频度检查超过”位=1
设置卡片请求拒绝指示位=1
上次联机ATC寄存器=0？
是
设置CVR中“新卡”位=1
否
否
ADA中“如果是新卡，当交易无法联机时拒绝交易”位=1
是
设置卡片请求拒绝指示位=1
C
C
卡片支持脱机PIN?
是
卡片收到过检验指令？
是
否
上次交易PIN尝试限制数超过？
否
是
ADA中“上次交易PIN尝试限制数超过，拒绝交易”位=1？
否
是
设置卡片请求拒绝指示位=1
设置CVR中“PIN尝试限制数超过”位=1
设置CVR中“不能联机上送”位=1
不能联机(2)

图19　交易流程图（4）

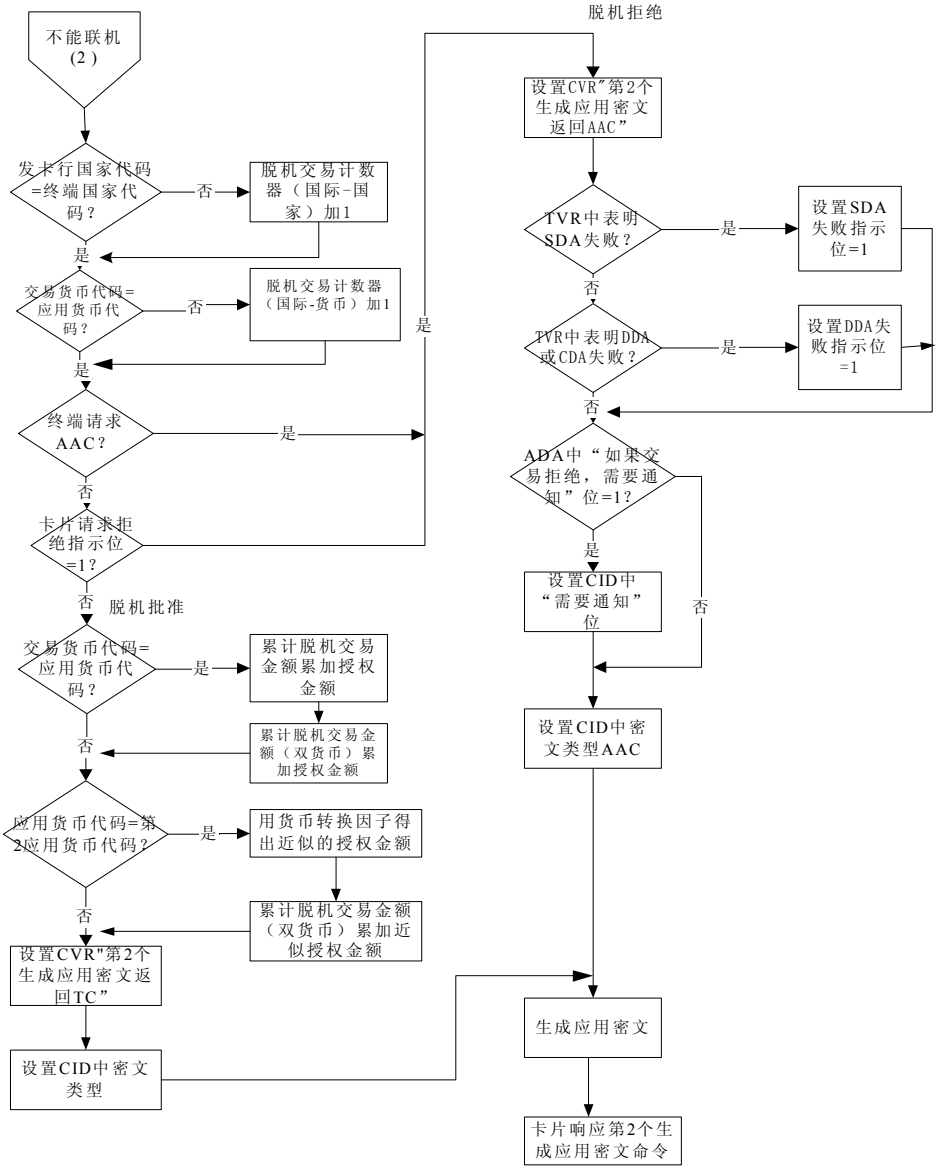


图20　交易流程图（5）

16.10　前期相关处理

读应用数据

从卡片中读出交易明细文件短文件标识符。

卡片行为分析

卡片行为分析处理后，卡片作出交易联机、交易拒绝或交易接受的决定。只有当卡片作出交易请求联机授权的交易才执行交易结束处理步骤。此时终端向卡片发送第2个生成应用密文（GENERATE AC）命令。

联机处理

如果卡片收到终端发送的外部认证命令，卡片验证命令中的ARPC后设置指示器为“发卡行验证执行并通过”或“发卡行验证执行并失败”。

16.11　后续相关处理

卡片行为分析（后续交易）

在下一次交易时，卡片使用交易结束处理时设置的计数器和指示位进行判断和检查。

17 发卡行脚本处理

发卡行可以不用重新发卡而是通过发卡行脚本处理来修改卡片中的个人化数据。发卡行将脚本命令放在授权响应报文中传送给终端，终端将命令转发给卡片。当满足安全要求以后，卡片执行命令。

支持的命令有：

——修改卡片参数；

——锁定或解锁应用；

——锁卡；

——重置 PIN 尝试计数器；

——修改脱机 PIN 值。

脚本处理通过锁定恶意透支和失窃的卡片来限制信用和伪卡风险。卡片参数可以在不需要重新发卡的情况下根据持卡人情况的变化而修改。

17.1 卡片数据

表42描述了在发卡行脚本处理过程中卡片使用的计数器和指示位。

表42 发卡行脚本处理——卡片数据

数据元	描述
应用交易计数器（ATC）	每次交易加 1 的计数器。在脚本处理中用于计算过程密钥
卡片验证结果（CVR）	在后续交易的卡片行为分析处理中，CVR 中的一些内容被设置： ● 上次联机交易，第 2 次生成应用密文（GENERATE AC）命令后卡片收到的有安全报文的命令的个数，值来自发卡行脚本命令计数器 ● 发卡行脚本命令失败位设置为“1”——如果发卡行脚本失败指示位为“1”
发卡行脚本命令计数器	记录第 2 次生成应用密文后卡片收到的有安全报文的命令的个数。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位	在第 2 次生成应用密文（GENERATE AC）命令后，如果脚本命令执行失败，指示位置“1”，失败的情况有： ● 安全报文错误（计算的 MAC 和命令中的 MAC 不等） ● 安全报文通过但是命令执行失败 ● 需要安全报文但是不存在 不含安全报文的脚本命令执行失败不影响这个指示位。在下次交易中的结束处理步骤中可能被复位

17.2 终端数据

表43列出了发卡行脚本处理过程中使用的终端数据。

表43 发卡行脚本处理——终端数据

数据元	描述
发卡行脚本结果	记录卡片对发卡行脚本命令处理的结果，此结果要包括在清算报文和下次联机授权中
终端验证结果（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命令之前，发卡行脚本失败 ● 最后一个生成应用密文命令之后，发卡行脚本失败 JR/T 0025 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
交易状态信息（TSI）	TSI 中包括一个表明执行发卡行脚本处理标记

17.3 发卡行脚本操作中的密钥管理

发卡行脚本操作中的密钥包含：安全报文鉴别密钥和安全报文加密密钥。详见JR/T 0025.7中描述。

图21是安全报文鉴别（MAC）密钥的生成和使用。

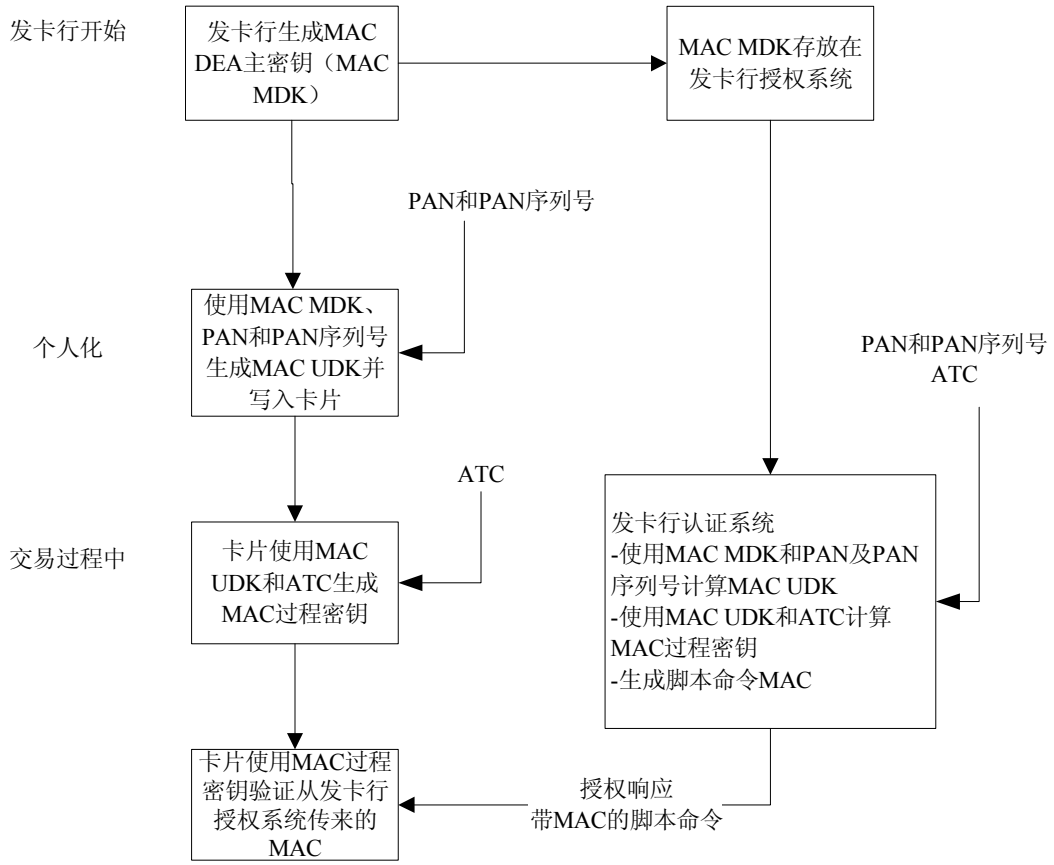


图21　MAC 密钥的生成和使用

图22是安全报文加密密钥的生成和使用。

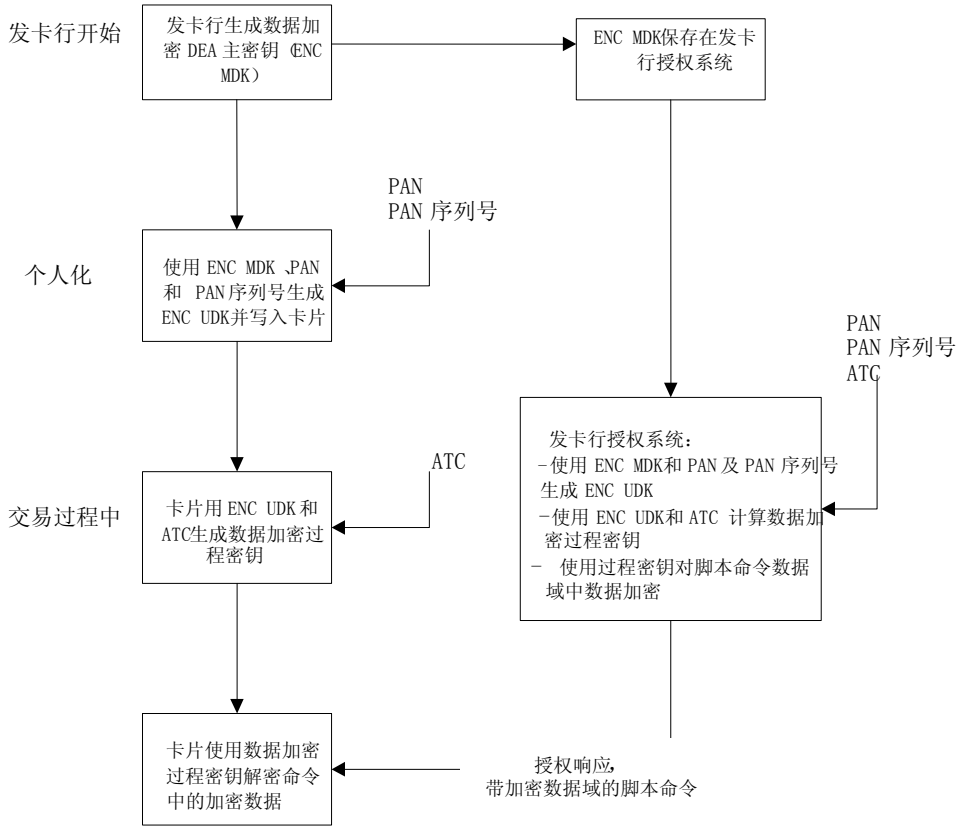


图22　安全报文加密密钥的生成和使用

17.4　认证响应数据

表44列出的是授权响应中发卡行脚本数据。

表44　发卡行脚本处理——联机响应数据

数据元	描述
发卡行脚本模板	JR/T 0025 规范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 2 次生成应用密文命令后，传送给卡片的发卡行专有脚本数据
发卡行脚本标识符	发卡行用来唯一标识发卡行脚本
发卡行脚本命令	脚本中的每一个发卡行脚本命令都按照 BER-TLV 格式，用标签“86”开始

17.5　命令

下面列出的功能是发卡行脚本处理过程中可以执行的功能。推荐使用发卡行脚本命令处理这些功能。命令的编码在附录B。

除了卡片锁定命令，所有命令处理的都是当前选择应用。

应用锁定

如果发卡行决定当前使用的应用无效，执行应用锁定功能。此时锁定的应用可以在后面由发卡行解锁。

使用应用锁定（APPLICATION BLOCK）命令锁应用。应用锁定后，和应用有关的文件状态指示器要指明应用已经锁定。即使应用锁定，卡片内部数据访问仍然有效。一个锁定的应用，卡片对生成应用密文命令总是返回AAC。

如果应用在交易过程中锁定，卡片和终端允许交易继续执行到结束处理步骤。但是在后续交易时，卡片不允许锁定的应用被选择进行金融交易【终端可能选择一个锁定的应用进行解锁，因此卡片应对生成应用密文（GENERATE AC）命令响应AAC】。

应用解锁

应用解锁解除了应用的锁定状态。应用解锁要在发卡行指定的特殊设备上执行。

因为应用解锁要在特殊设备上执行。处理流程不需要采用正常授权或金融交易的处理规则。在卡片对第1个生成应用密文（GENERATE AC）命令响应AAC后，设备要能将交易联机上送。即使卡片支持发卡行认证，也不需要执行。卡片风险管理和终端风险管理都不是应进行的。也不需要第2个生成应用密文（GENERATE AC）命令【如果由于一些原因，卡片在第2个生成应用密文（GENERATE AC）命令发送之前解锁了，设备要将响应的密文当AAC处理】。

卡片锁定

卡片锁定（CARD BLOCK）命令是一个二次发卡命令，使得卡片上的所有应用永久失效。

卡片锁定命令使卡片上所有应用无效而且实行卡片下电。除非卡片锁定，支付系统环境（PSE）不会无效而且总是可以访问。

如果卡片在交易处理过程中锁定，卡片和终端允许交易继续进行到交易结束步骤。一个锁定的卡片不能用发卡行脚本命令或其它命令解锁，因此卡片已经失效。此时PSE也无效。卡片对选择命令响应“功能不支持”（SW1 SW2=“6A81”）。卡片也不允许任何其它形式的应用选择。

