

中国金融集成电路（IC）卡  
借记/贷记规范  
第三部分：应用规范

中国金融集成电路（IC）卡标准修订工作组

二零零四年五月

# 目 次

1. 引言	1
2. 范围	1
3. 参考资料	1
4. 定义	1
5. 缩略语和符号表示	2
6. 文件、数据元、数据对象列表	3
6.1 文件结构	3
6.1.1 应用数据文件(ADF)	4
6.1.2 应用基本文件 (AEF)	4
6.1.3 文件到 ISO/IEC 7816-4 的文件结构的映射	4
6.1.4 目录结构	4
6.1.5 文件引用	5
6.2 数据元	5
6.3 数据对象列表 (DOL)	5
7. 借记/贷记交易处理流程	6
7.1 功能概述	6
7.1.1 应用选择 (强制)	6
7.1.2 应用初始化 (强制)	6
7.1.3 读应用数据 (强制)	6
7.1.4 脱机数据认证 (可选)	7
7.1.5 处理限制 (强制)	7
7.1.6 持卡人验证 (强制)	7
7.1.7 终端风险管理 (强制)	7
7.1.8 终端行为分析 (强制)	7
7.1.9 卡片行为分析 (强制)	8
7.1.10 联机处理 (可选)	8
7.1.11 发卡行脚本处理 (可选)	8
7.1.12 完成 (强制)	8
7.2 交易步骤	10
7.2.1 应用选择	10
7.2.2 应用初始化	13
7.2.3 读应用数据	16
7.2.4 脱机数据认证	19
7.2.5 处理限制	26
7.2.6 持卡人验证	29
7.2.7 终端风险管理	36
7.2.8 终端行为分析	41
7.2.9 卡片行为分析	45
7.2.10 联机处理	48
7.2.11 发卡行脚本处理	52
7.2.12 交易结束	56
7.2.13 卡片交易明细记录	60
8. 安全、密钥和数字证书	60

## 图 表

图表 7-1: 交易流程实例.....	9
图表 7-2: 应用选择处理流程图.....	12
图表 7-3: 应用初始化处理流程图.....	15
图表 7-4: 读应用数据处理流程图.....	18
图表 7-5: 脱机数据认证处理流程图.....	21
图表 7-6: 脱机数据认证处理流程.....	24
图表 7-7: 处理限制流程图.....	28
图表 7-8: 持卡人验证方法列表处理流程图.....	32
图表 7-9: PIN 验证处理流程图 (1) .....	34
图表 7-10: PIN 验证处理流程图 (2) .....	35
图表 7-11: 终端风险管理处理流程图(1).....	39
图表 7-12: 终端风险管理处理流程图(2).....	40
图表 7-13: 终端行为分析处理流程图.....	44
图表 7-14: 卡片行为分析处理流程图.....	47
图表 7-15: 联机处理流程图.....	51
图表 7-16: 发卡行脚本处理流程图.....	55
图表 7-17: 交易结束处理流程图.....	59

## 表 格

表格 6.1.5-1: SFI 结构.....	5
表格 7.2.1-1: 应用选择—卡片数据.....	10
表格 7.2.1-2: 应用选择—终端数据.....	10
表格 7.2.2-1: 初始化应用处理—卡片数据.....	13
表格 7.2.3-1: 读应用数据—上次卡片返回的卡数据.....	16
表格 7.2.3-2: 读取应用数据—卡片数据.....	16
表格 7.2.3-3: 读应用数据—卡片必备数据对象.....	17
表格 7.2.4-1: 脱机数据认证处理优先权.....	19
表格 7.2.4-2: 静态数据认证中使用的终端数据.....	20
表格 7.2.4-3: 静态数据认证中使用的卡片数据.....	20
表格 7.2.4-4: 动态数据认证中使用的终端数据.....	22
表格 7.2.4-5: 动态数据认证中使用的卡片数据.....	22
表格 7.2.4-6: 复合动态数据认证/应用密文生成中使用的卡片数据: .....	22
表格 7.2.5-1: 处理限制—卡片数据.....	26
表格 7.2.5-2: 处理限制—终端数据.....	26
表格 7.2.6-1: 持卡人验证方法列表处理—卡片数据.....	29
表格 7.2.6-2: 脱机密码验证处理—卡片数据.....	30
表格 7.2.6-3: 持卡人验证处理—终端数据.....	30
表格 7.2.7-1: 终端风险管理—卡数据.....	36
表格 7.2.7-2: 终端风险管理—终端数据.....	37
表格 7.2.8-1: 检查脱机处理结果—卡片数据.....	41
表格 7.2.8-2: 要求密文处理—卡片数据.....	41
表格 7.2.8-3: 检查脱机处理结果—终端数据.....	42
表格 7.2.8-4: 要求密文处理—终端数据.....	42

表格 7.2.9-1: 卡片行为分析—卡片数据 .....	45
表格 7.2.9-2: 卡片行为分析 — 卡片对 GENERATE AC 命令的响应 .....	46
表格 7.2.10-1: 联机处理—终端使用的卡片数据 .....	48
表格 7.2.10-2: 联机处理—卡片内部使用数据 .....	48
表格 7.2.10-3: 联机处理—终端需改变数据 .....	49
表格 7.2.10-4: 联机处理—发卡行可能返回的响应数据 .....	49
表格 7.2.11-1: 发卡行脚本处理—卡片使用的计数器和指示器 .....	53
表格 7.2.11-2: 发卡行脚本处理—终端使用的数据元 .....	53
表格 7.2.11-3: 发卡行脚本处理—联机响应数据 .....	53
表格 7.2.12-1: 交易结束—卡片使用数据元 .....	56
表格 7.2.12-2: 交易结束—GENERATE AC 命令卡片响应数据 .....	57
表格 7.2.12-3: 交易结束—终端使用数据 .....	57
表格 7.2.12-4: 交易结束—终端处理结果（脱机） .....	58
表格 7.2.12-5: 交易结束—终端处理结果（联机） .....	58
表格 7.2.13-1: 卡片交易明细—数据格式 .....	60

## 1. 引言

《中国金融集成电路（IC）卡借记/贷记应用规范》目的在于：

- 帮助银行和供应商理解 IC 卡给借贷记支付服务所带来的变化，特别是在 IC 卡和终端之间的处理方面
- 提出了 PBOC 对基于芯片卡借贷记项目的最低需求
- 确定了银行和供应商为适应市场需求所能够执行的选项
- 定义了 PBOC 关于可选择 EMV 特性的实施
- 提供了卡和终端之间处理的技术性概述，用于理解此处理和在 PBOC 借记/贷记交易流程中有相关事宜的步骤。

由于 PBOC 集成电路卡规范是以 EMV 为基础，作为参考和开发目的，可以把它们的规范说明一并使用。

## 2. 范围

《中国金融集成电路（IC）卡借记/贷记应用应用规范》适用于由银行发行或接受的金融借记贷记 IC 卡。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、集成和维护等部门（单位）。

## 3. 参考资料

### EMV 规范文档

- EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0, Book 1, Application Independent ICC to Terminal Interface Requirements
- EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0, Book 2, Security and Key Management
- EMV 2000 Integrated Circuit Card Specifications for Payment Systems, Version 4.0, Book 3, Application Specification
- EMV 2000 Integrated Circuit Card Specifications for Payment Systems, Version 4.0, Book 4, Cardholder, Attendant and Acquirer Interface Requirements

### VIS 规范文档

- VISA Integrated Circuit Card Application Overview , Version 1.4.0
- VISA Integrated Circuit Card Card Specification , Version 1.4.0
- VISA Integrated Circuit Card Terminal Specification , Version 1.4.0

### 中国集成电路（IC）卡文档

- 《中国金融集成电路(IC)卡规范》第1部分：卡片规范（V1.0）
- 《中国金融集成电路(IC)卡规范》第2部分：应用规范（V1.0）
- 《中国金融集成电路（IC）卡规范》第3部分：终端规范（V1.0）

## 4. 定义

以下定义适用于本规范：

应用 Application	卡片和终端之间的应用协议和相关的数据集
命令 Command	终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答
密文 Cryptogram	加密运算的结果
金融交易 Financial	持卡人、商户和收单行之间基于收、付款方式的商品或服务交换行为

Transaction	
功能 Function	由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易
集成电路 Integrated Circuit(IC)	完成处理和/或存储功能的电子器件
集成电路卡 (IC 卡) Integrated Circuit(s) Card	内部封装一个或多个集成电路用于执行处理和存储功能的卡片
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
发卡行行为代码 (Issuer Action Code)	发卡行根据 TVR 的内容选择的动作。
磁条 Magstripe	包括磁编码信息的条状物
路径 Path	没有分隔的文件标识符的连接
支付系统环境 Payment System Environment	当符合本规范的支付系统应用被选择，或者用于支付系统应用目的的目录定义文件 (DDF) 被选择后，IC 卡中所确立的逻辑条件
响应 Response	IC 卡处理完收到的命令报文后，返回给终端的报文
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。
终端 Terminal	为完成金融交易而在交易点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其它部件和接口，例如与主机通讯的接口
终端行为代码 (Terminal Action Code)	终端行为代码 (缺省、拒绝、联机) 反映了收单行根据 TVR 的内容选择的动作。