当发卡行决定对卡片禁止使用任何功能，执行卡片锁定。例如丢失或被偷窃的卡片。在卡片锁定后，卡片上的应用都不能被解锁。

发卡行脚本中的卡片锁定命令用来实现锁卡功能。

PIN修改/解锁

PIN修改/解锁（PIN CHANGE/UNBLOCK）命令用来对PIN解锁或解锁加同时修改PIN值，卡片通过重新设置PIN尝试计数器到最大值（PIN尝试限制数）实现PIN解锁。

——PIN 解锁；

——PIN 修改/解锁命令执行成功，PIN 尝试计数器复位成 PIN 尝试限制数；

——修改 PIN 值；

——如果要修改 PIN 值，PIN 数据要用对称算法加密。算法描述在 17.6.3 中描述。当 PIN 值修改时，PIN 的尝试次数计数器自动复位成 PIN 尝试限制数；

——修改 PIN 值应在一个发卡行控制的安全环境中执行。

设置数据

卡片中的专有基本数据对象允许使用设置数据（PUT DATA）命令修改。只有有标签的基本数据对象才允许使用此命令修改。

在本部分中，下列数据可以使用设置数据（PUT DATA）命令修改，这些数据放在卡片内部专有文件中：

——连续脱机交易上限（“9F59”）；

——连续脱机交易下限（“9F58”）；

——连续脱机交易限制数（国际-国家）；

——连续脱机交易限制数（国际-货币）；

——累计脱机交易金额限制数；

——累计脱机交易金额限制数（双货币）；

——累计脱机交易金额上限；

——货币转换因子。

JR/T 0025定义的连续脱机交易上限（“9F14”）和连续脱机交易下限（“9F23”）存在短文件标识符SFI1-10之间，使用发卡行脚本命令中的修改记录（UPDATE RECORD）命令修改。

修改记录

修改记录（UPDATE RECORD）命令用来修改文件中的一条记录内容，修改的内容在修改记录（UPDATE RECORD）命令的数据域中。

17.6 处理流程

17.6.1 授权响应报文

授权响应报文中的标签“72”表明，在第2个生成应用密文（GENERATE AC）命令后，执行发卡行脚本处理。一个脚本中可以包含多个命令。

附录B中定义了发卡行脚本命令的编码。

有用来修改、复位卡片内容的命令都应包括安全报文，见17.6.3。

17.6.2 卡片脚本处理

因为卡片不能识别命令是发卡行脚本命令还是其它命令，因此，卡片不能拒绝在第2个生成应用密文（GENERATE AC）命令之前送来的命令。

17.6.4中描述了卡片中JR/T 0025专有的指示位，记录在第2个生成应用密文（GENERATE AC）命令之后收到的发卡行脚本命令执行情况。

17.6.3 卡片安全报文

在执行一个发卡行脚本命令之前，卡片使用安全报文认证发卡行。在脚本处理时不进行联机处理中描述的发卡行认证方法。

安全规范中描述了安全报文的执行方法。

使用安全报文的基本目的是保证数据的机密性、信息完整性和认证发卡行。信息完整和鉴别发卡行可以使用MAC，数据机密通过加密数据实现，例如PIN加密。

——报文鉴别（MACing）

报文鉴别（MACing）用来认证发卡行是发卡行脚本命令的合法发出方，并且保证命令在发出后没有被修改；

MAC 用命令中的所有数据计算而成，包括命令头。先进行数据加密（如果需要）后生成 MAC。

——数据加密

数据加密用来保证命令中的明文数据的机密性。在生成命令的 MAC 之前进行。发卡行和卡片中的应用都要知道数据加密方法。

MAC生成和数据加密的描述见附录C。

17.6.4 结果指示器

卡片使用发卡行脚本命令计数器记录第2个生成应用密文（GENERATE AC）命令后收到的有安全报文的命令个数。

在卡片处理第2个生成应用密文（GENERATE AC）命令后收到的命令时，如果下面列出的错误出现一种，卡片设置发卡行脚本失败指示位为“1”：

——需要安全报文但是没有提供；

——安全报文验证失败；

——安全报文通过但是命令执行失败。

不需要安全报文的命令执行失败时，不设置指示位。

17.6.5 流程图

图23是卡片在发卡行脚本处理过程中，卡片处理每个命令的流程。

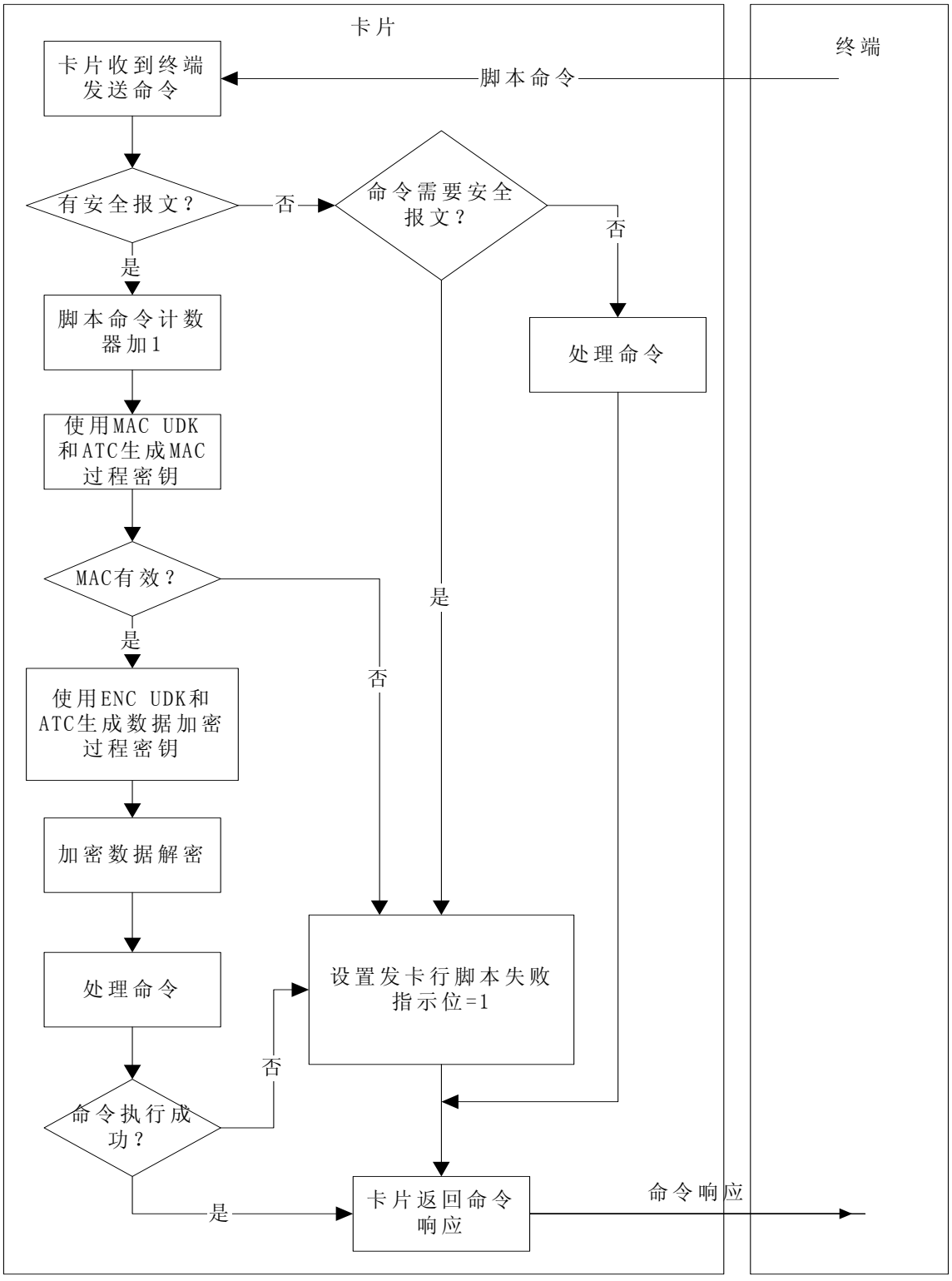


图23　发卡行脚本处理流程图

17.7　前期相关处理

联机操作

终端收到的联机响应中可以包括发卡行脚本。

交易结束

如果终端收到的联机响应中包括发卡行脚本，在交易结束处理后，执行发卡行脚本处理。

17.8 后续相关处理

卡片行为分析（后续应用）

在下次交易的卡片行为分析阶段：

——卡片设置 CVR 中第 4 字节第 8-5 位值为发卡行脚本命令计数器的值；

——如果发卡行脚本失败指示位为“1”，卡片设置 CVR 中“上次交易发卡行脚本处理失败”位为“1”。

交易结束（后续应用）

一个联机交易以后，如果下列条件满足一条，发卡行脚本失败指示位和发卡行脚本计数器复位成“0”：

——发卡行认证成功；

——发卡行认证可选并且没有执行；

——发卡行认证不支持。

18 卡片记录交易明细

在卡片风险分析和交易结束这两个处理过程中，当卡片决定接受交易返回TC之前，卡片要进行记录交易明细步骤。

18.1 交易明细记录文件

交易明细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日志入口数据元（标签“9F4D”）中规定，交易明细记录文件的短文件标识符取值范围应在11-30之间，JR/T 0025推荐值为11，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。

记录内容由日志格式（标签“9F4F”）决定。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）命令取得日志格式数据元，可知交易明细记录文件需要记录的内容。

日志格式和交易日志记录在应用锁定后仍可以访问。

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日志入口数据元。如果日志入口数据元不存在，应用不支持交易日志功能；

——发送一个取数据（GET DATA）命令取得日志格式数据元；

——发送读记录（READ RECORD）命令读交易日志记录。交易明细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。

18.2 JR/T 0025 建议

日志入口数据元内容：“0B0A”，交易明细文件的SFI为11，记录个数为10个。

日志格式数据元内容是下表定义的数据对象的标识和长度。

交易明细记录的内容在表45中列出。

表45 交易明细记录文件内容

数据	标签	长度（字节）
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6
其它金额	9F03	6
终端国家代码	9F1A	2

数据	标签	长度（字节）
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

在应用选择阶段，卡片对选择（SELECT）命令的响应信息中的发卡行自定义数据中包含了日志入口数据元，还在PDOL数据元中，列出了需要终端输入的数据。则在下一条获取处理选项（GPO）指令中，终端要把PDOL中列出的终端数据元送给卡片，卡片将这些数据保存起来。在卡片经过卡片风险管理或交易结束处理，做出接受交易的结论后，卡片将根据日志格式中规定的交易明细内容一起保存到交易明细文件中。

交易明细文件中的终端数据元，终端可以通过PDOL或CDOL将这些数据传入卡片。

如果发卡行发卡时没有建立交易明细文件，但是在选择应用的响应中包含了日志入口数据元，则卡片仍然不能记录交易明细。

只有当上一条生成应用密文（GENERATE AC）命令中，卡片响应TC的前提下，卡片才进行记录交易明细的处理。一次交易最多记录一次交易明细。

附 录 A
（规范性附录）
卡片和发卡行数据元表

A.1 卡片和发卡行数据元描述

表A.1中列出了JR/T 0025所用的卡片和发卡行数据元，包括的格式有：格式（F）、标签（T）和长度（L）。

支持的格式有：

——n（数字型）；

——cn（压缩数字型）；

——b（二进制）；

——an（字母数字）；

——ans（特殊字母数字）。

当数据定义的长度超过数据实际长度，而位数没有占满时，补位规则如下：

——格式 n 的数据元右对齐，左补 0；

——格式 cn 的数据元左对齐，右补 F；

——格式 an 的数据元左对齐，右补 0；

——格式 ans 的数据元左对齐，右补 0。

需求列中列出的是对数据元的需求情况：

——M（必备）：此数据应存在并提供给终端，终端在读应用数据过程中，如果没有读到必备数据，终端中止交易；

——R（需求）：数据应存在，在读应用数据过程中，终端不检查；

——C（有条件）：在一定条件下应存在；

——O（可选）：可选数据元。

表 A.1 卡片和终端的数据元描述

名字（格式、标签和长度）	需求	描述	值
应用密文（AC） F：b64 T：9F26 L：8	R	生成应用密文命令返回的密文	
应用货币代码 F：n3 T：9F42 L：2	C 如果 CVM 中要求金额检查，需要此数据。	按 GB/T 12406 编码	
应用货币代码 F：n3 T：9F51 L：2	C 如果执行频度检查	JR/T 0025 专有数据。按 GB/T 12406 编码	
应用货币指数 F：n1	O	指出金额数据中小数点从最右边开始第几个位置	

名字（格式、标签和长度）	需求	描述	值
T：9F44 L：1			
应用缺省行为 （ADA） F：b16 T：9F52 L：2	C 如果支持发卡行认证。JR/T 0025专有数据。	定义在一些特定条件下卡片执行的发卡行指定的行为。如果卡片中没有此数据，缺省认为全零	字节1： 位8：1=如果发卡行认证失败，下次联机交易 位7：1=如果发卡行认证执行但失败，拒绝交易 位6：1=如果发卡行认证必备但没有收到ARPC，拒绝交易 位5：1=如果交易拒绝，生成通知 位4：1=如果PIN在本次交易中尝试次数超限而且交易拒绝，生成通知 位3：1=如果因为发卡行认证失败或没有执行导致交易拒绝，生成通知 位2：1=如果是新卡，联机交易 位1：1=如果是新卡，当交易无法联机时拒绝交易 字节2： 位8：1=如果PIN在本次交易中尝试次数超限，应用锁定 位7：1=如果PIN在前次交易中尝试次数超限，拒绝交易 位6：1=如果PIN在前次交易中尝试次数超限定，联机交易 位5：1=如果PIN在前次交易中尝试次数超限，当交易无法联机时拒绝交易 位4：1=如果发卡行脚本命令在前次交易中失败，联机交易 位3：1=如果PIN在前次交易中尝试次数超限，拒绝交易并锁应用 位2－1：RFU（000）
应用自定义数据 F：b8－256 T：9F05 L：1－32	O	和卡片应用有关的发卡行指定数据	
应用生效日期 F：n6 YYMMDD T：5F25 L：3	O	卡片中应用启用日期	
应用失效日期 F：n6 YYMMDD T：5F24 L：3	M	卡片中应用的失效日期	

名字（格式、标签和长度）	需求	描述	值
应用文件定位器（AFL） F：var. T：94 L：var.最大 252	R	指出和应用相关的数据存放位置（短文件标识符和记录号）	对于每一个要读的文件，AFL 包括 4 个字节： 字节 1： 位 8－4=SFI 短文件标识符 位 3－1=000 字节 2：文件中要读的第 1 个记录的记录号（不能为 0） 字节 3：文件中要读的最后一个记录的记录号（等于或大于字节 2） 字节 4：从字节 2 中的记录号开始，存放认证用静态数据记录的个数（值从 0 到字节 3-字节 2+1 的值）
应用标识符（AID） F：b40－128 T：4F L：5－16	R	按 GB/T 16649.5 规定标识应用。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	
应用交互特征（AIP） F：b16 T：82 L：2	M	一个列表，说明此应用中卡片支持指定功能的能力	字节 1： 位 8：1=RFU 位 7：1=支持 SDA 位 6：1=支持 DDA 位 5：1=支持持卡人认证 位 4：1=执行终端风险管理 位 3：1=支持发卡行认证 位 2：RFU（0） 位 1：1=支持 CDA 字节 2：RFU（“00”）
应用标签 F：ans1－16 T：50 L：1－16	R （EMV 规定将要成为必备数据）	和 AID 相关的便于记忆的数据。 用于应用选择。存在于 ADF 的 FCI 中（可选）和 ADF 目录入口中（必备）	
应用首选名称 F：ans1－16 T：9F12 L：1－16	O	和 AID 相关的便于记忆的数据。如果终端支持在发卡行代码表索引数据中指定的字符类型，终端在应用选择过程中显示应用首选名称	
应用主账号（PAN） F：var.最大 cn19 T：5A L：var.最大 10	M	持卡人有效账号	
应用主账号序列号	O	用来表示卡片中使用同一	

名字（格式、标签和长度）	需求	描述	值
F：n2 T：5F34 L：1		个账号的不同应用	
应用优先指示器 F：b8 T：87 L：1	C	如果卡片中有多个应用，指出同一目录中的应用的优先级	位 8 1：没有持卡人确认应用不能选择 0：没有持卡人确认应用可以选择 位 7-5：RFU（000） 位 4-1： 0000：不指定优先级 xxxx：应用显示和选择的顺序，从 1-15.1 的优先级最高
应用模板 F：b T：61 L：var. 最大 252	C 如果有 PSE	按 GB/T 16649.5 的规定，包含和应用目录入口相关的 1 个或多个数据对象	
应用交易计数器 F：b 16 T：9F36 L：2.	R	记录个人化以后交易处理的次数。由卡片中的应用维护	初始值为 0，执行一次交易加 1
应用用途控制 F：b 16 T：9F07 L：2	O	标明发卡行指定的卡片应用上的一些限制，包括地域使用和服务类型等。	字节 1： 位 8：1=国内现金交易有效 位 7：1=国际现金交易有效 位 6：1=国内商品有效 位 5：1=国际商品有效 位 4：1=国内服务有效 位 3：1=国际服务有效 位 2：1=ATM 有效 位 1：1=除 ATM 外的终端有效 字节 2： 位 8：1=允许国内返现 位 7：1=允许国际返现 位 6－1：RFU（000000） JR/T 0025 限制：字节 1 中，位 4，6 值相同；位 3，5 值相同
应用版本号 F：b16 T：9F08 L：2	M	支付系统给应用分配的版本号	
授权响应码 F：an2 T：8A	来自发卡行或终端	标明了交易结果	发卡行生成的代码，按 GB/T 15150 标准 下面的代码由终端生成： Y1：脱机接受

名字（格式、标签和长度）	需求	描述	值
L：2			Z1：脱机拒绝 Y3：不能联机（脱机接受） Z3：不能联机（脱机拒绝）
卡片风险管理数据对象列表 1（CDOL1） F：b T：8C L：var. 最大 252	M	列出第 1 个生成应用密文命令中，卡片请求终端传送的数据。 内容是终端数据对象（标签和长度）	
卡片风险管理数据对象列表 2（CDOL2） F：b T：8D L：var. 最大 252	M	列出第 2 个生成应用密文命令中，卡片请求终端传送的数据。 内容是终端数据对象（标签和长度）	
卡片验证结果（CVR） F：b32 T：- L：4.	M	JR/T 0025 专有数据。记录卡片在本次和上次交易中出现的异常情况。要作为发卡行应用数据的一部分返回给终端	字节 1： 长度字节 03 字节 2： 位 8－7： 00=第 2 个 GENERATE AC 返回 AAC 01=第 2 个 GENERATE AC 返回 TC 10=不请求第 2 个 GENERATE AC 11=RFU 位 6－5： 00=第 1 个 GENERATE AC 返回 AAC 01=第 1 个 GENERATE AC 返回 TC 10=第 1 个 GENERATE AC 返回 ARQC 11=不能返回 11 位 4：1=发卡行认证执行但失败 位 3：1 =脱机 PIN 执行 位 2：1=脱机 PIN 认证失败 位 1：1 =不能联机 字节 3： 位 8：1=上次联机交易没有完成 位 7：1=PIN 锁定 位 6：1=超过频率检查 位 5：1=新卡 位 4：1=上次联机交易发卡行认证失败 位 3：1=联机授权后，发卡行认证没有执行 位 2：1=由于 PIN 锁卡片锁定应用 位 1：1=上次交易 SDA 失败交易拒绝 字节 4： 位 8－5：上次交易第 2 个生成应用密文（GENERATE AC）命令后收到的带有安全报文的发卡行脚本命

名字（格式、标签和长度）	需求	描述	值
			令 位 4：1 =上次交易发卡行脚本处理失败指针 位 3：1=上次交易 DDA 失败交易拒绝 位 2：1 =DDA 执行 位 1：RFU（0） 在应用初始化时，字节 2-4 置零
持卡人姓名 F：ans2－26 T：5F20 L：2－26	R	持卡人姓名,按GB/T 17552的规定	
持卡人姓名扩展 F：ans 1－19 T：9F0B L：1-19	O	如果持卡人姓名大于26字节，多出部分放在此数据元中。按 GB/T 17552 的规定	
持卡人证件号 F：an40 T：9F61 L：1-40	O	持卡人证件号	
持卡人证件类型 F：cn1 T：9F62 L：1	O	表明持卡人证件类型	00：身份证 01：军官证 02：护照 03：入境证 04：临时身份证 05：其它
持卡人验证方法（CVM）列表 F：b T：8E L：var.最大 252	R	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注：一个应用中可以有多个 CVM 列表，例如一个用于国内交易，一个用于国际交易	字节 1－4：金额 X（二进制） 字节 5－8：金额 Y（二进制） 字节 9（CVM Code）： 位 8：0=只有符合此规范的取值（如果为 1，说明有自定义的值） 位 7： 1=如果此 CVM 失败，应用后续的 0 = 如果此 CVM 失败，则持卡人验证失败 位 6－1（CVM Type）： 000000=CVM 失败处理 000001=卡片执行明文 PIN 核对 000010=联机加密 PIN 验证 000011=卡片执行明文 PIN 核对+签名（纸上） 000100=保留 000101=保留 011110=签名（纸上） 011111=无需 CVM

名字（格式、标签和长度）	需求	描述	值
			000110－011101=保留给加入的支付系统 100000－101111=保留给各自独立的支付系统 110000－111110=保留给发卡行 111111=RFU JR/T0025 定义： 100000 =持卡人证件出示 字节 10（CVM Condition Code）： 00=总是 01=如果是 ATM 现金交易 02=如果不是 ATM 现金或有人值守现金或返现交易 03=如果终端支持这个 CVM 04=如果是人工值守现金交易 05=如果是返现交易 06=如果交易货币等于应用货币代码而且小于 X 值 07=如果交易货币等于应用货币代码而且大于 X 值 08 =如果交易货币等于应用货币代码而且小于 Y 值 09=如果交易货币等于应用货币代码而且大于 Y 值 0A－7F：RFU 80－FF：RFU 保留给各个支付系统 下一个 CVM 用另两个 CVM 码和 CVM 条件字节表示
CA 公钥索引（PKI） F： b8 T： 8F L： 1	C 如果支持 SDA 或 DDA	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥	
连续脱机交易计数器（国际-货币） F： b8 T： － L： 1	C 如果执行国际-货币频度检查	JR/T 0025 专有数据元。记录自从上次联机后，不使用指定应用货币的脱机交易次数	初始值为 0，每接受一次国际-货币交易脱机后加 1
连续脱机交易限制数（国际-货币） F： b8 T： 9F53 L： 1	C 如果执行国际-货币频度检查	JR/T 0025 专有数据元。不使用指定应用货币的连续脱机交易次数最大数，超过后交易请求联机	
连续脱机交易计数器（国际-国家）	C 如果执行国际-	JR/T 0025 专有数据元。记录自从上次联机后，不在	初始值为 0，每接受一次国际-国家交易脱机后加 1

名字（格式、标签和长度）	需求	描述	值
F： b8 T： - L： 1	国家频度检查	发卡行所在国家内进行的脱机交易次数	
连续脱机交易限制数（国际-国家） F： b8 T： 9F72 L： 1	C 如果执行国际-国家频度检查	JR/T 0025 专有数据元。不在发卡行所在国家的连续脱机交易次数最大数，超过后交易请求联机	
密文信息数据 F： b8 T： 9F27 L： 1	R	表明卡片返回的密文类型并指出终端要进行的操作	位 8－7： 00=AAC 01=TC 10=ARQC 11=AAR （JR/T 0025 不支持） 位 6－5：RFU（00） 位 4：1=需要通知 位 3－1（原因/通知/授权参考码）： 000=无信息 001 = 不允许服务 010=PIN 尝试次数超过 011=发卡行认证失败 xxx = RFU
密文版本号 F： n2 T： - L： 1	R	JR/T 0025 专有数据。标明生成密文的算法版本。作为发卡行应用数据的一部分传送	JR/T 0025 指定密文版本号 01（‘01’）
累计脱机交易金额 F： n12 T： - L： 6	C 如果执行累计金额频度检查	JR/T 0025 专有数据。记录自从上次联机交易完成后，使用应用指定货币的脱机交易累计金额	初始值为 0。累加每次使用应用指定货币的脱机交易的授权金额。在某些联机交易后可以被复位成零
累计脱机交易金额限制数 F： n12 T： 9F54 L： 6	C 如果执行累计金额频度检查	JR/T 0025 专有数据。累计脱机交易金额的最大限制。超过交易请求联机	
累计脱机交易金额（双货币） F： n12 T： - L： 6	C 如果执行累计金额（双货币）频度检查	JR/T 0025 专有数据。记录自从上次联机交易完成后，使用应用指定货币和第 2 应用货币的脱机交易累计金额	初始值为 0。累加每次使用应用指定货币或第 2 应用货币的脱机交易的授权金额。在某些联机交易后可以被复位成零
累计脱机交易金额限制数（双货币） F： n12	C 如果执行累计金额（双货币）频	JR/T 0025 专有数据。累计脱机交易金额（双货币）的最大限制。超过交易请	

名字（格式、标签和长度）	需求	描述	值
T： 9F75 L： 6	度检查	求联机	
累计脱机交易金额上限 F： n 12 T： 9F5C L： 6	C 如果执行累计金额频度检查	JR/T 0025 专有数据。累计脱机交易金额和累计脱机交易金额（双货币）的最大限制数。如果超过而且交易无法联机时，拒绝交易	
货币转换因子 F： 8n T： 9F73 L： 4	C 如果执行双货币频度检查	用来将第 2 应用货币转换成指定应用货币的10进制数	字节 1 位 8-5：小数点位置。从右边开始移动的位数 位 4-1：转换因子的第 1 个数字 字节 2-4：剩下的 6 个数字
数据认证码 F： b 16 T： 9F45 L： 2	O	发卡行指定数值。在 SDA 过程中，终端从签名的静态应用数据中恢复出来。作为签名的静态应用数据保存在卡片中	
安全报文加密密钥 F： b 128 T： - L： 16	C 如果执行修改 PIN	JR/T 0025 自定义数据元。双长度的安全报文加密密钥，16 字节。发卡行脚本命令中的数据域需要加密时使用	
专用文件（DF）名称 F： b 40－128 T： 84 L： 5－16	R	按 ISO 7816-4 规定的，DF 的名字	
分散密钥索引（DKI） F： b 8 T： - L： 1	O	JR/T 0025 专有数据。发卡行用来明确使用哪个主密钥分散得到卡片中的子密钥。用于卡片联机处理和发卡行认证。在发卡行应用数据中返回给终端	发卡行指定。 如果不存在，缺省值为 0
目录数据文件（DDF）名称 F： b 40－128 T： 9D L： 5－16	C 如果支持目录选择	标识目录名	
目录自定义模板 F： var. T： 73 L： var. 最大 252	O	按 GB/T 16649.5，目录中发卡行自定义部分	

名字（格式、标签和长度）	需求	描述	值
动态数据认证数据对象列表（DDOL） F： b T： 9F49 L： var. 最大 252	C 如果支持 DDA	在内部认证命令中需要终端送到卡片中的数据列表，包括数据对象的标签和长度	
动态数据认证(DDA)失败指示位 F： b 1 T： - L： -	C 如果支持 DDA	JR/T 0025 专有数据。标明当上次交易拒绝时 DDA 是否失败	位 1：1=上次交易 DDA 失败而且交易拒绝
文件控制信息(FCI)发卡行自定义数据 F： var. T： BF0C L： var. 最大 222	O	FCI 中的发卡行自定义部分	
文件控制信息(FCI)专用模板 F： var. T： A5 L： var.	R	按 ISO 7816-4，标识 FCI 模板中，专用于 JR/T 0025 的数据对象	
文件控制信息(FCI)模板 F： var. T： 6F L： var.最大 252	R	按 ISO 7816-4，标识 FCI 模板	
IC 卡动态数据 F： - T： - L： var.	C 如果支持 DDA	IC 卡生成或保存的动态数据。在签名的动态应用数据中传送给终端。终端用来证明脱机动态数据认证执行了	
IC 动态数 F： b T： 9F4C L： 2－8	C 如果支持 DDA	DDA 处理过程中，卡片生成的随时间变化不同的随机数。包括在签名动态数据中送到终端，由终端恢复	
IC 卡私钥 F： b T： - L： N_{IC}	C 如果支持 DDA	IC 卡公私钥对中的私钥部分。用于脱机动态数据认证。有两种格式：模/私钥指数形式和中国余数定理（CRT）形式	
IC 卡公钥指数 F： b	C 如果支持 DDA	IC 卡公钥指数用于验证签名的动态应用数据	

名字（格式、标签和长度）	需求	描述	值
T： 9F47 L： 1 or 3			
IC 卡公钥证书 F： b T： 9F46 L： N_I	C 如果支持 DDA	发卡行认证过的 IC 卡公钥	
IC 卡公钥余数 F： b T： 9F48 L： $N_{IC} - N_i + 42$	C 如果需要	没有放入 IC 卡公钥证书的 IC 卡公钥部分	
发卡行行为代码（IAC）-缺省 F： b40 T： 9F0D L： 5	R 将变成必备	指定当交易请求联机但是终端不能完成联机上送的交易拒绝的条件	值和终端验证结果（TVR）中的每一位对应
发卡行行为代码（IAC）-拒绝 F： b40 T： 9F0E L： 5	R 将变成必备	指定交易不进行联机直接拒绝的条件	值和终端验证结果（TVR）中的每一位对应
发卡行行为代码（IAC）-联机 F： b40 T： 9F0F L： 5	R 将变成必备	指定交易联机上送的条件	值和终端验证结果（TVR）中的每一位对应
发卡行应用数据 F： b T： 9F10 L： var. 最大 32	R	在一个联机交易中，要传送到发卡行的专有应用数据。 第 1 字节是 JR/T 0025 自定义数据长度。 格式内容： 长度（07）（1 字节） 分散密钥索引（1 字节） 密文版本号（1 字节） 卡片验证结果（CVR）（4 字节） 算法标识（1 字节） 如果有发卡行自定义数据。在上述数据后跟一个发卡行自定义数据长度字节和 1-15 字节的发卡行自	