## 5. 缩略语和符号表示

以下缩略语和符号表示适用于本规范：

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
ADF	应用数据文件
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
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	应用交易序号 (Application Transaction Counter)
ATM	自动柜员机
AUC	应用用途控制
BER	基本编码规则 (Basic Encoding Rules)
CA	认证中心
CAM	联机卡片认证
CDA	复合动态数据认证/应用密文生成
CDOL	卡片风险管理数据对象列表 (Card Risk Management Data Object List)
CID	密文信息数据
CLA	命令报文的类别字节 (Class Byte of the Command Message)
cn	压缩数字格式
C-TPDU	命令 TPDU (Command TPDU)
CVM	持卡人验证方法 (Cardholder Verification Method)
CVR	卡片验证结果
DDA	动态数据认证
DDF	目录数据文件 (Directory Definition File)
DDOL	动态数据认证数据对象列表 (Dynamic Data Authentication Data Object List)
DF	专用文件 (Dedicated File)
DIR	目录 (Directory)
DOL	数据对象列表
GPO	获取处理选项 (GET PROCESSING OPTIONS)
EF	基本文件

EMV	Europay MasterCard VISA
FCI	文件控制信息
IAC	发卡行行为代码
IC	集成电路(Integrated Circuit)
IC 卡	集成电路卡(Integrated Circuit Card)
Lr	响应数据域的长度(Length of Response Data Field)
M	必备(Mandatory)
MAC	报文鉴别代码(Message Authentication Code)
MDK	主密钥
MF	主文件(Mater File)
n	数字型(Numeric)
O	可选(Optional)
P1	参数 1(Parameter 1)
P2	参数 2(Parameter 2)
P3	参数 3(Parameter 3)
PAN	主帐号
PBOC	中国人民银行
PKI	公钥基础设施
PIN	个人识别码
PIX	专用应用标识符扩展
RFU	保留(Reserved for Future Use)
RID	注册应用提供商标识(Registered Application Provider Identifier)
R-TPDU	响应 TPDU(Response TPDU)
SAD	签名的静态应用数据
SDA	静态数据认证
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
TC	交易证书
TDOL	交易证书数据对象列表
TLV	标签、长度、值(Tag Length Value)
TSI	交易状态信息
TVR	终端验证结果
UDK	子密钥
专用的	本规范内未定义或/和超出本规范范围的
必须	表示强制的要求
应该	表示推荐的要求

## 6. 文件、数据元、数据对象列表

### 6.1 文件结构

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

本部分描述了符合本规范的应用文件结构。

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

IC 卡中的能够读/写的数据文件中的数据对象是以记录方式保存的。文件的结构和引用方法取决于该文件的用途。文件的结构和引用的方法将在下面描述。除了下一节描述的目录文件以外，其它的 IC 卡可读/写数据文件的布局均由发卡行定义。

### 6.1.1 应用数据文件(ADF)

ADF 的树形结构:

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

从终端的角度看, ADF 是一个只包含封装在其文件控制信息(FCI)中的数据对象的文件, 参见《中国金融集成电路 (IC) 卡借记/贷记应用卡片规范》表格 B-27。

### 6.1.2 应用基本文件 (AEF)

短文件标识符(SFI)范围为 1-10 的 AEF, 包含一个基本数据对象或由多个"基本编码规则—标签长度值"(BER-TLV)的数据对象根据《中国金融集成电路 (IC) 卡借记/贷记应用卡片规范》附录 A 组成的结构 BER-TLV 数据对象 (记录)。一旦选定之后, 范围为 1-10 的 AEF 只能如6.1.3所述通过它的短文件标识符(SFI)来引用。

本规范中, 一个数据文件包括一组按记录号引用的记录序列。1-10 号 SFI 引用的数据文件中只包括那些不由卡片解释的数据, 即不在卡片内部过程中使用的数据。这种文件的结构定义成线性结构。根据 ISO/IEC 7816-4 规定, 文件结构既可以固定的, 也可以是线性可变的。这由发卡行自行选择, 并且根据本规范不会影响对文件的读操作。

### 6.1.3 文件到 ISO/IEC 7816-4 的文件结构的映射

使用下列到 ISO/IEC 7816-4 的映射:

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

在本规范中, 如果嵌入了 DF, 对与之相连的 EF 的访问是透明的。

### 6.1.4 目录结构

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

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

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

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

- 《EMV2000 支付系统集成电路卡规范 第一册》第 8 章描述的一个或多个应用模板(标签为‘61’)。
- 可能在目录自定义模板(标签为‘73’)中出现的其他数据对象, 此模板中包含的数据对象不在本规范的范围内容义。

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



6.1.5 文件引用

根据文件的种类，文件可以通过文件名或 SFI 引用。

6.1.5.1 通过文件名引用

卡片中的任何 ADF 或 DDF 都可以通过它的 DF 名引用。ADF 的 DF 名与它的 AID 对应或以 AID 作为 DF 名的开头。一张卡片中的每个 DF 名字必须在该卡内是唯一的。

6.1.5.2 通过 SFI 引用

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

SFI 的结构如下表所示：

表格 6.1.5-1：SFI 结构

数值	意义
1~10	EMV2000 规范定义
11~20	本规范定义
21~30	发卡行定义

每个 SFI 在一个应用以内必须是唯一的。范围为 11~20 的 SFI 引用的 AEF 由本规范分配管理。

6.2 数据元

定义并解释中国集成电路（IC）卡借记/贷记应用数据交换过程中卡片和终端所需的相关数据元。包括数据元的名称、标识、功能等。主要定义国内借记/贷记应用所需的特定数据元。

6.3 数据对象列表（DOL）

有时，终端应卡片的要求需要建立可变的数据元列表用来向卡片发送。为了减少 IC 卡内对这些数据的处理，这个列表不需要进行 TLV 编码，而只是把若干数据单元连接成一个复合域。因为复合域中的数据单元不是 TLV 编码的，所以当 IC 卡收到数据时，IC 卡必须知道该复合域的格式。因此，需要在 IC 卡内包含一个数据对象列表(DOL)来定义复合域中的数据格式。本规范使用的 DOL 包括：

数据对象列表	描 述
处理选项数据对象列表（PDOL）	是卡片请求的终端数据元的标签和长度的可选列表。它是终端在 SELECT 命令响应中得到的卡片 FCI 的一部分。终端在 GET PROCESSING OPTIONS 命令中向提供卡片的该列表请求的数据元。
卡风险管理数据对象列表中要求的数据（CDOL1）	在第一次 Generate AC 命令中需要传送给卡片的数据对象列表。CDOL1 是终端在读应用记录处理过程中从卡片中读出的。
CDOL2	在第二次 Generate AC 命令中需要传送给卡片的数据对象列表。CDOL2 是终端在读应用记录处理过程中从卡片中读出的。
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）
动态脱机数据认证对象列表（DDOL）	指定在 INTERNAL AUTHENTICATE 指令中，卡片要求终端送入卡片的终端数据标签和长度列表。

一个 DOL 是用一些条目连接而成的列表。每个条目代表一个加入复合域的单个数据元。每个条目地格式包括 1~2 个字节的标签来表明需要的数据对象，然后是 1 个字节的长度部分，表明本区域在命令数据中占据的字节长度。只有那些在《中国金融集成电路（IC）卡借记/贷记应用卡片规范》附录 A 中定义为基本数据对象的标签才可以在 DOL 中使用。

终端必须完成下列步骤以建立结构域：

1 从 IC 卡读取 DOL。

2 连接 DOL 中列出的所有数据单元。按照下列规则进行连接：

a) 如果 DOL 中指出的数据对象的标签无法被终端识别，或这个标签代表了一个结构数据对象，终端将提供一个长度为 DOL 指定长度的数据单元，并必须把该数据单元所有的数值部分设置为 16 进制的 0。

b) 如果该列表上的一个数据对象在终端上可以识别，但是表现为 IC 卡上不出现的可选静态数据，那么在命令区域上代表数据对象的部分必须用 16 进制的 0 来填满。

c) 如果在 DOL 条目中指出的长度小于实际数据对象的长度，则需要将实际的数据对象削减至 DOL 指出的长度。如果数据对象是数字格式(n)的，则从数据单元的的最左端开始削减字节。如果数据对象是其它格式的，则从数据单元的最右端开始削减字节。如果指出的长度比实际的数据长度大，需要把实际的数据填充至指定长度：

- 如果数据对象是数字格式(n)的, 则从数据单元头部开始填充 16 进制的 0。
- 如果数据对象是压缩数字格式(cn)的, 则在数据单元的末尾填充 16 进制的 FF。
- 如果数据对象是其它格式的, 则在数据单元的末尾填充 16 进制的 0。

d) 如果表上的一个数据对象在终端可以识别，但不代表在当前交易中适用的数据，代表该数据对象的命令域部分将填充 16 进制的 0。

数据单元在表上的连接顺序应该与相应的数据对象在 DOL 中出现的顺序一一对应。

## 7. 借记/贷记交易处理流程

### 7.1 功能概述

以下功能在中国集成电路（IC）卡借记/贷记交易处理中得到使用。尽管在强制性（M）的功能中有些步骤也许是可选择的，但标记为强制性的功能还是应该在所有交易中得到执行。标记为可选（O）的功能是可选择的并根据卡或终端的参数，或根据两者的参数共同决定