名字（格式、标签和长度）	需求	描述	值
		定义数据	
发卡行认证数据 F： b64－128 T： 91 L： 8－16	O	用于发卡行认证的数据，从发卡行传来由终端送入卡片。 JR/T 0025 中，发卡行认证数据包括两部分： ARPC（8 字节） 授权响应码（2 字节）	
发卡行认证失败指示位 F：b1 T： － L： －	C 如果支持发卡行认证	JR/T 0025 专有数据元。表明上次交易出现的发卡行认证错误的情况。有： 发卡行认证执行但失败 发卡行认证没有执行但是必备	位 1：1 =上次联机交易发卡行验证失败
发卡行认证指示位 F： b8 T： 9F56 L： －1	C 如果支持发卡行认证	JR/T 0025 专有数据。标明当支持发卡行认证时，是必备还是可选	位 8： 1=发卡行认证必备 0=发卡行认证可选 位 7－1：RFU （0000000）
发卡行代码表索引 F： n2 T：9F11 L：1	C 如果有应用首选名称	按 ISO/IEC 8859，显示应用首选名称的代码表	01 = ISO/IEC 8859-1 02 = ISO/IEC 8859-2 03 = ISO/IEC 8859-3 04 = ISO/IEC 8859-4 05 = ISO/IEC 8859-5 06 = ISO/IEC 8859-6 07 = ISO/IEC 8859-7 08 = ISO/IEC 8859-8 09 = ISO/IEC 8859-9 10 = ISO/IEC 8859-10
发卡行国家代码 F： n 3 T： 5F28 L： 2	C 如果有应用用途控制	按 GB/T 2659 指出发卡行的国家	
发卡行国家代码 F： n3 T： 9F57 L： 2	C 如果支持卡片频度检查	JR/T 0025 专有数据。按 GB/T 2659指出发卡行的国家	
发卡行公钥证书 F： b T： 90 L： N_{CA}	C 如果支持 SDA，DDA	CA 认证过的发卡行公钥。用于脱机数据认证	
发卡行公钥指数	C	发卡行公钥指数，用来验	

名字（格式、标签和长度）	需求	描述	值
F： b T： 9F32 L： 1 或 3	如果支持 SDA，DDA	证签名的静态应用数据和 IC 卡公钥证书	
发卡行公钥余数 F： b T： 92 L： $N_I-N_{CA}+36$	C 如果需要	没有放入发卡行公钥证书中的发卡行公钥部分	
发卡行脚本命令 F： b T： 86 L： var 最大 261	O	从发卡行到终端，由终端送入卡片。包括在授权响应中的发卡行脚本中。见附录 B 中的命令描述	见附录 B
发卡行脚本命令计数器 F： b4 T： - L： -	C 如果支持发卡行脚本	JR/T 0025 专有数据。记录上次交易中，卡片处理的带安全报文的发卡行脚本命令个数	位 4－1：第 2 个生成应用密文命令后收到的有安全报文的脚本命令个数 值‘F’表示有 15 个或更多的发卡行脚本命令
发卡行脚本失败指示位 F： b1 T： - L： -	C 如果支持发卡行脚本	JR/T 0025 专有数据。当上次交易发卡行脚本处理失败时设置	位 1：上次交易发卡行脚本处理失败
发卡行脚本模板 2 F： b T： 72 L： var.	C 如果支持发卡行脚本	最后的生成应用密文命令后，包括发送到卡片的发卡行专用数据	
发卡行 URL F： ans T： 5F50 L： var.	O	存放发卡行服务器在互联网上的位置	
发卡行 URL2 F： ans T： 9F5A L： var.	O	JR/T 0025 定义的。存放发卡行服务器在互联网上的位置	
首选语言 F： an2 T： 5F2D L： 2－8	O	顺序存放的 1-4 种语言。根据 GB/T 4880.1 编码	
上次联机应用交易计数器（ATC）寄存器 F： b16	C 如果卡片或终端执行频度检查或新卡检查	上次联机上送交易时的 ATC 值	初始值为 0

名字（格式、标签和长度）	需求	描述	值
T： 9F13 L： 2			
日志入口 F： b16 T： 9F4D L： 2	O	提供日志文件的 SFI 和日志文件记录个数	字节 1： 循环交易日志文件的 SFI 字节 2： 交易日志文件中的记录个数
日志格式 F： b T： 9F4F L： var.	O	列出日志记录中数据对象的标签和长度	
连续脱机交易下限 F： b8 T： 9F14 L： 1	C 如果执行终端频度检查	发卡行指定的有联机能力的终端允许连续脱机交易的最大次数	
连续脱机交易下限 F： b8 T： 9F58 L： 1	C 如果执行卡片频度检查	JR/T 0025 专有数据。发卡行指定的有联机能力的终端允许连续脱机交易的最大次数	
安全报文鉴别(MAC)密钥 F： b128 T： - L： 16	C 如果支持发卡行脚本使用安全报文	JR/T 0025 专有数据。双长度安全报文鉴别（MAC）密钥，16 字节。当发卡行脚本需要安全报文时用来计算 MAC	
卡片请求脱机拒绝指示位 F： b1 T： - L： -	C 如果卡片风险管理检查允许得出拒绝结论	JR/T 0025 专有数据。在交易处理过程中，当卡片决定交易拒绝时设置	
联机授权指示位 F： b1 T： - L： -	C 如果卡片支持发卡行授权或发卡行脚本处理	JR/T 0025 专有数据。如果卡片请求 ARQC 但是终端不能完成时设置	位 1：1 =本次或上次交易中，需要联机授权但是没有实现
卡片请求联机指示位 F： b1 T： - L： -	R	JR/T 0025 专有数据。在交易处理过程中，当卡片决定交易联机时设置	
PIN 尝试计数器 F： b8 T： 9F17 L： 1	C 如果支持脱机 PIN	剩余的 PIN 尝试次数	初始值为 PIN 尝试限制数。验证失败一次减 1。验证成功或发卡行修改/解锁成功则复位到最大值（PIN 尝试限制数）

名字（格式、标签和长度）	需求	描述	值
PIN 尝试限制数 F： b8 T： - L： 1	C 如果支持脱机 PIN	JR/T 0025 自定义数据。发卡行指定的 PIN 允许的连续错误次数	
处理选项数据对象列表（PDOL） F： b T： 9F38 L： var.	C 在终端进行应用初始化时需要	指定在取处理选项命令中终端送入卡片的数据。包括终端数据对象（标签和长度）	
扩展的专用应用标识符（PIX） F： b T： - L： 0－11	R	按 GB/T 16649.5 规定的，AID 的组成部分之一	
脱机 PIN F： b T： - L： 8	C 如果支持脱机 PIN	JR/T 0025 专有数据。在卡片个人化时由发卡行写入卡片	
注册的应用提供商标识（RID） F： b T： - L： 5	R	按 GB/T 16649.5 规定的，AID 的组成部分之一	
响应报文模板格式 1 F： var. T： 80 L： var.	R	IC 卡命令响应信息，包括数据对象（不包括标签和长度）	
响应报文模板格式 2 F： var. T： 77 L： var.	C 如果支持 CDA	IC 卡命令响应信息，包括数据对象（包括标签和长度）	
第 2 应用货币 F： n3 T： 9F76 L： 2	C 如果支持双货币频度检查。	第 2 种货币，要转换成应用指定货币。按 GB/T 12406 编码	
服务码 F： n3 T： 5F30 L： 2	O	按 GB/T 17552 的规定，和在磁条 1 和 2 中定义的数据一致	

名字（格式、标签和长度）	需求	描述	值
短文件标识符(SFI) F： b 8 T： 88 L： 1	R	命令中用于标识文件。字节中高三位为 0	1－10：JR/T 0025 定义 11－20：支付系统定义 21－30：发卡行定义
签名的动态应用数据 F： b T： 9F4B L： N_{IC}	C 如果支持 DDA	卡片生成的动态数据签名。在 DDA 过程中由终端验证	
签名的静态应用数据（SAD） F： b T： 93 L： N_I	C 如果支持 SDA	发卡行签名的数据签名。用卡片内的指定数据生成。在 SDA 过程中由终端验证	
静态数据认证(SDA)失败指针 F： b1 T： - L： -	C 如果支持 SDA	JR/T 0025 专有数据。标明当上次交易拒绝时 SDA 是否失败	位 1： 1 =上次交易 SDA 失败而且交易拒绝
静态数据认证标签列表 F： - T： 9F4A L： var.	C	列出基本数据对象标签，标签的值包括在签名的静态应用数据中或 IC 卡公钥证书中	可以只包括应用交互特征（AIP）的标签
磁条 1 自定义数据 F： ans T： 9F1F L： var.	R 将会改为可选	按 GB/T 17552 的规定，磁条 1 中的自定义数据	
磁条 2 等效数据 F： b T： 57 L： var. 最大 19 n， var. 最大 19 1 n4 n3 0 或 n5 n， var. hex.	M	按 GB/T 17552 的规定，磁条 2 的数据。不包括起始位、结束位和 LRC（验证码），包括： 应用主账号（PAN） 分隔符（“D”） 失效日期（YYMM） 服务码 PIN 验证域 自定义数据（由支付系统定义） 补 F（如果不是偶数个）	磁条 2 等效数据要保存在短文件标识符位 1，记录 1 中
交易证书数据对象	C	终端使用列出的数据对象	

名字（格式、标签和长度）	需求	描述	值
列表（TDOL） F： b T： 97 L： var. 最大 252	如果需要预先哈希	（标签和长度）生成 TC 哈希值	
应用密文（AC）密钥 F： b128 T： - L： 16	M	JR/T 0025 专有数据。双长度应用密文密钥，16 字节。用于卡片联机授权，发卡行联机授权和生成应用密文	
连续脱机交易上限 F： b8 T： 9F23 L： 1	C 如果支持终端频度检查	发卡行指定的卡片需要联机处理前允许连续脱机交易次数最大值	
连续脱机交易上限 F： b 8 T： 9F59 L： 1	C 如果无法联机，卡片风险管理可以得出交易拒绝结论	JR/T 0025 专有数据。发卡行指定的卡片需要联机处理前允许连续脱机交易次数最大值	
JR/T 0025 自定义数据 F： b56 T： - L： var 7-9	R	发卡行应用数据的一部分。包括一个长度字节、分散密钥索引、密文版本号和卡片验证结果。在生成应用密文命令中返回给终端	
卡产品标识信息 F: b 128 T: 9F63 L: 16	O	用于标识发卡行和卡片产品种类，在联机交易时上送发卡行。	字节 1－字节 8：银行标识码[1] 字节 9－11：卡产品标识 字节 9： 位 8：1=市民卡 位 7：1=军人卡 位 6：1=积分卡 位 5：1=交通卡 位 4：1=社保卡 位 3：1=学生卡 位 2：1=航空卡 位 1：1=公共缴费类卡 字节 10：本规范保留 字节 11：发卡行保留 字节 12－14：本规范保留 字节 15－16：发卡行保留

[1] 当前参考《联网联合技术规范 2.0》附录 A

名字（格式、标签和长度）	需求	描述	值

A.2 卡片和发卡行数据元需求

表A.2中是卡片和发卡行数据元的需求。

A.2.1 标签

标签列是数据元的标签（Tag）。

A.2.2 需求

必备/有条件/可选列是数据元的需求情况。加*号表示需求在未来会有变化，具体描述在“其它”列。

A.2.3 数据完整性（备份）

备份列是数据是否需要备份。

在一些特殊的情况下，例如在交易过程中突然拔出卡片、突然掉电等。卡片要有能力保护一些应用数据的不被破坏。

A.2.4 修改能力

修改列是数据是否可以被修改。如果允许，则修改命令在命令列中列出。

A.2.5 取回能力

取回列是数据是否可以被终端取回或通过命令返回给终端。标明“SD”的数据表明此数据只能在特殊设备上取回，不能在金融交易过程中由终端取出。

A.2.6 静态或动态

卡片风险管理数据里，“静态”表明数据不能修改但是可以用取数据命令返回给终端。“动态”表明数据不能通过终端发命令修改，而且也不能返回给终端。

A.2.7 秘密数据

标明“秘密”的数据表示要在卡片中安全保存。终端或其它设备不能得到这些数据，而且也不能因为一些特殊情况而被修改。PIN可以通过由安全报文的命令PIN修改/解锁修改。

A.2.8 ADF或DDF数据

ADF或DDF列是数据是存在支付系统DDF还是ADF目录下。终端在应用选择阶段用读记录命令读出。

A.2.9 数据需求表

表 A.2 数据需求

名称	标签	必备/有条件/可选	条件	备份需求	修改	取回	静态/动态	秘密数据	在ADF或DDF	其它
应用密文（AC）	9F26	R				生成应用密文				
应用货币代码	9F42	C	29		N	读记录				和9F51匹配
应用货币代码	9F51	C	1，2或3		N	取数据（特殊设备）	静态			和9F42匹配
应用货币指数	9F44	C	1，2，3或29		N	读记录				
应用缺省行为（ADA）	9F52	C	19				静态			

名称	标签	必备/有条件/可选	条件	备份需求	修改	取回	静态/动态	秘密数据	在ADF或DDF	其它
应用自定义数据	9F05	O			N	读记录				
应用生效日期	5F25	O			N	读记录				
应用失效日期	5F24	M			N	读记录				
应用文件定位器（AFL）	94	R			N	取处理选项				
应用标识符(AID)	4F	R			N	读记录			ADF	
应用交互特征（AIP）	82	M			N	取处理选项				
应用标签	50	R*			N	读记录选择			ADF	将来是必备
应用首选名称	9F12	O			N	读记录选择			ADF	
应用PAN	5A	M			N	读记录				
应用PAN序列号	5F34	O			N	读记录				
应用优先指示器	87	C	20		N	读记录选择			ADF	
应用交易计数器（ATC）	9F36	R		备份	N	取数据5，6				
应用用途控制（AUC）	9F07	O			N	读记录				
应用版本号	9F08	M			N	读记录				
卡片风险管理数据对象列表1（CDOL1）	8C	M			N	读记录				
卡片风险管理数据对象列表2（CDOL2）	8D	M			N	读记录				
卡片验证结果（CVR）					N	生成应用密文				9F10的一部分
持卡人姓名	5F20	R			N	读记录				将来是C（9）
持卡人姓名扩展	9F0B	O			N	读记录				
持卡人证件号	9F61	O			N	读记录				
持卡人证件类型	9F62	O			N	读记录				
持卡人验证方法（CVM）列表	8E	R			N	读记录				
CA公钥索引	8F	C	30或31		N	读记录				
连续脱机交易计数器(国际-货币)		C	1	备份或缺省为9F53	N	N	动态			
连续脱机交易限制数(国际-货币)	9F53	C	1		设置	取数据（特殊设				

名称	标签	必备/有条件/可选	条件	备份需求	修改	取回	静态/动态	秘密数据	在ADF或DDF	其它
					数据	备）				
连续脱机交易计数器(国际-国家)		C	7	备份或缺省为9F72	N	N	动态			
连续脱机交易限制数(国际-国家)	9F72	C	7		设置数据	取数据（特殊设备）				
密文信息数据（CID）	9F27	R				生成应用密文				
密文版本号		R			N	生成应用密文				9F10 的一部分
累计脱机交易金额		C	2	备份或缺省为9F54	N					
累计脱机交易金额限制数	9F54	C	2		设置数据	取数据（特殊设备）				
累计脱机交易金额上限	9F5C	O	2或3		设置数据	取数据（特殊设备）				
累计脱机交易金额（双货币）		C	3	备份或缺省为9F75	N	N	动态			
累计脱机交易金额限制数（双货币）	9F75	C	3		设置数据	取数据（特殊设备）				
货币转换因子	9F73	C	3		设置数据	取数据（特殊设备）				
数据认证码	9F45	O				读记录				93的一部分
数据加密DEA密钥		C	10		N	N		秘密		
专用(DF)文件名称	84	R			N	选择				
分散密钥索引		O			N	N				9F10 的一部分
目录定义文件	5D	C	11		N	读记录			DDF	

名称	标签	必备/有条件/可选	条件	备份需求	修改	取回	静态/动态	秘密数据	在ADF或DDF	其它
（DDF）名称										
目录自定义模板	73	O			N	读记录			ADF DDF	
动态数据认证数据对象列表（DDOL）	9F49	C	31		N	读记录				
DDA失败指示位		C	31	备份或缺省为0	N	N	动态			
文件控制信息（FCI）发卡行自定义数据	BF0C	O			N	选择				
FCI专有模板	A5	R			N	选择				
FCI模板	6F	R			N	选择				
ICC动态数据		C	31			内部认证				
ICC动态数	9F4C	C	31			内部认证				9F4B的一部分
IC卡公私钥数据										
● 私钥		C	31		N	N		秘密		
● 公钥证书	9F47	C	31		N	读记录				
● 公钥模数	9F46	C	31		N	读记录				
● 公钥余数	9F48	C	15		N	读记录				
发卡行行为代码-缺省	9F0D	R*			N	读记录				将来必备
发卡行行为代码-拒绝	9F0E	R*			N	读记录				将来必备
发卡行行为代码-联机	9F0F	R*			N	读记录				将来必备
发卡行应用数据	9F10	R			N	生成应用密文				
发卡行认证数据	91	O	19							
发卡行认证失败指示位		C	19	备份或缺省为0或1	N	N	动态			
发卡行认证指示位	9F56	C	19		N	取数据（特殊设备）	静态			
发卡行代码表索引	9F11	C	16		N	选择				
发卡行国家代码	5F28	C	17		N	读记录				和9F57匹配
发卡行国家代码	9F57	C	7		N	取数据（特殊设	静态			和5F28匹配

名称	标签	必备/有条件/可选	条件	备份需求	修改	取回	静态/动态	秘密数据	在ADF或DDF	其它
						备）				
发卡行公钥数据										
● 发卡行公钥证书	90	C	30或31		N	读记录				
	9F32	C	30或31		N	读记录				
● 发卡行公钥模数 ● 发卡行公钥余数	92	C	15		N	读记录				
发卡行脚本命令计数器		C	18	备份或缺省为0	N	N	动态			
发卡行脚本失败指示位		C	18	备份或缺省为0或1	N	N	动态			
发卡行脚本模板2	72	C	18							
发卡行URL	9F50	O				选择				
发卡行URL2	9F5A	O				选择				
首选语言	5F2D	O				选择				
上次联机ATC寄存器	9F13	C	4、5、6、8或24	备份或缺省为1	N	取数据5，6或24				
日志入口	9F4D	O				选择应用			ADF	
日志格式	9F4F	O				取数据				
连续脱机交易下限	9F14	C	5、6、24	备份	修改记录	读记录				
连续脱机交易下限	9F58	C	4	备份	设置数据	取数据（特殊设备）				
报文鉴别码(MAC)DEA密钥		C	18和28		N	N		秘密		
联机授权指示位		R		缺省为1或备份	N	N	动态			
PIN尝试计数器	9F17	C	21	备份或缺省为限制数	PIN修改/解锁	取数据27				
PIN尝试限制数		C	21		N	N		秘密		
处理选项数据对	9F38	C	22			选择				

名称	标签	必备/有条件/可选	条件	备份需求	修改	取回	静态/动态	秘密数据	在ADF或DDF	其它
象列表（PDOL）										
脱机PIN		C	21	备份	PIN修改/解锁	N		秘密		
响应报文模板格式1	80	R			N	N				
第2应用货币代码	9F76	C	3		N	取数据（特殊设备）	静态			
服务码	5F30	O			N	读记录				
短文件标识符（SFI）	88				N	选择 取处理选项				
签名的动态应用数据	9F4B	C	31		n/a	内部认证				
签名的静态应用数据	93	C	30		N	读记录				
SDA失败指示位		C	30	备份或缺省为0	N	N	动态			
静态数据认证标签列表	9F4A	C	（30或31）和32		N	读记录				
磁条1自定义数据	9F1F	R			修改记录25	读记录				未来可选
磁条2等效数据	57	M			修改记录25	读记录				应是SFI为1的记录1
交易证书数据对象列表（TDOL）	97	C	23		N	读记录				
唯一DEA密钥		R			N	N		秘密		
连续脱机交易上限	9F23	C	5、6和24	备份	修改记	读记录				

名称	标签	必备/有条件/可选	条件	备份需求	修改	取回	静态/动态	秘密数据	在ADF或DDF	其它
					录					
连续脱机交易上限	9F59	C	8	备份	设置数据	取数据（特殊设备）				
卡产品标识信息	9F63	O			N	读记录				

A.2.10 数据需求表-条件号对应表

数据需求表中条件号对应的具体条件见表A.3。

表 A.3 条件号对应条件

条件号/码	描述
特殊设备	只能在指定设备上取回数据，普通金融交易过程中不执行
1	如果卡片执行连续脱机交易-国际货币频度检查
2	如果卡片执行累计金额频度检查
3	如果卡片执行累计金额（双货币）频度检查
4	如果卡片执行连续脱机交易下限频度检查
5	如果终端执行连续脱机交易下限频度检查
6	如果终端执行连续脱机交易上限频度检查
7	如果卡片执行连续脱机交易-国际国家频度检查
8	如果卡片执行连续脱机交易上限频度检查
9	如果磁条中有
10	如果支持修改参考PIN值或其它秘密数据
11	如果应用选择使用目录方式
15	如果证书中的公钥不完整的剩余部分
16	如果有应用首选名称
17	如果有应用用途控制（AUC）
18	如果支持发卡行脚本
19	如果支持发卡行认证
20	如果卡片中有多个支付应用
21	如果支持脱机PIN
22	如果应用初始化时需要终端数据
23	如果要求预哈希
24	如果执行新卡检查
25	如果支持修改PVV
26	如果支持持卡人验证
27	如果显示“最后一次PIN机会”
28	如果支持安全报文
29	如果CVM列表中使用了金额
30	如果支持SDA

条件号/码	描述
31	如果支持 DDA
32	如果要签名基本数据对象
34	需要记录交易明细

附 录 B
（规范性附录）
命令规范－描述卡片支持的命令

此附录中描述了各个章条中使用到的卡片命令。

——应用锁定（APPLICATION BLOCK）（发卡行脚本命令）；

——应用解锁（APPLICATION UNBLOCK）（发卡行脚本命令）；

——卡片锁定（CARD BLOCK）（发卡行脚本命令）；

——外部认证（EXTERNAL AUTHENTICATE）；

——生成应用密文（GENERATE APPLICATION CRYPTGRAM （AC））；

——取数据（GET DATA）；

——获取处理选项（GPO）；

——内部认证（INTERNAL AUTHENTICATE）；

——PIN 修改/解锁（PIN CHANGE/UNBLOCK）（发卡行脚本命令）；

——设置数据（PUT DATA）（发卡行脚本命令）；

——读记录（READ RECORD）；

——选择（SELECT）；

——修改记录（UPDATE RECORD）（发卡行脚本命令）；

——验证（VERIFY）。

上述命令可以在其它情况下使用，例如个人化卡片。

终端发送命令给卡片，卡片处理完毕后，返回命令响应给终端。每个命令包括的CLA、INS字节标明了命令类型，参数字节P1 P2提供了处理信息。命令还可能包括一个数据域。

命令响应包括两个状态字SW1和SW2，描述了命令运行结果。当命令执行成功，SW1和SW2等于“9000”，其它值说明命令执行错误。命令的响应中还可以包括响应数据。

B.1 发卡行脚本命令的基本处理原则

一些特殊功能的发卡行脚本命令要在非金融交易过程中，在发卡行控制的设备上发送给卡片，例如：APPLICATION UNBLOCK和PIN CHANGE/UNBLOCK。

发卡行脚本命令要求安全报文。报文鉴别码（MAC）用来验证命令来自有效的发卡行并且保证命令在传送过程中没有被修改。如果命令中包括秘密数据例如持卡人PIN，需要数据加密进行保护。

B.2 应用锁定C-APDU/R-APDU

B.2.1 定义和范围

APPLICATION BLOCK命令是使当前被选择的应用无效的一个发卡行脚本命令。

在成功的APPLICATION BLOCK命令之后：

——对选择（SELECT）命令，无效的应用应该返回状态字节“选择文件无效”（SW1 SW2=“6283”）；

——对生成应用密文（GENERATE AC）命令，一个无效的应用应该返回 AAC 代替 AC 作为响应。

B.2.2 命令报文

APPLICATION BLOCK命令报文根据表B.1编码。

表 B.1 APPLICATION BLOCK命令报文

编码	值
CLA	‘84’
INS	‘1E’
P1	‘00’；其它值保留
P2	‘00’；其它值保留
Lc	数据域字节长度
数据域	4 字节 MAC 值
Le	不存在

B.2.3 命令报文的数据域

命令报文的数据域中包含了根据JR/T 0025.7中描述的安全报文格式编码的MAC数据。

B.2.4 响应报文的数据域

响应报文没有数据域。

B.2.5 响应报文返回的处理状态

不论应用是否有效，“9000”编码总表示命令成功执行。

B.3 应用解锁C-APDU/R-APDU

B.3.1 定义和范围

APPLICATION UNBLOCK命令是一个发卡行脚本命令，用来恢复当前被选择的应用。

当APPLICATION UNBLOCK命令成功执行后，此前通过应用锁定附加在该应用上的限制被解除。

B.3.2 命令报文

APPLICATION UNBLOCK命令报文通过表B.2编码。

表 B.2 APPLICATION UNBLOCK命令报文

编码	值
CLA	‘84’
INS	‘18’
P1	‘00’；其它值保留
P2	‘00’；其它值保留
Lc	数据域字节长度
数据域	4 字节 MAC 值
Le	不存在

B.3.3 命令报文的数据域

命令报文的数据域中包含了根据安全规范中描述的安全报文格式编码的MAC数据。

B.3.4 响应报文的数据域

响应报文中没有数据域。

B.3.5 响应报文返回的处理状态

不论应用是否有效，“9000”编码表示命令成功执行。

B.4 卡片锁定C-APDU/R-APDU

B.4.1 定义和范围

CARD BLOCK命令是一个发行后命令，用来永久地停止IC卡中所有的应用。

CARD BLOCK命令停止IC卡中所有的应用，包括那些被隐式选中的应用。

当一个CARD BLOCK命令成功后，所有随后的选择命令都将收到状态字节为“功能不支持”（SW1 SW2=“6A81”）的反馈，并且不执行任何其它动作。

B.4.2 命令报文

CARD BLOCK命令报文根据表B.3编码。

表 B.3 CARD BLOCK命令报文

编码	值
CLA	‘84’
INS	‘16’
P1	‘00’；其它值保留
P2	‘00’；其它值保留
Lc	数据域字节长度
数据域	4 字节 MAC 值
Le	不存在

B.4.3 命令报文的数据域

命令报文的数据域中包含了根据安全规范中描述的安全报文格式编码的MAC数据。

B.4.4 响应报文的数据域

响应报文没有数据域。

B.4.5 响应报文返回的处理状态

不论卡是否已经被锁，“9000”编码都表示命令成功执行。

B.5 外部认证C-APDU/R-APDU

B.5.1 定义和范围

外部认证（EXTERNAL AUTHENTICATE）命令要求IC卡中的应用认证一个密文。

IC卡的响应应该包括该命令的处理状态。

一次交易中只执行最多一次外部认证命令。

B.5.2 命令报文

外部认证（EXTERNAL AUTHENTICATE）命令报文根据表B.4编码。

表 B.4 外部认证（EXTERNAL AUTHENTICATE）命令报文

编码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	‘00’
Lc	8－16
数据域	发卡行认证数据
Le	不存在

在外部认证（EXTERNAL AUTHENTICATE）命令中的引用算法（P1）值为‘00’，表示该域无信息。对算法的引用或者在使用本命令前就已经完成，或者在本命令的数据域中定义。

B.5.3 命令报文的数据域

按照JR/T 0025的规定，本命令报文的数据域包含标签为‘91’的值域，编码如下：

——前 8 个字节为必选的授权响应密文 ARPC；

——附加的 1-8 个可选字节是专有数据。

在JR/T 0025中，发卡行认证数据包括下列两个数据元：

——ARPC（8 字节）；

——授权响应码（2 字节）。

B.5.4 响应报文的数据域

响应报文没有数据域。

B.5.5 响应报文返回的处理状态

“9000”编码表示命令成功执行。

如果验证失败，返回“6300”，如果在本次交易中卡片已经接收过外部认证命令，卡片返回“6985”。

B.6 生成应用密文C-APDU/R-APDU

B.6.1 定义和范围

生成应用密文（GENERATE AC）命令传送交易相关数据到IC卡，IC卡计算并且返回一个密文。这个密文是一个由JR/T 0025定义的应用密文（AC），表B.5列出了密文类型。

表 B.5 生成应用的密文类型

类型	意义
应用认证密文（AAC）	拒绝交易
授权请求密文（ARQC）	请求联机授权
交易证书（TC）	批准交易

由IC卡返回的密文可能由于IC卡的内部处理过程而与命令报文中要求的密文不一样。

B.6.2 命令报文

生成应用密文（GENERATE AC）命令报文根据表B.6编码。

表 B.6 生成应用密文（GENERATE AC）命令报文

编码	值
CLA	‘80’
INS	‘AE’
P1	引用控制参数（见表 B.7）
P2	‘00’
Lc	Var.
数据域	交易相关数据
Le	‘00’

生成应用密文（GENERATE AC）命令中的引用控制参数根据表B.7编码。

表 B.7 GENERATE AC引用控制参数

b8	b7	B6	b5	b4	b3	b2	b1	意义
0	0							AAC
0	1							TC
1	0							ARQC
1	1							保留
			0					未明确请求复合动态数据认证/应用密文生成
			1					请求复合动态数据认证/应用密文生成
		x		x	x	x	x	保留

B.6.3 命令报文的数据域

命令报文的数据域是用来生成应用密文的终端数据，具体的数据内容在附录D中描述。

B.6.4 响应报文的数据域

密文的生成算法在附录D中描述。

响应报文的数据域包含一个BER-TLV编码的数据对象。这个数据对象需要按照以下两种格式之一编码。

格式1：

响应报文中的数据对象是一个标签为‘80’的基本数据对象。数据域由表B.8所示的数据对象连接而成，各数据对象之间没有分隔符（标签和长度）。

表 B.8 GENERATE AC响应报文数据域格式1

值	存在性
密文信息数据	必备
应用交易计数器（ATC）	必备
应用密文（AC）	必备
发卡行应用数据	可选

格式2：

响应报文的数据对象是一个标签为‘77’的结构数据对象。数据域中可以包含多个BER-TLV编码对象，但是应包括密文信息数据、应用交易序号和由IC卡计算出的密文（可以是应用密文或专有密文）。对于响应报文中可能包含的专有数据对象的应用和解释，不在JR/T 0025的范围之内。

如果响应报文是如本部分第9章、第14章及第16章定义的签名数据，对CDA的响应，则采用格式2。该响应数据单元格式见JR/T 0025.7的5.3.6。

如果卡片不执行CDA，命令的响应报文数据域中的数据对象按照格式1编码。如果卡片执行CDA，命令的响应报文数据域中的数据对象按照格式2编码。

以上两种格式中，在生成应用密文命令的响应报文中包括的密文数据按照表B.9的方式编码。

表 B.9 密文信息数据编码

b8	b7	b6	b5	b4	b3	b2	b1	意义
0	0							AAC
0	1							TC
1	0							ARQC
1	1							RFU
		x	x					支付系统密文
				0				未请求通知
				1				请求通知
					x	x	x	原因/通知/授权参考码
					0	0	0	无信息
					0	0	1	不允许服务
					0	1	0	PIN 重试超限
					0	1	1	发卡行鉴定失败
					x	x	x	其它值保留