#### 7.1.1 应用选择（强制）

当中国集成电路（IC）卡借记/贷记卡片插入终端时，终端决定哪些应用由卡片和终端共同支持，终端有两种选择应用的方式：

1. 终端检测终端和卡片都支持的应用并将这些应用显示，供用户选择；
2. 终端根据发卡行事先定义的优先级别自动选择卡片上优先级最高的应用。

#### 7.1.2 应用初始化（强制）

在终端选择应用之后，必须请求卡片读取该应用的应用数据。由这些数据得知卡片具备的功能以及需要提供给卡片哪些支持。根据交易特性，例如国内或国际的，卡有可能指示不同的数据或支持功能。终端读取卡指示的数据并使用支持的功能列表来决定要执行的处理。

#### 7.1.3 读应用数据（强制）

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

#### 7.1.4 脱机数据认证（可选）

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

脱机静态数据认证(SDA)验证卡片在个人化以后重要的应用数据是否被非法修改。终端使用卡片上的发卡行公钥验证卡片静态数据，同时卡片上还包括发卡行公钥证书以及数字签名，数字签名中包括一个用发卡行私钥加密重要应用数据得到的HASH值。如果用实际数据产生的HASH值与从卡片中恢复出的HASH值相匹配，则证实了卡片数据并未被修改。

动态数据认证(DDA)主要是用于防止伪造卡片。动态数据认证有标准动态数据认证(DDA)和复合动态数据认证(DDA/AC-CDA)两种。终端要求卡片提供由IC卡私钥加密动态交易数据生成的密文，动态交易数据是由终端和卡片为当前交易产生的唯一数据。终端用从卡片数据中获取的IC卡公钥来解密动态签名。还原的数据与原始数据匹配证实了此卡不是由合法卡复制出的赝品卡。复合动态数据认证/应用密文生成把动态签名生成与卡片的应用密文生成相结合，确保卡片行为分析时返回的应用密文来自于有效卡。

#### 7.1.5 处理限制（强制）

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

#### 7.1.6 持卡人验证（强制）

终端必须具备持卡人身份验证功能。持卡人身份验证用来确认持卡人的合法性，以防止丢失或被盗卡片的使用。终端通过检查卡片的卡片验证方法列表(CVMs)确定使用何种验证方法。有以下几种方法：

- 脱机明文 PIN 验证
- 联机 PIN 验证
- 签名
- CVM 失败
- 无需 CVM
- 签名与脱机明文 PIN 验证组合
- 身份证件验证

#### 7.1.7 终端风险管理（强制）

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

#### 7.1.8 终端行为分析（强制）

终端必须具备终端行为分析功能。终端行为分析根据脱机数据认证、处理限制、持卡人验证、终端风险管理的结果以及终端和卡片中设置的风险管理参数决定如何继续交易（核准脱机、脱机拒绝、联机授权）。在由卡发送到终端的发卡行行为代码(IACs)域设立卡片规则，在终端行为代码(TACs)设立终端规则。决定交易处理之后，终端向卡片请求应用密文。不同的应用密文对应不同的交易处

理：以交易证书（TC）为核准，授权请求码（ARQC）为联机请求，应用认证密文（AAC）为拒绝。

#### 7.1.9 卡片行为分析（强制）

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

IC 卡可以决定以下方式继续交易：

1. 同意脱机完成
2. 联机授权
3. 拒绝交易

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

#### 7.1.10 联机处理（可选）

如果卡片或终端决定交易需要进行联机授权，同时终端具备联机能力，终端将卡片产生的 ARQC 报文送至发卡行进行联机授权。此报文包括 ARQC 密文，用来生成 ARQC 的数据以及表示脱机处理结果的指示器。在联机处理中，发卡行在联机卡片认证（CAM）过程中验证 ARQC 来认证卡片。发卡行可以在它的授权决定中考虑这些 CAM 结果和脱机处理结果。

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

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

#### 7.1.11 发卡行脚本处理（可选）

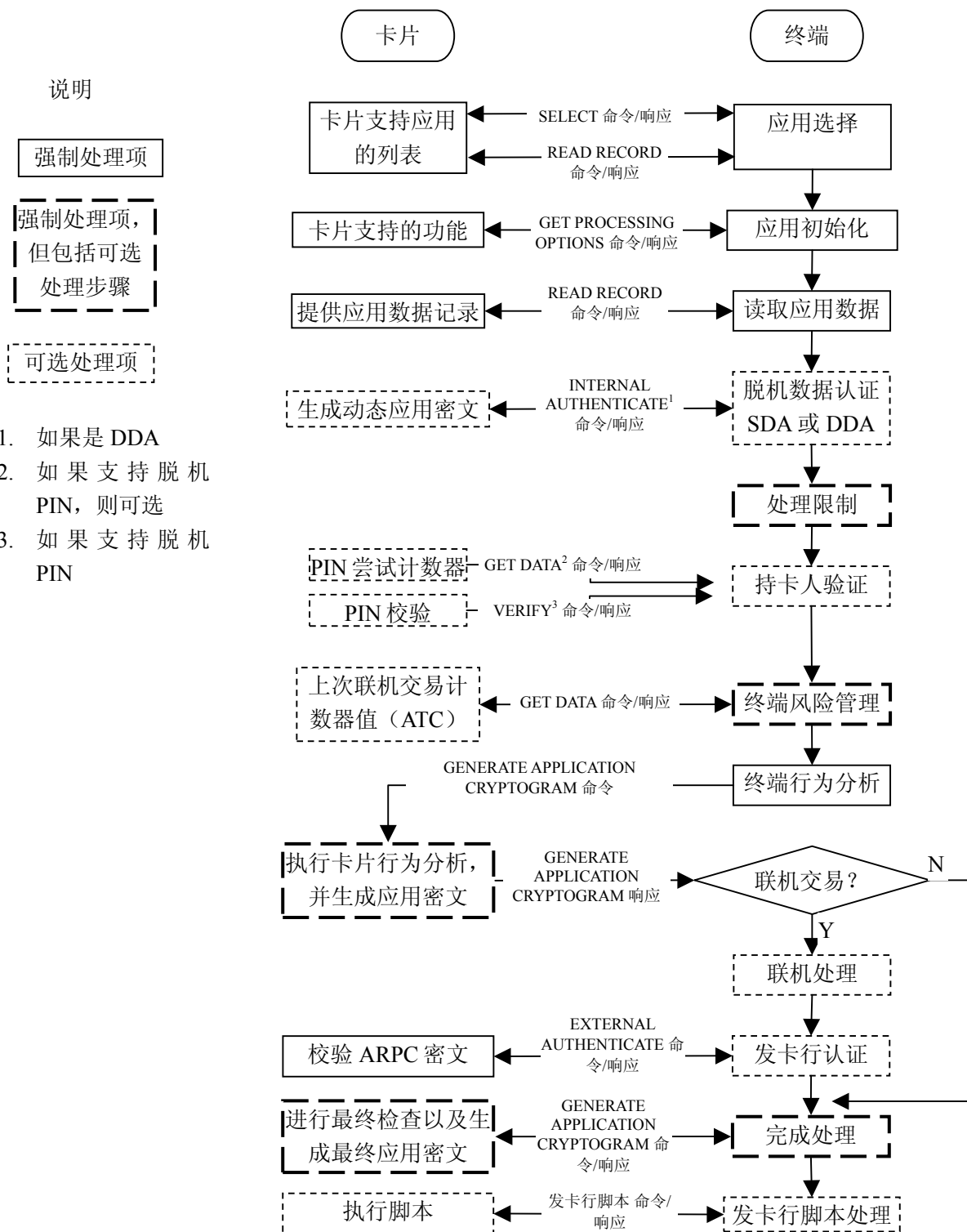
如果发卡行在授权响应报文中包含了脚本，虽然终端可能对脚本不能理解，但终端仍需要将这些脚本命令发送给 IC 卡。在使用这些更新之前，卡片执行安全检查以确保脚本来自有效的发卡行，且在传输中未有变动。这些命令对当前交易并不产生影响，主要会影响卡片的后续功能，如卡片解锁、锁卡、修改密码等。

#### 7.1.12 完成（强制）

除非交易在前几个步骤因处理异常被终止，否则终端必须执行此功能用来结束交易。

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

如果终端在授权消息之后传送清算信息，则 TC 应包括在该清算信息里。对于发卡行批准而卡片拒绝的交易，终端必须发起冲正。



图表 7-1：交易流程实例

## 7.2 交易步骤

### 7.2.1 应用选择

#### 7.2.1.1 描述

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

- 终端建立一个共同支持的应用的候选列表。
- 列表中的某个应用被选择并确认用来处理交易。

#### 7.2.1.2 卡片数据

表格 7.2.1-1：应用选择—卡片数据

数据元	说明
应用数据文件（ADF）	ADF 是一个文件，它是包含应用数据元的应用基本文件（AEF）入口。ADF 包含有关应用的信息例如应用的名称、首选语言、以及与应用优先权。
应用基本文件（AEF）	AEF 包含处理中应用所用到的数据元。
应用标识（AID）	AID 由注册的应用提供者标识（RID）以及专用应用标识符扩展（PIX）组成。
目录定义文件（DDF）	DDF 是指明在它下面文件结构的文件。
目录文件	目录文件是列出目录里所包含文件的文件。终端使用 READ RECORD 命令来访问它。
文件控制信息（FCI）	FCI 是来自卡的有关应用的信息，提供对由终端发出的 SELECT 命令做出响应。
支付系统目录	支付系统目录是包含有遵守中国集成电路（IC）卡规范应用的目录文件。
支付系统环境（PSE）	PSE 是名为“IPAY. SYS. DDF01”的 DDF。指明在 PSE 下面的文件结构的目录文件叫做支付系统目录。
处理选项数据对象列表（PDOL）	PDOL 是卡所需终端数据的标签和长度列表。终端在 SELECT 命令的卡片响应中获得它。终端在 GET PROCESSING OPTIONS 命令下提供列表中所要求的数据给卡片。
短文件标识（SFI）	SFI 是基本文件（EF）的指示器。

#### 7.2.1.3 终端数据

表格 7.2.1-2：应用选择—终端数据

数据元	说明
应用标识（AID）	AID 由注册的应用提供者标识（RID）以及专用应用标识符扩展（PIX）组成。
应用选择指示器	指示终端里相关联的 AID 是否必须与卡里的 AID 包括 AID 的长度严格匹配，或等于终端里 AID 的长度。
支持应用列表	终端应当保存终端支持应用的 AID 列表。

#### 7.2.1.4 命令

##### SELECT

终端发送 SELECT 命令到卡片以获得来自卡片支持的应用的相关信息。这个信息可以是发卡行参数例如应用选择优先权，应用名称，以及向持卡人显示信息所用的优先语言。

在卡片对 SELECT 命令的响应中，响应码用来表示处理结果。如果卡片做出响应包括处理选项数据对象列表（PDOL），则在应用初始化时处理 PDOL。

##### READ RECORD

终端发送 READ RECORD 命令到卡片，读取在 AID 选择方法列表中 PSE（如果支持目录选择）或其它

的 DDF 中的记录。命令包括读取文件的短文件标识 (SFI) 以及文件里的记录数字。

卡片对 READ RECORD 作出响应，为终端提供所要求的记录。

#### 7.2.1.5 建立候选应用列表

终端通过两个途径建立共同支持应用的列表。

- 如果终端支持目录选择法，将首先尝试此方法。如果尝试失败，终端就使用 AID 列表方法。目录选择法中，终端从卡片读取一个文件。这个文件是卡片支持的应用列表。终端将卡片应用列表和终端应用列表里共同支持的所有应用包括在候选目录中。
- AID 列表选择方法对于卡片和终端都是强制性的。在 AID 列表选择方法中，终端对终端应用列表中包含的每个应用都向卡片发送一个 SELECT 命令。如果卡片响应表示卡也支持该应用，终端就将应用添加到候选目录中。

#### 7.2.1.6 标识并选出应用

如果没有共同支持的应用，交易将被终止。如果至少有一个共同支持的应用，处理过程将如以下章节所述。

##### 7.2.1.6.1 终端决定应用

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

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

##### 7.2.1.6.2 持卡人决定应用

###### 终端支持持卡人确认

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

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

如果用目录选择法来建立应用列表，卡片对 SELECT 命令的响应可能说明该应用已被锁定。如果发生此种情况，而且在应用列表上有更多可用的应用，终端应该将该应用从可用应用列表中移出并选择下一个可用的应用进行持卡人确认。

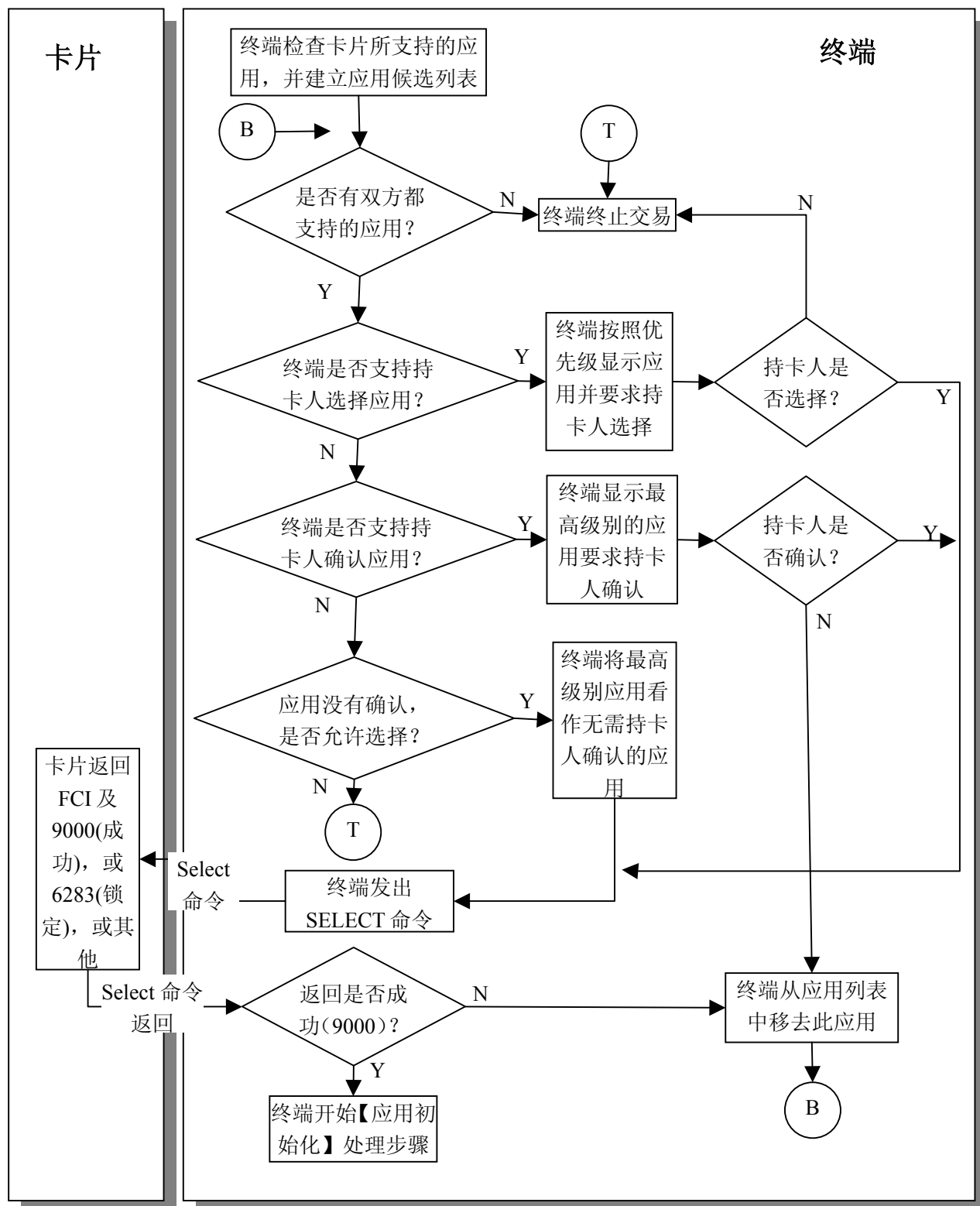
###### 终端支持持卡人选择

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

如果用目录选择法建立应用列表，卡对 SELECT 命令的响应可能说明应用已被锁定。如果发生此种情况，而且在应用列表上有更多可用的应用，终端应该显示“重试”并显示已排除了被拒绝应用的可用应用列表。

如果持卡人不选择应用，终端就终止交易。

### 7.2.1.7 流程图



图表 7-2：应用选择处理流程图



7.2.1.8 后续相关处理

初始化应用处理

终端发送到卡的 GET PROCESSING OPTIONS 包括 PDOL 指定的所有终端数据元。如果 PDOL 得到支持，应用选择时 PDOL 会被包括在 SELECT 响应里。如果地理限制不允许执行初始化所选择的应用，终端就终止交易，并返回应用选择再选择另一个应用。

7.2.2 应用初始化

7.2.2.1 描述

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

卡片在 GET PROCESSING OPTIONS 命令的响应中提供了应用文件定位器（AFL），AFL 是终端需要从卡片读取的文件和记录的列表。卡片也提供应用交互特征（AIP），它是处理交易时卡片所执行功能的列表。

7.2.2.2 卡片数据

表格 7.2.2-1：初始化应用处理—卡片数据

数据元	说明
应用文件定位器（AFL）	指示交易处理过程中终端需要的卡片数据所在卡片文件的短文件标识符（SFI）和记录范围。
应用交互特征（AIP）	指示在此应用中卡片支持特定功能的能力列表，包括静态数据认证（SDA），动态数据认证（标准 DDA），持卡人验证，发卡行认证，以及复合动态数据认证（DDA/AC）。
文件控制信息（FCI）	FCI 是卡片相关应用的信息，在终端发送的 SELECT 命令的响应中。
处理选项数据对象列表（PDOL）	PDOL 是卡片请求的终端数据元的标签和长度的可选列表。它是终端在 SELECT 命令响应中得到的卡片 FCI 的一部分。终端在 GET PROCESSING OPTIONS 命令中向提供卡片的该列表请求的数据元。