B.6.5 响应报文返回的处理状态

“9000”编码表示命令成功执行。

一次交易卡片最多处理两个生成应用密文命令，如果收到三个及以上个数，卡片返回“6985”。

B.7 取数据C-APDU/R-APDU

B.7.1 定义和范围

下面描述的是在非金融交易过程中在特殊设备上使用取数据（GET DATA）命令访问到的数据和一个金融交易过程中，使用取数据（GET DATA）命令访问数据。

——特殊设备

表 B.10 列出的静态数据可以在发卡行控制的特殊设备上通过取数据（GET DATA）命令访问。普通终端不能用取数据命令获得。

表 B.10 使用取数据（GET DATA）命令访问的静态数据

数据元
应用货币代码
应用缺省行为
连续脱机交易限制数（国际-国家）
连续脱机交易限制数（国际-货币）
累计脱机交易金额限制数
累计脱机交易金额限制数（双货币）
累计脱机交易金额上限
货币转换因子
发卡行认证指示位
发卡行国家代码
连续脱机交易下限
连续脱机交易上限
第 2 应用货币代码

——金融交易

取数据(GET DATA)命令用来从当前应用中取得一个没有封装在记录中的基本数据对象。取数据(GET DATA）命令可以用来获取基本数据对象ATC（标签为“9F36”）、上次联机ATC寄存器（标签为“9F13”）或PIN重试计数器（标签为“9F17”）、日志格式（标签为“9F4F”）。

B.7.2 命令报文

取数据（GET DATA）命令报文根据表B.11编码。

表 B.11 取数据（GET DATA）命令报文

编码	值
CLA	‘80’
INS	‘CA’
P1 P2	要访问数据的标签
Lc	不存在
数据域	不存在
Le	‘00’

B.7.3 命令报文的数据域

命令报文没有数据域。

B.7.4 响应报文的数据域

响应报文的数据域中包含有如命令报文的P1 P2所述的基本数据对象。（即包括它的标签和它的长度）。

B.7.5 响应报文返回的处理状态

“9000”编码表示命令成功执行。

如果命令中请求的数据是专有数据不能返回，卡片返回“6A88”。

B.8 获取处理选项C-APDU/R-APDU

B.8.1 定义和范围

获取处理选项（GPO）命令用来启动IC卡内的交易。

IC卡的响应报文中包含应用交互特征（AIP）和应用文件定位器（AFL）。

B.8.2 命令报文

获取处理选项（GPO）命令报文根据表B.12编码。

表 B.12 获取处理选项（GPO）命令报文

编码	值
CLA	‘80’
INS	‘A8’
P1 P2	‘00’
Lc	‘00’
数据域	PDOL 相关数据（如果存在）或 8300
Le	‘00’

B.8.3 命令报文的数据域

命令报文的数据域根据IC卡提供的处理选项数据对象列表（PDOL）编码。PDOL通过标签“83”标记。当IC卡没有提供数据对象列表时，这个模板的长度域设置为‘0’。否则，这个模板的数据长度域的值等于传输给IC卡的数据对象的值域的总长度。

B.8.4 响应报文的数据域

响应报文的数据域包含一个BER-TLV编码数据对象。

这个数据对象需要按照下列格式编码：

响应报文中的数据对象是一个标签为‘80’的基本数据对象。数据域由如表B.13所示的应用交互特征（AIP）和应用文件定位器（AFL）的值域连接而成，各数据对象之间没有分隔符（标签和长度）。

表 B.13 GPO响应报文数据域格式

‘80’	长度	应用交互特征	AFL

应用交互特征定义了可以被IC卡中的应用支持的功能。

AFL包括一个不含有分隔符的由文件与记录组成的列表。

B.8.5 响应报文返回的处理状态

“9000”编码表示命令成功执行。

B.9 内部认证C-APDU/A-APDU

B.9.1 定义和范围

内部认证（INTERNAL AUTHENTICATE）命令引发卡片使用从IFD收到的随机数、数据和卡片中储存的私钥来计算出“签名动态应用数据”的过程。

B.9.2 命令报文

内部认证（INTERNAL AUTHENTICATE）命令根据表 B.14 编码。

表 B.14 内部认证（INTERNAL AUTHENTICATE）命令报文

编码	值
CLA	‘00’
INS	‘88’
P1	‘00’
P2	‘00’
Lc	认证相关数据长度
数据域	认证相关数据
Le	‘00’

在内部认证（INTERNAL AUTHENTICATE）命令中的算法引用（P1）域值为‘00’，这表示该值无意义。对算法的引用应该或者在使用本命令前就已经完成，或者在本命令的数据域中定义。

B.9.3 命令报文的数据域

命令报文的数据域包括该应用专有的与认证有关的数据。它是根据JR/T 0025.7中定义的动态数据认证数据对象列表（DDOL）规则来编码的。

为了确保内部认证（INTERNAL AUTHENTICATE）命令返回数据在256字节限制内，签名的动态应用数据加上可选的TLV格式编码的长度应该限制在JR/T 0025.7中定义的范围内。

B.9.4 响应报文的数据域

响应报文的数据域包括一个BER-TLV编码数据对象。这个数据对象的编码格式为：

响应报文中的数据对象是一个标签为‘80’的基本数据对象。数据域中包括签名动态应用数据。签名动态应用数据按照JR/T 0025.7中的规则定义。

B.9.5 响应报文返回的处理状态

“9000”编码表示命令成功执行。

B.10 PIN修改/解锁C-APDU/R-APDU

B.10.1 定义和范围

PIN CHANGE/UNBLOCK命令是一个发卡行脚本命令。它的目的是让发卡行解锁PIN或同时既改变PIN也解锁PIN。

当PIN CHANGE/UNBLOCK命令成功后，卡片将执行下列功能：

——PIN 尝试记数器的值将复位到 PIN 尝试限制数（最大值）；

——如果有请求，脱机 PIN 值将被设置为新的 PIN 值。

为了保密，如果本命令包含有PIN数据，则该数据应该加密。

注： 脱机PIN是存储在卡中与应用相关的PIN，它用来验证在验证命令中传来的PIN数据。

B.10.2 命令报文

PIN CHANGE/UNBLOCK命令报文根据表B.15编码。

表 B.15 PIN CHANGE/UNBLOCK命令报文

编码	值
CLA	‘84’
INS	‘24’
P1	‘00’
P2	‘00’、‘01’或‘02’
Lc	数据字节数
数据	加密 PIN 数据成员（如果存在）和 MAC 数据
Le	不存在

当P2为“00”，PIN尝试计数器复位。

当P2为“01”，PIN尝试计数器复位同时PIN修改，PIN修改时使用当前的PIN。

当P2为“02”，PIN尝试计数器复位同时PIN修改，PIN修改是不使用当前的PIN。

B.10.3 命令报文的数据域

本命令报文的数据域包括PIN加密数据，后面可以加上4到8字节的安全报文MAC数据。

如果P2等于‘00’，参考PIN解锁，PIN尝试计数器被复位到PIN尝试限制数。命令数据域只包含MAC。因为PIN修改/解锁命令中不包含新的PIN值，所以PIN不会更新。

P2等于‘01’或‘02’的值的处理步骤分别在B.10.1和B.10.2中描述。

B.10.3.1 使用当前PIN修改PIN值

如果命令中的P2参数等于“01”，命令数据域包括PIN加密数据和MAC，PIN加密数据的产生过程按照下列步骤进行：

步骤 1：发卡行确定用来给数据进行加密的安全报文加密主密钥，并分散生成卡片的安全报文加密子密钥：ENC UDK-A 和 ENC UDK-B；

步骤 2：生成过程密钥 Ks；

步骤 3：生成 8 字节 PIN 数据块 D3：

a）生成一个 8 字节数据块 D1；

字节 1		字节 2		字节 3		字节 4		字节 5	字节 6	字节 7	字节 8
0	0	0	0	0	0	0	0	ENC UDK-A 的最右边 4 个字节			

b）生成第 2 个 8 字节数据块 D2；

字节 1		字节 2		字节 3		字节 4		字节 5		字节 6		字节 7		字节 8	
0	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

N：新PIN的数字个数（16进制）

P：新PIN值，长度4-12个数字（2-6字节）

c）D1 和 D2 执行异或得到 D3。

步骤 4：使用当前 PIN 生成 8 字节数据块 D4；

字节 1		字节 2		字节 3		字节 4		字节 5		字节 6		字节 7		字节 8	
P	P	P	P	P/0	P/0	P/0	P/0	P/0	P/0	P/0	P/0	0	0	0	0

步骤 5：将数据块 D3 和 D4 执行异或得到 D；

步骤 6：用 Ks 对 D 进行加密，得到 PIN 加密数据。

B.10.3.2 不使用当前PIN修改PIN值

如果命令中的P2参数等于“02”，命令数据域包括PIN加密数据和MAC，PIN加密数据的产生过程按照下列步骤进行：

步骤 1：发卡行确定用来给数据进行加密的安全报文加密主密钥，并分散生成卡片的安全报文加密子密钥：ENC UDK-A 和 ENC UDK-B；

步骤 2：生成过程密钥 Ks；

步骤 3：生成 8 字节 PIN 数据块 D3：

a）生成一个 8 字节数据块 D1；

字节 1		字节 2		字节 3		字节 4		字节 5	字节 6	字节 7	字节 8
0	0	0	0	0	0	0	0	ENC UDK-A 的最右边 4 个字节			

b）生成第 2 个 8 字节数据块 D2；

字节 1		字节 2		字节 3		字节 4		字节 5		字节 6		字节 7		字节 8	
0	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

N：新PIN的数字个数（16进制）；

P：新PIN值，长度4-12个数字（2-6字节）。

c）D1 和 D2 执行异或得到 D。

步骤 4：用 Ks 对 D 进行加密，得到 PIN 加密数据。

B.10.4 响应报文的数据域

响应报文没有数据域。

B.10.5 响应报文返回的处理状态

“9000”编码表示命令成功执行。

B.11 设置数据C-APDU/R-APDU

B.11.1 定义和范围

设置数据（PUT DATA）命令用来修改卡片中的一些基本数据对象的值。只有有标签的数据才能使用这条命令修改。此命令不能用来修改结构数据对象。

B.11.1.1 可以用设置数据命令修改的数据

表B.16列出的数据可以使用此命令修改。

表 B.16 使用设置数据（PUT DATA）命令修改的数据

数据元
连续脱机交易限制数（国际-国家）
连续脱机交易限制数（国际-货币）
累计脱机交易金额限制数
累计脱机交易金额限制数（双货币）
累计脱机交易金额上限
货币转换因子
连续脱机交易下限（9F58）
连续脱机交易上限（9F59）

B.11.2 命令报文

设置数据（PUT DATA）命令报文根据表B.17编码。

表 B.17 设置数据（PUT DATA）命令报文

编码	值
CLA	‘04’
INS	‘DA’
P1 P2	要修改的数据对象的标签
Lc	数据域字节数
数据域	数据对象的新值（不包括标签和长度）和 MAC 数据
Le	不存在

B.11.3 命令报文的数据域

命令数据域中包括的是要修改的数据对象的值，后面加一个4到8字节的MAC。MAC的计算见附录C中描述。

B.11.4 响应报文的数据域

响应报文没有数据域。

B.11.5 响应报文返回的处理状态

“9000”编码表示命令成功执行。

表B.18列出了命令可能返回的警告信息。

表 B.18 设置数据（PUT DATA）命令的警告响应码

SW1	SW2	含义
62	00	没有信息返回
62	81	数据可能被破坏

表B.19列出了命令可能返回的错误信息。

表 B.19 设置数据（PUT DATA）命令的错误响应码

SW1	SW2	含义
64	00	没有准确诊断
65	81	内存失败
67	00	长度错误
68	82	不支持安全报文
69	82	安全状态不满足
69	86	命令不允许
69	87	安全报文数据对象丢失
69	88	安全报文数据对象不正确
6A	80	错误的参数
6A	81	功能不支持
6A	84	文件中没有足够空间
6A	85	Lc 和 TLV 结构不一致

B.12 读记录C-APDU/R-APPDU

B.12.1 定义和范围

读记录（READ RECORD）命令从一个线性文件中读一条文件记录。

从IC卡返回的响应中将包含这条被读出的记录。

B.12.2 命令报文

读记录（READ RECORD）命令报文根据表B.20编码。

表 B.20 读记录（READ RECORD）命令报文

编码	值
CLA	‘00’
INS	‘B2’
P1	记录号
P2	引用控制参数，见表 B.21
Lc	不存在
数据域	不存在
Le	‘00’

表B.21定义了命令报文的引用控制参数。

表 B.21读记录（READ RECORD）命令引用控制参数

b8	B7	b6	b5	b4	b3	b2	b1	意义
x	x	x	x	x				SFI
					1	0	0	读 P1 指定记录

B.12.3 命令报文的数据域

命令报文中没有数据域。

B.12.4 响应报文的数据域

任何成功的读记录（READ RECORD）命令的响应报文的数据域都包含读出的记录值。对于在1-10范围内的SFI，这个记录是一个BER-TLV结构数据对象。它按照表B.22编码。

表 B.22 READ RECORD响应报文数据域

'70'	长度	记录模板

对于不在1-10范围内的SFI的读记录命令响应报文，不在JR/T 0025的描述范围内。

B.12.5 响应报文返回的处理状态

“9000”编码表示命令成功执行。

B.13 选择C-APDU/R-APDU

B.13.1 定义和范围

选择（SELECT）命令通过文件名或AID来选择IC卡中的PSE、DDF或ADF。应用选择在本部分的第6章中描述。

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

从IC卡返回的响应报文包含回送FCI。

B.13.2 命令报文

选择（SELECT）命令报文编码见表B.23。

表 B.23 选择（SELECT）命令报文

代码	值
CLA	'00'
INS	'A4'
P1	引用控制参数（见表 B.24）
P2	选择选项（见表 B.25）
Lc	'05' - '10'
Data	文件名
Le	'00'

表B.24定义了选择（SELECT）命令报文的引用控制参数。

表 B.24 选择（SELECT）命令引用控制参数

B8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0				
					1			通过名称选择
						0	0	

表 B.25定义了选择（SELECT）命令报文的选择选项P2。

表 B.25 选择（SELECT）命令的可选参数

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

B.13.3 命令报文数据域

命令报文数据域应包括所选择的PSE名、DF名或AID。

B.13.4 响应报文数据域

响应报文中数据域应包括所选择的PSE、DDF或ADF的FCI。表B.26、表B.27和表B.28定义了JR/T 0025所应用的标识。对于JR/T 0025所不规定的FCI中回送的附加标签应该被忽略。

表B.26定义了成功选择PSE后回送的FCI。

表 B.26 选择PSE的响应报文 （FCI）

标识	值			存在性
‘6F’	FCI 模板			M
	‘84’	DF 名（1PAY.SYS.DDF01）		M
	‘A5’	FCI 数据专用模板		M
		‘88’	目录基本文件的 SFI	M
		‘5F2D’	首选语言	O
		‘9F11’	发卡行代码表索引	O
		‘BF0C’	发卡行自定义数据（FCI）	O
		‘xxxx’（JR/T 0025.3 和本部分规定的标签）	来自从应用提供商、发卡行或 IC 卡供应商的 1 个或多个附加（专用）数据元	O

表B.27定义了成功选择DDF后回送的FCI。

表 B.27 选择DDF的响应报文 （FCI）

标签	值			存在性
‘6F’	FCI 模板			M
	‘84’	DF 名		M
	‘A5’	FCI 数据专用模板		M
		‘88’	目录基本文件的 SFI	M
		‘BF0C’	发卡行自定义数据（FCI）	O
		‘xxxx’（JR/T 0025.3 和本部分规定的标签）	来自从应用提供商、发卡行或 IC 卡供应商的 1 个或多个附加（专用）数据元	O

B.28表定义了成功选择ADF后回送的FCI。

表 B.28 选择ADF的响应报文 （FCI）

标签	值			存在性
‘6F’	FCI 模板			M
	‘84’	DF 名		M
	‘A5’	FCI 数据专用模板		M
		‘50’	应用标签	M
		‘87’	应用优先指示器	O
		‘9F38’	PDOL	O
		‘5F2D’	首选语言	O
		‘9F11’	发卡行代码表索引	O

	‘9F12’	应用优先名称		O
	‘BF0C’	发卡行自定义数据（FCI）		O
		‘xxxx’ （JR/T 0025.3 和本部分规定的标签）	来自从应用提供商、发卡行或 IC 卡供应商的 1 个或多个附加（专用）数据元	O
		‘9F4D’	日志入口	O

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

B.13.5 响应报文状态字

此命令执行成功的状态字是“9000”。

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

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

B.14 修改记录C-APDU/R-APDU

B.14.1 定义和范围

修改记录（UPDATE RECORD）命令用来修改文件中一条记录的内容，修改的内容在命令数据域中。

B.14.2 命令报文

修改记录（UPDATE RECORD）命令报文编码见表B.29。

表 B.29 修改记录（UPDATE RECORD）命令报文

代码	值
CLA	‘04’
INS	‘DC’
P1	记录号
P2	引用控制参数，见表 B.30
Lc	记录数据加 MAC 的长度
Data	记录数据和 MAC
Le	不存在

表B.30定义了命令报文的引用控制参数。

表 B.30 修改记录（UPDATE RECORD）命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	意义
x	x	x	x	x				SFI
					1	0	0	P1 为记录号

B.14.3 命令报文的数据域

数据域中是要修改的新记录内容。MAC长度为4到8字节。算法见附录C。

B.14.4 响应报文的数据域

响应报文没有数据域。

B.14.5 响应报文返回的处理状态

“9000”编码表示命令成功执行。

表B.31列出了命令可能返回的警告信息。

表 B.31 修改记录（UPDATE RECORD）命令的警告响应码

SW1	SW2	含义
62	00	没有信息返回
62	81	数据可能被破坏

表B.32列出了命令可能返回的错误信息。

表 B.32 修改记录（UPDATE RECORD）命令的错误响应码

SW1	SW2	含义
64	00	没有准确诊断
65	81	内存失败
67	00	长度错误
68	82	不支持安全报文
69	81	命令与文件结构不匹配
69	82	安全状态不满足
69	86	命令不允许
69	87	安全报文数据对象丢失
69	88	安全报文数据对象不正确
6A	81	功能不支持
6A	82	文件没找到
6A	83	记录没找到
6A	84	文件中没有足够空间
6A	85	Lc 和 TLV 结构不一致

B.15 验证C-APDU/R-APDU

B.15.1 定义和范围

验证（VERIFY）命令引发IC卡将命令报文数据域内的交易PIN数据和与该应用相关的参考PIN数据进行比较验证。验证方式由IC卡中的应用自行决定。如本部分第11章所述，当从CVM列表中选择的持卡人验证方法（CVM）是脱机PIN时，使用验证（VERIFY）命令。

B.15.2 命令报文

验证（VERIFY）命令报文根据表B.33编码。

表 B.33 验证（VERIFY）命令报文

编码	值
CLA	‘00’
INS	‘20
P1	‘00’
P2	参考数据定义
Lc	var.
数据	交易 PIN 数据
Le	不存在

表B.34定义了参考数据（P2）的意义。

表 B.34 验证（VERIFY）命令参考数据定义（P2）

b8	b7	b6	b5	b4	b3	b2	b1	意义
0	0	0	0	0	0	0	0	IS0/IEC 7816-4 定义[2]
1	0	0	0	0	0	0	0	明文 PIN，格式如下
1	0	0	0	0	x	x	x	JR/T 0025 保留
1	0	0	0	1	0	0	0	EMV 保留
1	0	0	0	1	0	x	x	JR/T 0025 保留
1	0	0	0	1	1	x	x	支付系统保留
1	0	0	1	x	x	x	x	发卡行保留

对于IC卡内的验证（VERIFY）命令的处理在本部分第11章中与CVM规则一起介绍。

明文脱机PIN数据块按如下格式组织。

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

其中

	名称	值
C	控制域	值为 0010 的四位二进制数（hex. 2）
N	PIN 长度	值在 0100 到 1100 之间的 4 位二进制数（hex. ‘4’到 ‘C’）
P	PIN 数字	值在 0000 到 1001 之间的 4 位二进制数（hex. ‘0’到 ‘9’）
P/F	PIN/填充位	由 PIN 长度决定
F	填充位	值为 1111 的四位二进制数（hex. ‘F’）

P2=‘00’表示没有使用特别的限定符。IC卡中处理验证命令的应用应该知道怎样明白无误的找到PIN数据。

B.15.3 命令报文的数据域

命令报文的数据域中包含标签‘99’的值域。

B.15.4 响应报文的数据域

响应报文中没有数据域。

B.15.5 响应报文中的处理状态

“9000”编码表示命令成功执行。

如果对当前选择的应用，通过验证命令对交易PIN数据和参考PIN数据进行的比较失败了，IC卡会返回SW2=‘Cx’，‘x’代表还可以重新验证的次数；如果IC卡返回了‘C0’，意味着不能再验证了，CVM会被锁死。随后，在这个应用中进行的所有验证命令都会失败，并返回SW1 SW2=“6983”。

[2] JR/T 0025 未采用 P2= ‘00’。

附 录 C
（规范性附录）
安全报文

本附录描述了发卡行脚本命令中如何使用安全报文。

安全报文的基本目的是确保数据的机密性，报文完整性和进行发卡行认证。报文完整性和发卡行鉴别通过MAC实现。数据保密通过加密命令明文数据实现。

C.1 安全报文格式

JR/T 0025中的安全报文均符合ISO 7816-4标准。当命令中CLA字节的低半字节为4，命令使用安全报文格式。

C.2 报文完整性和鉴别

报文鉴别码（MAC）使用命令中所有的数据元包括命令头生成。命令的完整性包括命令中的数据域部分（如果存在）使用安全报文来保证。

C.2.1 MAC位置

MAC是命令数据域中最后的数据元。

C.2.2 MAC长度

JR/T 0025规定MAC长度为4字节。

C.2.3 MAC密钥生成

在处理安全报文时使用MAC密钥过程密钥。过程密钥的生成见C.4。MAC过程密钥由卡片中的安全报文鉴别（MAC）密钥（MAC UDK）生成。

C.2.4 MAC计算

命令中需要加密的数据加密以后再计算MAC。MAC使用对称密钥算法计算的，步骤如下：

步骤 1：初始值为 8 字节全零（此步骤可省略）；

步骤 2：下列数据按顺序排列得到一个数据块 D：

——CLA、INS、P1、P2 和 Lc（Lc 的长度包括 MAC 的长度）；

——ATC（对于发卡行脚本处理，此 ATC 在请求中报文中上送）；

——应用密文（对于发卡行脚本处理，此应用密文通常是 ARQC，或 AAC，在请求报文中上送）；

——命令数据域中的明文或密文数据（如果存在）。

步骤 3：将上述数据块 D 分成 8 字节长的数据块 D1、D2、D3...最后一块数据块的字节长度为 1 到 8；

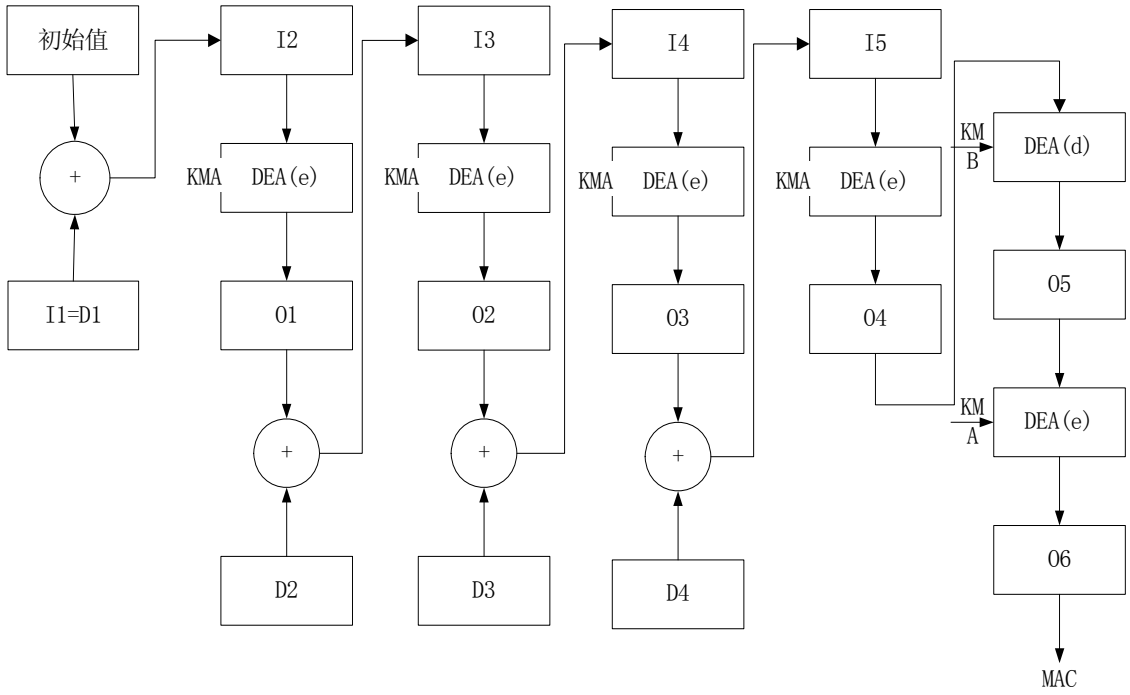
步骤 4：如果最后一块数据块的长度为 8 字节，后面补 8 字节数据块：80 00 00 00 00 00 00 00，执行步骤 5；

如果最后一块数据块的长度小于 8 字节，后面补一个字节 80，如果长度到 8 字节，执行步骤 5。如果仍然不够 8 字节，补 00 直到 8 字节；

步骤 5：用 MAC 过程密钥对数据块进行加密。MAC 过程密钥的生成见 C.4；

图 C.1 是使用 MAC 过程密钥 A 和 B 生成 MAC 的流程图。

步骤 6：MAC 的计算结果为 8 字节，从最左边的字节开始取 4 字节。



说明：

I = 输入	D = 数据块
DEA(e)= 数据加密算法（加密模式）	KMA = MAC过程密钥A
DEA(d)= 数据加密算法（解密模式）	KMB = MAC过程密钥B
O = 输出	+ = 异或

图 C.1 使用双长度DEA密钥计算MAC的算法

C.3 数据加密

数据加密用来确保命令中的关键数据的机密性。

C.3.1 数据加密密钥计算

在处理安全报文时使用安全报文加密过程密钥。过程密钥的生成见C.4。数据加密过程密钥由卡片中的安全报文加密密钥（ENC UDK）生成。

C.3.2 加密数据的结构

当命令中的明文数据需要加密时，首先要建立一个数据块，步骤如下：

——数据明文的长度 Ld（不包括补充字节长度）；

——数据明文；

——补充字节（“C.3.3 数据加密计算”中描述）。

然后对整个数据块进行加密。

C.3.3 数据加密计算

数据加密在MAC计算之前进行。步骤如下：

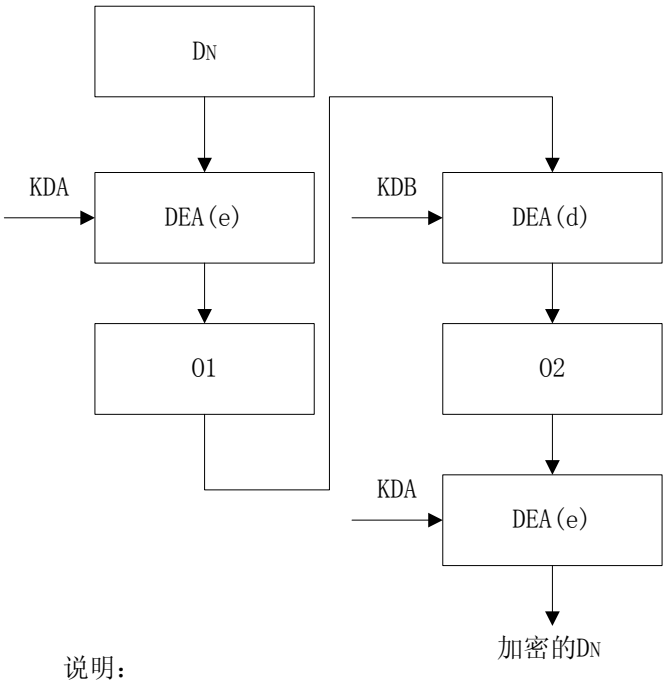
步骤 1：设 Ld 为明文数据的长度；

步骤 2：将数据 C.3.2 中得到的数据块分成 8 字节一组：D1、D2、D3……最后一组的长度为 1 到 8 字节；

步骤 3：如果最后一组数据块长度等于 8，执行步骤 4。如果长度小于 8，在后面补 80，如果长度到 8 字节，执行步骤 4。如果仍然不够 8 字节，补 00 直到 8 字节；

步骤 4：每个数据块使用数据加密过程密钥加密。过程密钥的生成见附录 C.4。

图C.2是使用数据加密过程密钥A和B对数据块加密的流程。



说明：

DEA(e)= 数据加密算法（加密模式）　D = 数据块
DEA(d)= 数据加密算法（解密模式）　KMA = MAC过程密钥A
O = 输出　KMB = MAC过程密钥B

图 C.2 用双长度DEA密钥进行数据加密

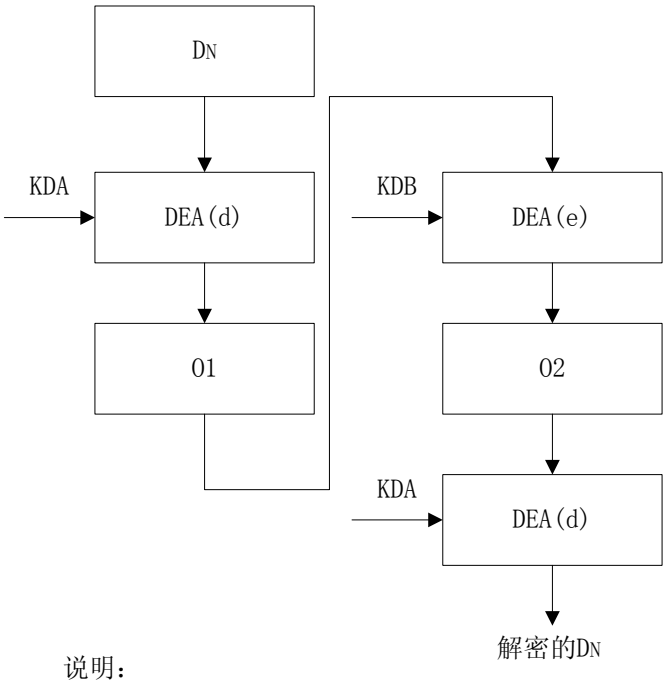
步骤 5：结束后，所有的加密后的数据块顺序连接（加密的 D1、加密的 D2、加密的 D3.....）就是命令数据域中的最终数据。