7.2.2.3 终端数据

终端将标签为“9F65”的交易明细数据元通过 PDOL 传送给卡片。

7.2.2.4 命令

GET PROCESSING OPTIONS

终端 GET PROCESSING OPTIONS 命令通知卡片交易处理开始。终端使用一个列表（若存在），叫做处理选项数据对象列表（PDOL），是卡片在应用选择时提供的。终端在 GET PROCESSING OPTIONS 命令提供卡片 PDOL 中指定的终端数据。

7.2.2.5 处理流程

7.2.2.5.1 终端处理

对应用初始化，终端：

1. 从 SELECT 命令响应中的文件控制信息（FCI）中提取处理选项数据对象列表（若存在）。
2. 向卡片发送 GET PROCESSING OPTIONS 命令。在这个命令中，终端组织所有卡片在 PDOL 中请求的数据元并传递给卡片。

#### 7.2.2.5.2 卡片处理

一旦收到 GET PROCESSING OPTIONS 命令，卡片就执行下列动作：

决定将要读取的文件或记录（它们可以根据国内/国际而不同）并定位或建立 AFL。终端可能在 GET PROCESSING OPTIONS 响应中得到不同的 AIP 返回。

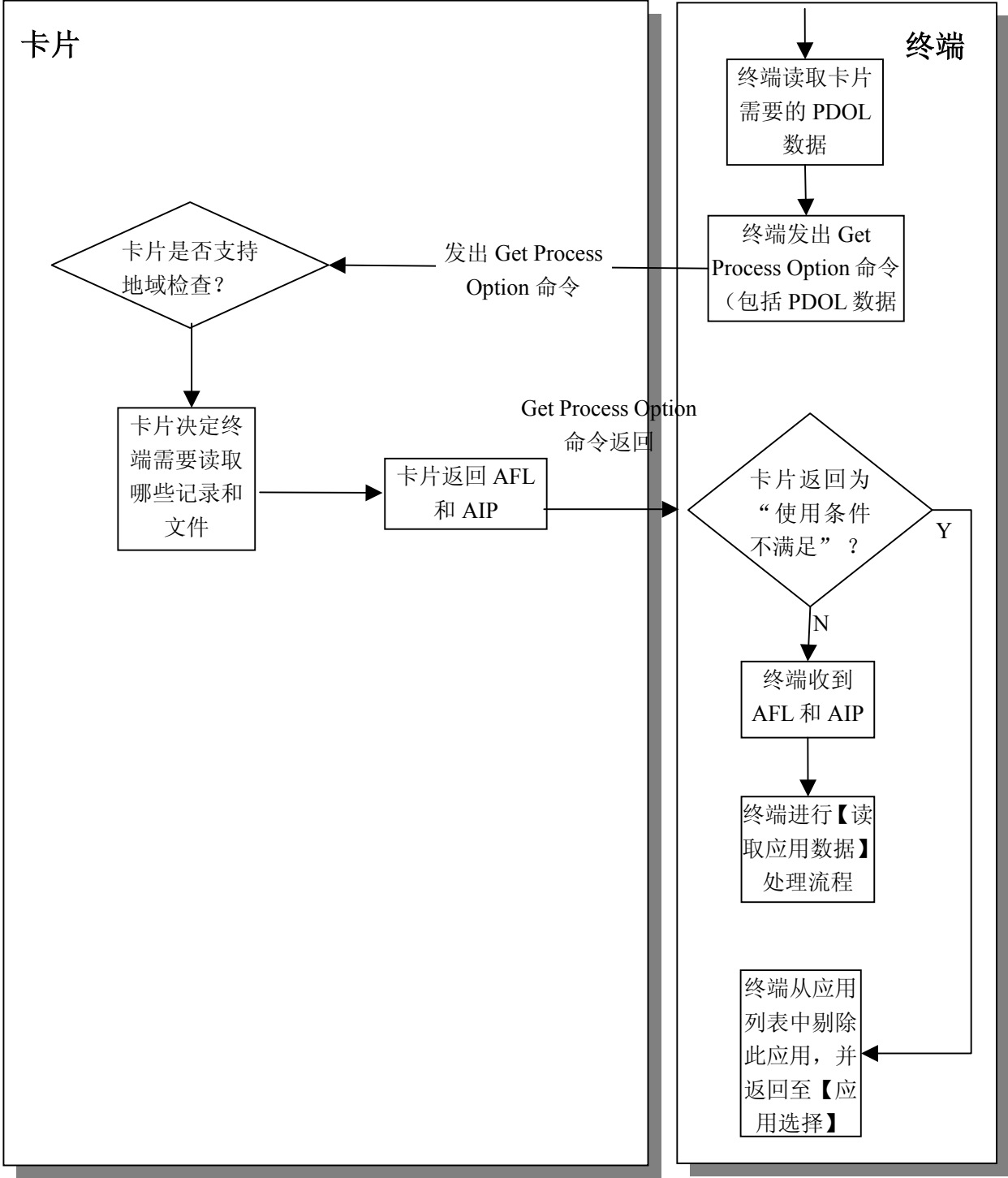
#### 7.2.2.5.3 终端处理

终端对卡片 GET PROCESSING OPTIONS 命令响应进行如下处理：

1. 接收卡片对 GET PROCESSING OPTIONS 命令的响应
2. 如果卡片响应为“使用条件不满足”，终端：
  - a. 将该应用从可用应用列表里删除
  - b. 返回应用选择
3. 如果卡片用 AIP 和 AFL 做出响应，终端：

开始读取应用数据

7.2.2.6 流程图



图表 7-3：应用初始化处理流程图

7.2.2.7 前期相关处理

应用选择

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

7.2.2.8 后续相关处理

读取应用数据

终端使用 GET PROCESSING OPTIONS 命令响应中由卡片提供的 AFL，来确定从卡片读取哪些应用数据以及哪些应用数据将要用到脱机数据认证中。

脱机数据认证

终端使用 GET PROCESSING OPTIONS 命令响应中由卡片提供的 AIP，来确定卡片是否支持脱机数据认证。

持卡人验证

终端使用 GET PROCESSING OPTIONS 命令响应中由卡片提供的 AIP，来确定卡片是否支持持卡人验证。

联机处理

终端使用 GET PROCESSING OPTIONS 命令响应中由卡片提供的 AIP，来确定卡片是否支持发卡行认证。

7.2.3 读应用数据

7.2.3.1 描述

读取应用数据时，终端读取交易处理中必要的卡片数据，并决定静态数据认证（SDA）或动态数据认证（DDA）中使用的数据。

7.2.3.2 卡片数据

表格 7.2.3-1：读应用数据—上次卡片返回的卡数据

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

表格 7.2.3-2：读取应用数据—卡片数据

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

下表列出了读记录时，IC 卡中必须具备的数据对象。本规范中定义的其它 IC 卡数据对象都是可选的。

表格 7.2.3-3: 读应用数据—卡片必备数据对象

标签	值	存在性
‘5F24’	应用失效日期	必备
‘5A’	应用主帐号	必备
‘8C’	卡片风险管理数据对象列表 1	必备
‘8D’	卡片风险管理数据对象列表 2	必备

### 7.2.3.3 终端数据

读取应用数据功能中不使用终端数据。

### 7.2.3.4 命令

#### READ RECORD

终端为每个要读取的记录向卡片发送一条 READ RECORD 命令给。此命令包括标识文件的一个短文件标识符 (SFI) 以及一个记录号来标识文件里的记录。

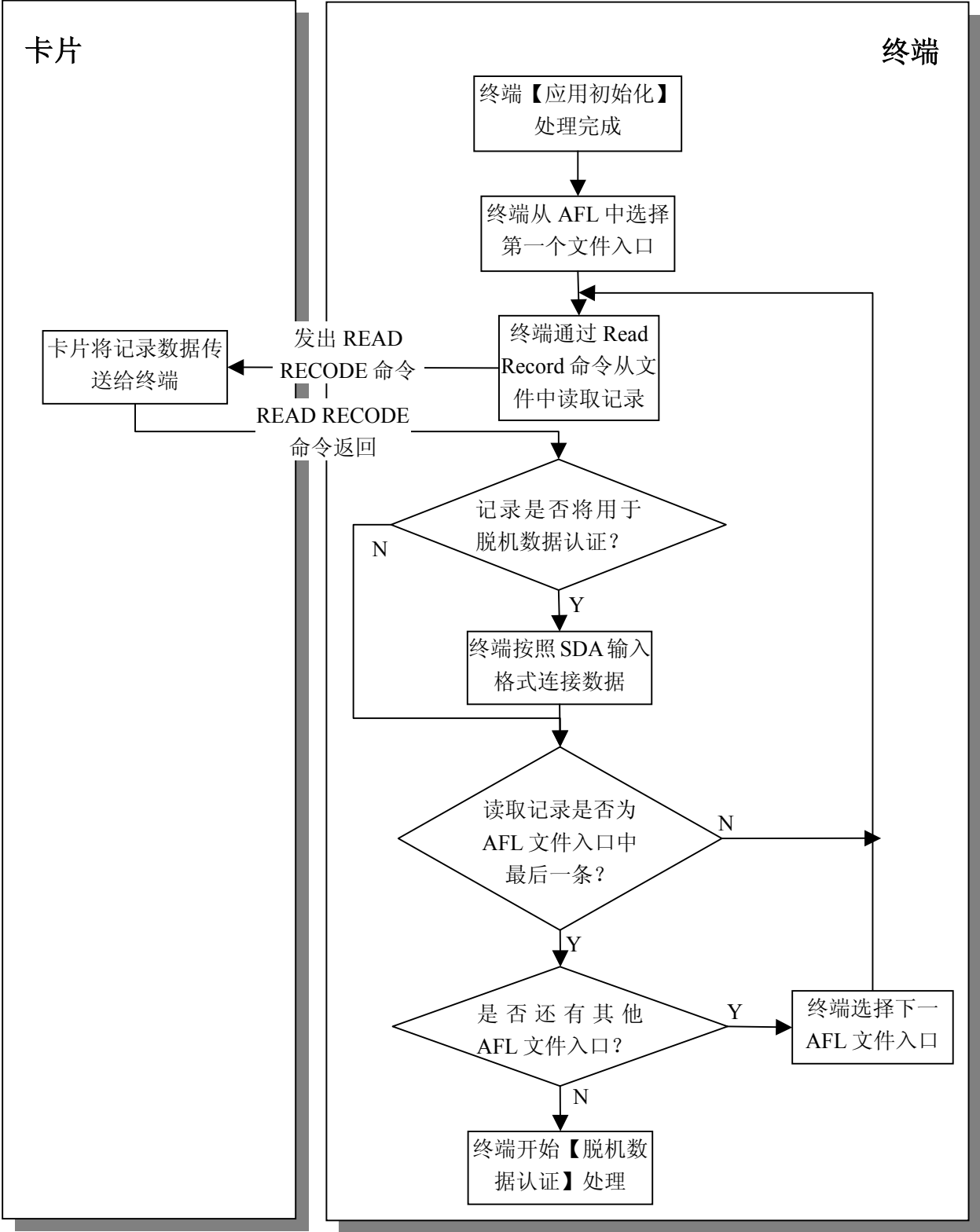
卡片在 READ RECORD 命令的响应提供被请求的记录。

### 7.2.3.5 处理流程

终端根据卡片的应用文件定位器 (AFL) 决定从卡片读取哪些记录。

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

7.2.3.6 流程图



图表 7-4：读应用数据处理流程图

7.2.3.7 前期相关处理

终端使用应用初始化时卡片提供的 AFL，以读取应用数据。

7.2.3.8 后续相关处理

脱机数据认证

SDA 和 DDA 用读取应用数据时建立的静态数据认证列表来验证带签名的静态数据。

其他功能

其他功能用读取应用数据时得到的数据进行处理。

7.2.4 脱机数据认证

7.2.4.1 描述

脱机数据认证是终端使用非对称 公钥技术认证来自卡片数据的处理过程。

脱机数据认证有两种形式：

- 静态数据认证（SDA）
- 动态数据认证（DDA）

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

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

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

所有允许脱机交易的终端对静态数据认证的支持是强制性的，并推荐支持动态数据认证。对于卡片而言，脱机数据认证支持是可选的。

7.2.4.2 密钥及认证

参见《中国金融集成电路（IC）卡借记/贷记应用安全规范》。

7.2.4.3 确定脱机数据认证的方法

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

表格 7.2.4-1：脱机数据认证处理优先权

卡应用交互特征（AIP） 表明卡支持	终端支持静态数据认证（SDA）	终端支持静态数据认证（SDA）和标准动态数据认证（DDA）	终端支持静态数据认证（SDA），标准动态数据认证（DDA）及复合动态数据认证/应用密文生成（CDA）
静态数据认证	静态数据认证	静态数据认证	静态数据认证
静态数据认证	静态数据认证	标准动态数据认证	标准动态数据认证

标准动态数据认证	证		
静态数据认证 标准动态数据认证 复合 DDA/应用密文生成	静态数据认证	标准动态数据认证	复合动态数据认证/应用密文生成

#### 7.2.4.4 静态数据认证（SDA）

当执行静态数据认证时，下表描述终端和卡片的重要数据以确认此卡片数据未被改变。

表格 7.2.4-2：静态数据认证中使用的终端数据

数据元	说明
认证中心（CA）公钥	储存在终端的支付系统公钥，用于恢复来自卡的用认证中心私钥签署的发卡行公钥证书。
认证中心（CA）公钥索引（PKI）	与 RID 一同使用，用来指定哪个 PBOC 认证中心公钥用于脱机数据认证。
注册的应用提供者标识（RID）	标识支付系统的应用标识符的一部分。
终端校验结果（TVR）	从终端角度来看的处理功能情况。

表格 7.2.4-3：静态数据认证中使用的卡片数据

数据元	说明
认证中心公钥索引(PKI)	静态数据认证中，用来标识脱机数据认证的每个 PBOC 公钥，与注册的应用提供者标识一起标识每个认证公钥。
发卡行公钥证书	发卡行公钥证书包含用 PBOC 认证中心私钥签署的发卡行公钥。
发卡行公钥指数	在非对称算法中使用该指数来恢复公钥证书。
发卡行公钥余项	如果有必要，发卡行公钥余项包含发卡行公钥未列入发卡行公钥证书的部分。
静态数据认证失败指示器	内部指示器，如果静态数据认证失败且交易被脱机拒绝进行，则它由卡片设置并保存。
签名静态应用数据(SAD)	静态应用数据是用发卡行私钥加密的签名，包含卡片重要数据的哈希值。

##### 7.2.4.4.1 处理流程

静态数据认证中，卡片没有执行任何处理。以下概述了终端执行的处理。

##### 1. 认证中心公钥的获取

终端使用卡片上的认证中心公钥索引（PKI）以及注册应用提供者标识来获取存储在终端的 PBOC 认证中心公钥和相关信息。

##### 2. 发卡行公钥的获取

终端用 PBOC 认证中心公钥从发卡行公钥证书中恢复出发卡行公钥。发卡行公钥证书的格式是经过验证的。

##### 3. 签名静态应用数据的验证

终端用发卡行公钥恢复签名静态应用数据，此数据包含卡片个人化所计算出的卡片数据的哈希值。终端计算实际数据元的哈希值。此哈希值与被恢复数据的哈希值相比较。如果这些哈希值不相等，则数据可能被改变过，静态数据认证失败了。

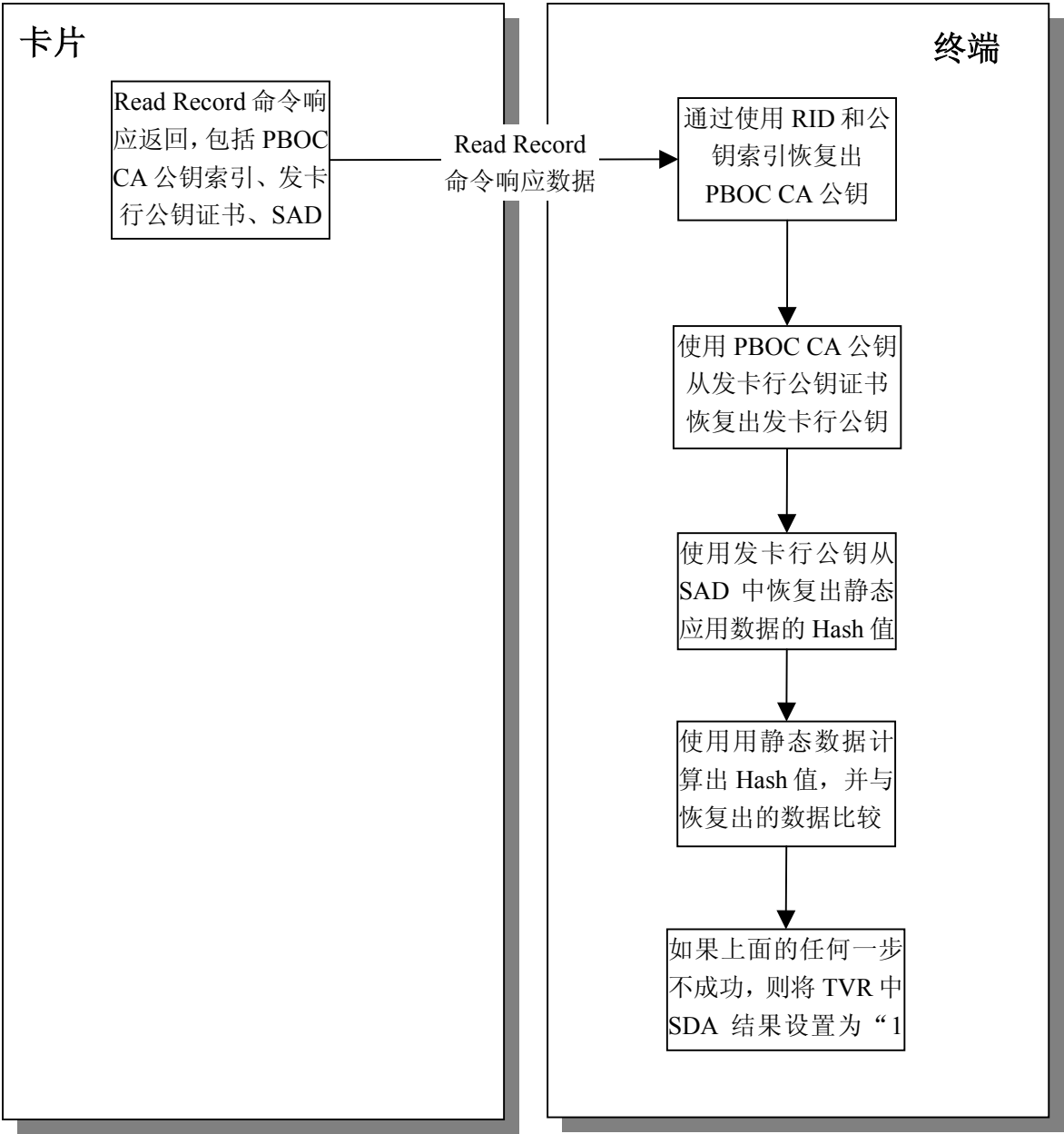
##### 4. 静态数据认证结果

如果以上所有步骤得以成功执行，则静态数据认证通过。

如果静态数据认证失败，终端设置终端验证结果中的相应指示器，以显示静态数据认证结果，并在随后的处理中使用该指示器决定交易的处理。



7.2.4.4.2 静态数据认证处理流程图



图表 7-5：脱机数据认证处理流程图

7.2.4.5 动态数据认证（DDA）

如果要执行脱机动态数据认证，终端用发卡行公钥和 PBOC 认证中心公钥验证卡片的静态数据，处理过程和静态数据认证相似。验证了静态数据后，终端向卡片申请动态签名。这要求使用内部认证命令实现标准动态数据认证以及使用第一个 AC 生成命令实现复合动态数据认证/应用密文生成。