C.3.4 数据解密计算

收到命令后，卡片要把命令数据域中的加密数据进行解密，步骤如下：

步骤 1：将命令数据中的数据分成 8 字节一组：D1、D2、D3.....每个数据组用数据加密过程密钥解密；

图C.3是使用数据加密过程密钥A和B对数据块进行解密的流程；



说明：

DEA(e)= 数据加密算法（加密模式）　D = 数据块
DEA(d)= 数据加密算法（解密模式）　KMA = MAC过程密钥A
O = 输出　KMB = MAC过程密钥B

图 C.3 使用双长度DEA密钥进行数据解密

步骤 2：结束后，所有的解密后的数据块顺序连接（解密的 D1、解密的 D2、解密的 D3...）就是命令数据域中的 Ld，数据明文和补充字节；

步骤 3：Ld 表明了数据的真实长度。

C.4 生成过程密钥

本部分描述了过程密钥的生成方法。步骤如下：

步骤 1：生成过程密钥的卡片密钥是：MAC DEA 密钥 A 和 B（MAC UDK），数据加密 DEA 密钥 A 和 B（ENC UDK）；

步骤 2：将两字节的 ATC 右对齐，前面补 6 个字节 00.....（见 JR/T 0025.7 部分）；

步骤 3：将两字节的 ATC 取反后右对齐，前面补 6 个字节 00.....（见 JR/T 0025.7 部分）。

附 录 D
（规范性附录）
认证密钥和算法

本附录描述了和生成应用密文相关的密钥和算法。

D.1 数据元

发卡行要决定生成应用密文的数据元。

表D.1列出了生成应用密文的数据顺序。

表 D.1 TC/AAC/ARQC数据元顺序

数据元	来自终端的数据	在交易证书（TC）哈希中的顺序	卡片内数据
授权金额	✓	✓	
其它金额	✓	✓	
终端国家代码	✓	✓	
终端验证结果	✓	✓	
交易货币代码	✓	✓	
交易日期	✓	✓	
交易类型	✓	✓	
不可预知数	✓	✓	
应用交互特征（AIP）			✓
应用交易计数器（ATC）			✓
卡片验证结果（CVR）			✓

D.2 生成TC、AAC和ARQC

密文生成的步骤如下：

步骤 1：终端将 CDOL 中指定的终端数据通过生成应用密文命令传送给卡片。如果 CDOL 中有要交易证书（TC）哈希结果，终端要将此数据放到命令数据域中。

步骤 2：根据卡片风险管理的结果，卡片决定返回的密文类型为 TC、AAC 或 ARQC。生成密文的数据块：

——交易证书（TC）哈希结果（如果存在）；

——生成应用密文命令中送进卡片的数据。不包括 TC 哈希结果；

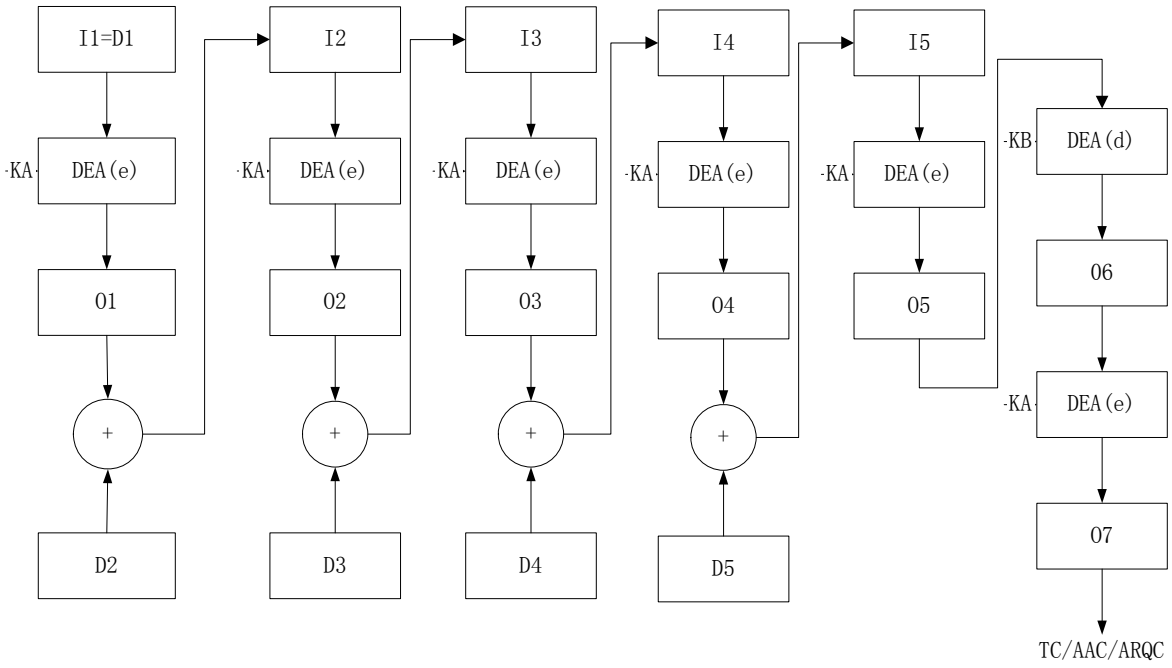
——卡片内部数据。

步骤 3：将上述数据块分成 8 字节一组：D1、D2、D3.....

步骤 4：如果最后一块数据块的长度为 8 字节，后面补 8 字节数据块：80 00 00 00 00 00 00 00；如果最后一块数据块的长度小于8字节，后面补一个字节80，如果仍然不够8字节，补00直到8字节。

步骤 5：使用过程密钥用对称密钥算法生成应用密文；

步骤 6：过程密钥是由卡片中唯一分散密钥（UDK）生成，具体生成方法在 C.4 中。图 D.1 是使用过程密钥 A 和 B 生成应用密文的流程。



说明：

I = 输入	D = 数据块
DEA(e)= 数据加密算法（加密模式）	KA = 密钥A
DEA(d)= 数据加密算法（解密模式）	KB = 密钥B
O = 输出	+ = 异或

图 D.1 TC/AAC/ARQC的生成算法

D.3 生成授权响应密文ARPC

卡片在收到外部认证命令时，生成一个ARPC和命令中传送进来的ARPC进行比较。生成ARPC的步骤如下：

步骤 1：将应用密文和授权响应码进行异或；

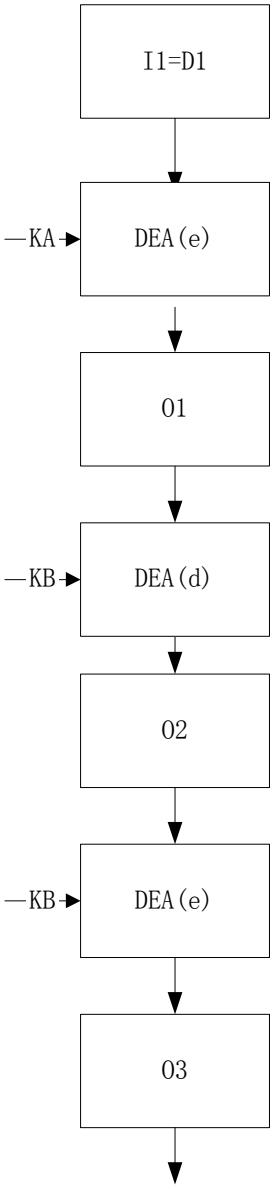
应用密文包括在上传的请求报文中，通常是ARQC，在一些特殊情况下是AAC。

授权响应码是在外部认证命令中送入卡片的。在执行异或前左对齐后面补6个字节00。

步骤 2：异或的结果是一个 8 字节的数据块 D1；

步骤 3：使用过程密钥用对称密钥算法计算 ARPC。

图D.2是ARPC的生成方法。



说明：

I = 输入	D = 数据块
DEA(e)= 数据加密算法（加密模式）	KA = 密钥A
DEA(d)= 数据加密算法（解密模式）	KB = 密钥B
O = 输出	

图 D.2 生成ARPC的算法

D.4 密钥分散方法

本部分描述了密钥分散的方法。卡片中的唯一DEA密钥是在卡片个人化时，从主密钥MDK分散生成的。图D.3是唯一DEA密钥A和B的生成流程。

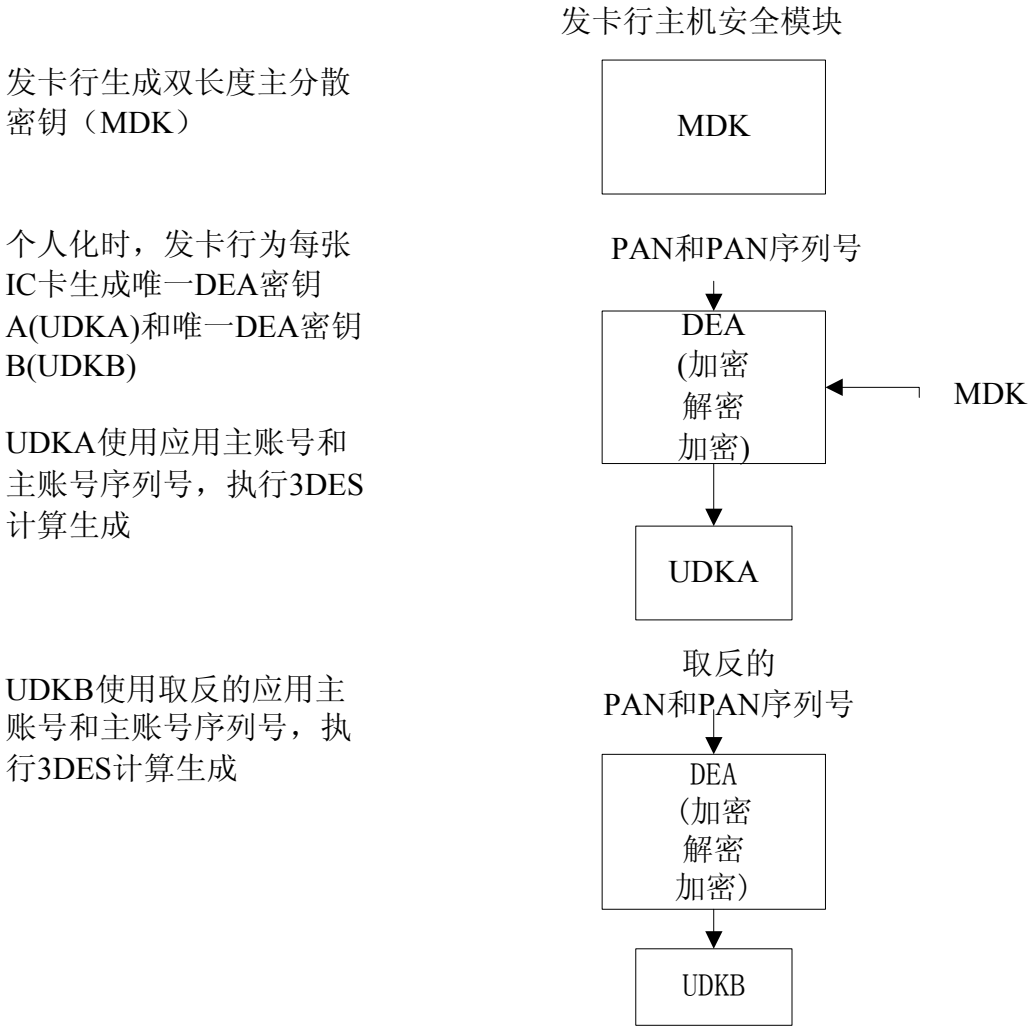


图 D.3 密钥分散

应用主账号（PAN）和应用主账号序列号用来组成一个8字节（16个数字）长的数据块D1，用来生成分散的唯一DEA密钥A。如果应用主账号序列号不存在，用一个字节00代替。如果应用主账号和应用主账号序列号的长度不等于16个数字：

——如果长度小于 16 个数字，右对齐，前面补 0；

——如果长度大于 16 个数字，取最右边 16 个数字。

上述数据块D1取反，用来生成分散的唯一DEA密钥B。

图D.4是卡片使用唯一DEA密钥A和B（UDKA和UDKB）进行卡片认证的过程。

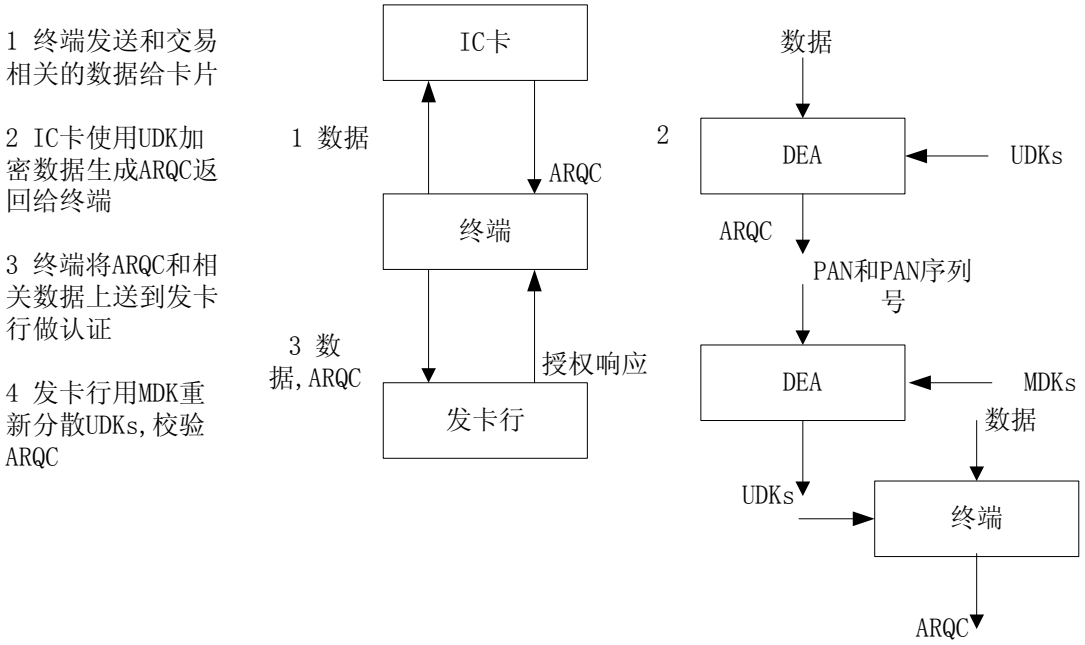


图 D.4 使用UDK执行卡片认证

如图D.4所示，主机安全模块要得到分散的UDK验证ARQC。

附 录 E
（规范性附录）
支持的密文版本

JR/T 0025定义的密文版本为01（0x01）。

表E.1列出的是生成TC/AAC和ARQC的数据元和顺序。

表 E.1 生成TC/AAC和ARQC的数据

数据元	来自终端的数据	卡片内数据
授权金额	✓	
其它金额	✓	
终端国家代码	✓	
终端验证结果	✓	
交易货币代码	✓	
交易日期	✓	
交易类型	✓	
不可预知数	✓	
应用交互特征（AIP）		✓
应用交易计数器（ATC）		✓
卡片验证结果（CVR）		✓

密文版本01使用安全规范中定义的对称密钥算法计算应用密文。

附 录 F
（规范性附录）
算法标识

发卡行自定义数据元中有一个JR/T 0025自定义数据“算法标识”。此数据定义了卡片计算应用密文和安全报文采用的算法。长度为1个字节。取值情况见表F.1。

表 F.1 算法标识

算法	值（16 进制）
3DES	01
SSF33	02

参考文献

[1] EMV支付系统集成电路卡规范：2004，第1册～第4册
[2] VISA集成电路卡应用概述，1.4.0版
[3] VISA集成电路卡卡片规范，1.4.0版
[4] VISA集成电路卡终端规范，1.4.0版