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

终端用已从 IC 卡公钥证书中恢复的 IC 卡公钥将卡片的签名解密。恢复的数据被用来与实际的数

据比较来确定动态数据认证是否通过。成功的动态数据认证意味着卡片数据没有被改变且不是伪卡。

#### 7.2.4.5.1 动态数据认证处理的数据元

终端将用静态数据认证的终端数据和下表中描述的附加动态数据认证数据进行动态数据认证。

表格 7.2.4-4：动态数据认证中使用的终端数据

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

所有的静态数据认证数据，除签名静态应用数据以外，都用于动态数据认证。此外，下表中描述的数据也用于动态数据认证。

表格 7.2.4-5：动态数据认证中使用的卡片数据

数据元	说明
动态数据认证失败指示器	内部指示器，如果标准动态数据认证失败且交易被脱机拒绝，则它由卡片设置并保存。
动态数据认证数据对象列表（DDOL）	动态数据认证处理中，要传递给卡片的终端数据对象的标签列表。
IC 卡动态数字	卡片生成的唯一数字，并作为复合动态数据认证/应用密文生成中动态签名的部分由终端验证。
IC 卡私钥	卡片用它生成动态签名。
IC 卡公钥证书	IC 卡公钥证书包含用发卡行私钥签名的 IC 卡公钥。
IC 卡公钥指数	在非对称算法中使用该指数来恢复 IC 卡公钥证书。
IC 卡公钥余项	如果有必要，IC 卡公钥余项包含 IC 卡公钥未列入 IC 卡公钥证书的部分。

所有在标准动态数据认证中使用的数据元，除动态数据认证数据对象列表以外，都用于复合动态数据认证/应用密文生成。此外，下表中描述的数据也被使用。

表格 7.2.4-6：复合动态数据认证/应用密文生成中使用的卡片数据：

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

#### 7.2.4.5.2 标准动态数据认证(DDA)处理流程

这个处理过程，除了动态签名由卡片生成以外，其他都是由终端执行的。以下概述了这个处理过程。

##### 1. 认证中心公钥的获取

终端用认证中心公钥索引（PKI）以及卡中的注册应用提供者标识来获取储存在终端中的 PBOC 认证中心公钥以及相关信息。

##### 2. 发卡行公钥的获取

终端用 PBOC 认证中心公钥从发卡行公钥证书中将发卡行公钥恢复。发卡行公钥证书的格式是经过验证的。

##### 3. IC 卡公钥的获取

终端用发卡行公钥解密包含 IC 卡公钥和静态应用数据哈希值的 IC 卡公钥证书。终端把此哈希值与被恢复数据的哈希值相比较来验证它。如果这些哈希值不相等，则动态数据认证失败。

##### 4. 动态签名生成（仅标准动态数据认证）

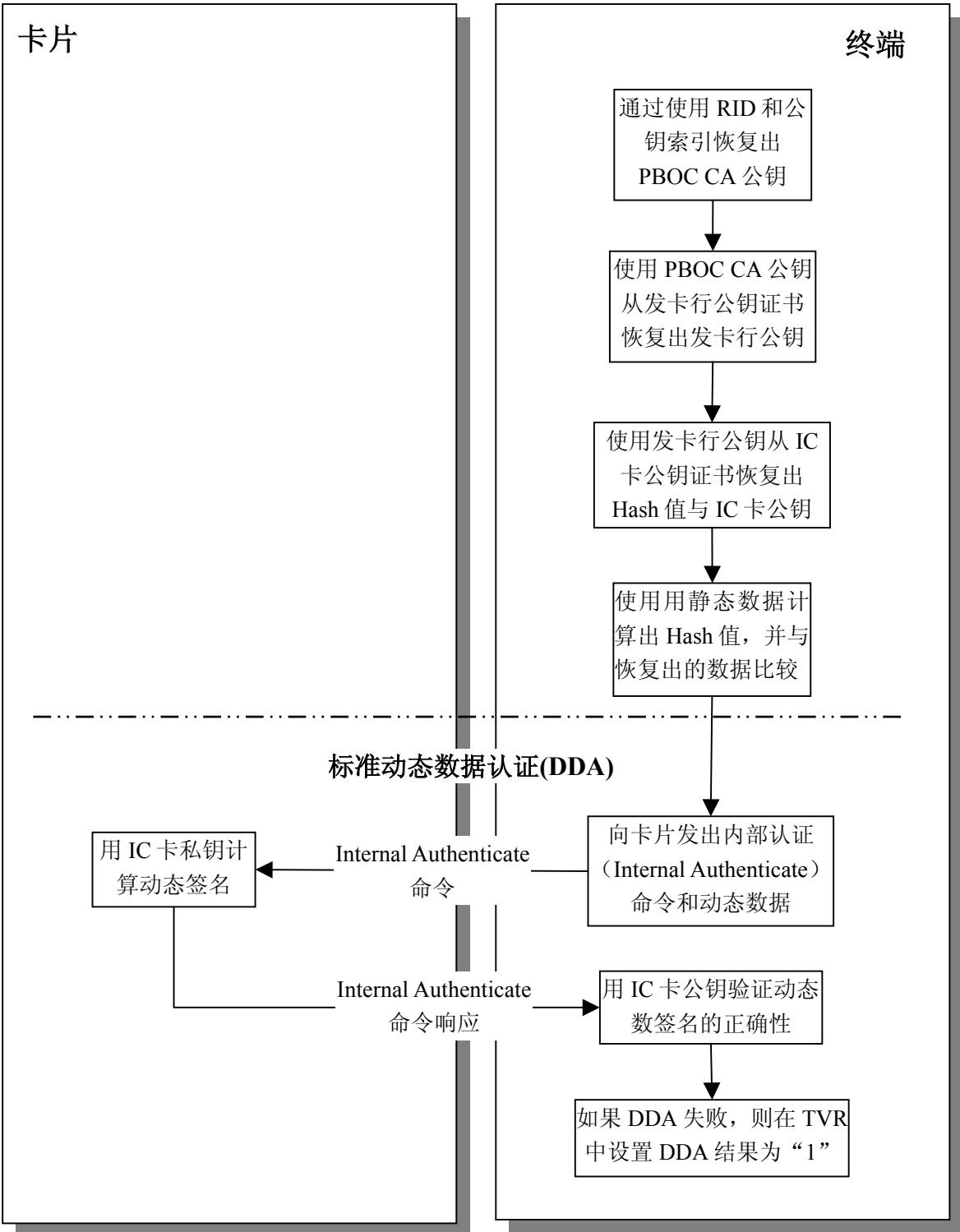
终端传送包括动态随机数的 INTERNAL AUTHENTICATE 命令到卡。

一收到 INTERNAL AUTHENTICATE 命令，卡片就用 IC 卡私钥加密终端、卡片动态数据的哈希值来生成一个动态签名。卡片再把此动态签名传递给终端。

##### 5. 动态签名校验（仅标准动态数据认证）

终端用从 IC 卡公钥证书恢复的 IC 卡公钥并解密动态签名。如果终端生成的实际动态数据哈希值与恢复的哈希值不一致，则动态数据认证失败。

7.2.4.5.3 动态数据认证处理流程图



图表 7-6：脱机数据认证处理流程

7.2.4.5.4 复合动态数据认证/应用密文生成(CDA)处理流程

对于复合动态数据认证/应用密文生成，终端执行标准动态数据认证的步骤 1 到 3。终端要求使用

第一个 GENERATE AC 命令生成的动态密文。不使用 INTERNAL AUTHENTICATE 命令。对此密文的要求和认证包括以下步骤：

#### 1. 动态签名生成（仅复合动态数据认证/应用密文生成）

终端行为分析中，如果终端要求一个联机密文（授权请求密文）或脱机批准密文（交易证书），第一个 GENERATE AC 命令表明复合动态数据认证/应用密文生成即将被执行。如果卡片决定的应用密文是一个交易证书或授权请求密文，卡片就用 IC 卡私钥签名应用密文及相关数据，并在 GENERATE AC 命令响应中把动态签名返回给终端。

#### 2. 动态签名校验（仅复合动态数据认证/应用密文生成）

卡片行为分析中，如果最初的 GENERATE AC 响应包含一个交易证书或授权请求密文，终端就用在 7.2.4.5.2 步骤 3 恢复的 IC 卡公钥将动态签名解密。如果签名成功地恢复了，处理就根据所收到的密文的类型继续下去。如果签名恢复失败，则交易就脱机拒绝。

### 7.2.4.6 前期相关处理

#### 读取应用数据

终端从卡片读取应用数据，此数据包括为支持脱机数据认证方法所要求的数据。应用文件定位器和静态数据认证标签列表指明了静态数据认证中用于认证静态数据哈希值的数据、以及动态数据认证中的 IC 卡公钥证书，

### 7.2.4.7 后续相关处理

#### 终端行为分析

终端用脱机数据认证结果，卡片和终端参数来决定交易是否要被脱机拒绝，还是进行联机认证，或脱机批准。当要执行复合动态数据认证/应用密文生成且交易要被发送联机或脱机批准时，终端在 GENERATE AC 命令里设置了复合动态数据认证/应用密文生成指示器。

#### 卡片行为分析

#### 静态数据认证和标准动态数据认证

如果上笔交易静态数据认证失败且交易被脱机拒绝，卡片就设置 CVR 中的相关指示器。如果上笔交易动态数据认证失败且交易被脱机拒绝，卡片也在 CVR 设置一个类似的指示器。

如果静态数据认证或动态数据认证失败了，且要脱机拒绝交易，就设置静态数据认证失败指示器或动态数据认证失败指示器。

#### 复合动态数据认证/应用密文生成

如果从终端收到 GENERATE AC 命令表明将要执行复合动态数据认证/应用密文生成，卡片就返回授权请求密文和交易证书应用密文，该密文用 IC 卡私钥签名。

#### 联机处理

#### 复合动态数据认证/应用密文生成

当返回的应用密文是动态签名，终端用 IC 卡公钥解密此签名。如果解密成功，终端就根据应用密文把处理继续下去。如果解密失败，则交易就脱机拒绝。

#### 完成

联机认证后，卡片允许根据发卡行认证选项和结果来重设静态数据认证失败指示器或动态数据认证失败指示器。

如果静态数据认证或动态数据认证失败了，且因联机认证不能完成，交易要被脱机拒绝，就设置

静态数据认证失败指示器或动态数据认证失败指示器。

## 复合动态数据认证/应用密文生成

如果复合动态数据认证/应用密文生成失败且返回的应用密文是授权请求密文，含应用认证密码的第二个 GENERATE AC 命令就被发送到卡。如果复合动态数据认证/应用密文生成失败且返回的应用密文是交易证书，则交易被脱机拒绝并不要求第二个 GENERATE AC 命令了。

### 7.2.5 处理限制

#### 7.2.5.1 描述

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

#### 7.2.5.2 卡片数据

下表列出并描述了处理限制中用到的卡数据元。这些数据元及其用法的详细说明请参阅《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 A，卡片和发卡行数据元表。

表格 7.2.5-1：处理限制—卡片数据

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

#### 7.2.5.3 终端数据

下表列出并描述了处理限制中用到的卡片数据元。这些数据元及其用法的详细说明请参阅《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 A，卡和发卡行数据元表。

表格 7.2.5-2：处理限制—终端数据

数据元	说明
应用版本号	该数据元（终端标签“9F09”）表明了终端的应用版本，它被终端用于应用版本号的检查，遵循此规范的卡应用版本号为 xxx（待定 1）。
终端性能	表明终端关于卡片数据输入，持卡人验证和安全的性能。由终端用于应用用途控制的检查。
终端国家代码	该数据元表明终端所在的国家，由终端用于应用用途控制检查。
交易日期	这是终端提供的交易发生的当地日期，由终端用于应用生效期和失效日期检查。
交易类型	该数据元表明金融交易的类型，由终端用于应用用途控制检查。

#### 7.2.5.4 应用版本号检查

终端把卡片的应用版本号和终端的应用版本号相比较，看它们是否相同。如果不相同，终端在终端验证结果（TVR）里显示出应用版本不一致。

#### 7.2.5.5 应用用途控制检查

应用用途控制检查过程中，终端检查了交易点各方面的情况以决定处理是否要继续。这些检查和为磁条卡交易执行的服务码检查类似，下列交易包括这些限制检查：

- 国内
  - ✓ 现金
  - ✓ 商品
  - ✓ 服务
- 国际
  - ✓ 现金
  - ✓ 商品
  - ✓ 服务
- ATM
- 除 ATM 外的设备

#### 7.2.5.6 应用生效日期检查

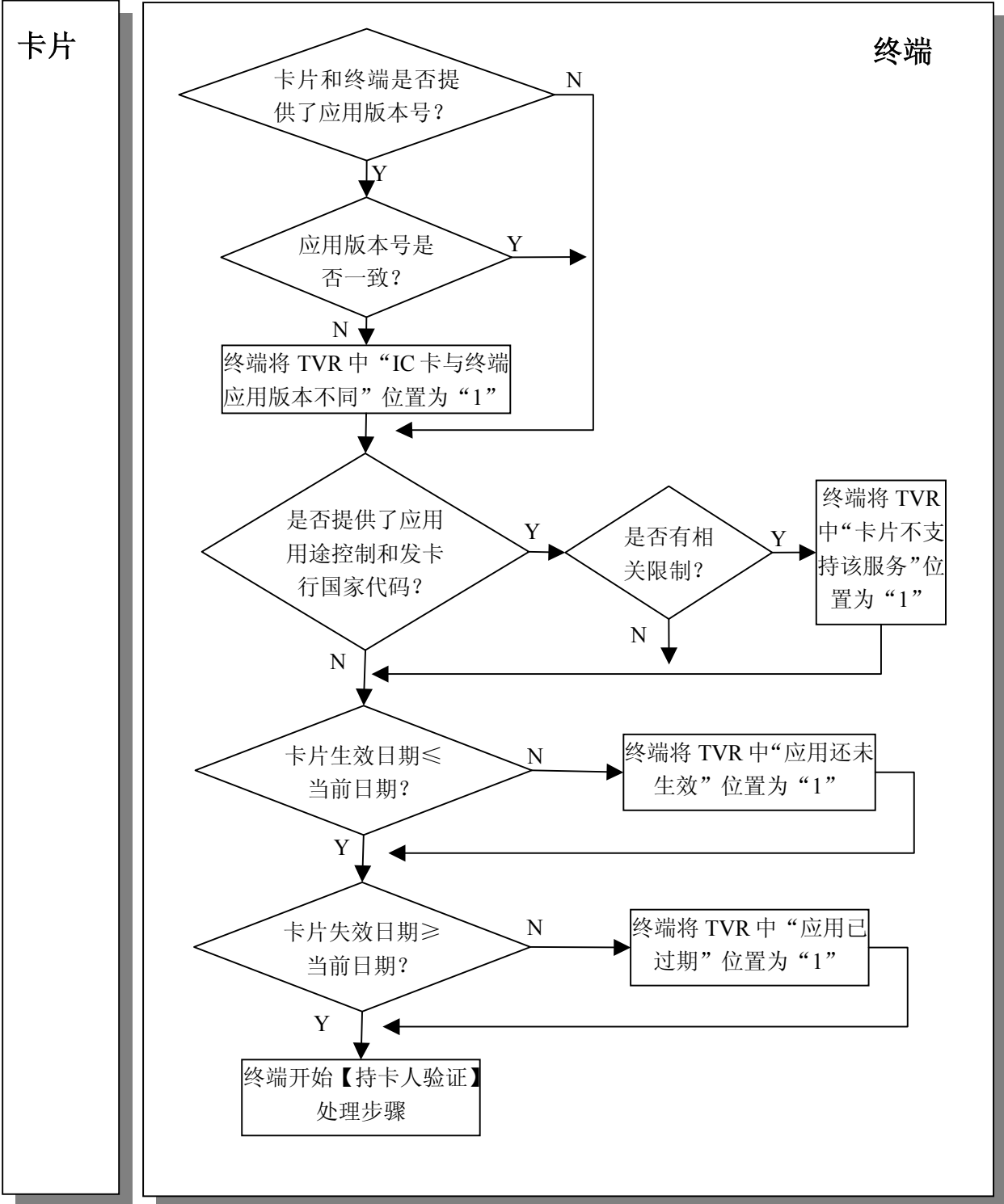
应用生效日期检查通过验证卡片的应用生效日期（如果存在）早于等于终端的当前交易日期，确认应用已经生效。如果生效日期晚于交易日期，终端就在终端验证结果中指示应用还未生效。

对于卡片，应用生效日期是可选的。对于终端，如果卡片存在该数据元，应用生效日期的检查就是强制性的。

#### 7.2.5.7 应用失效日期检查

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

7.2.5.8 处理限制流程图



图表 7-7：处理限制流程图



### 7.2.5.9 前期相关处理

#### 读取应用数据

终端使用 READ RECORD 命令获得应用版本号以及卡片的应用失效日期。如果存在，应用用途控制、发卡行国家代码和应用生效日期，则它们也被从卡中读取出来。

### 7.2.5.10 后续相关处理

#### 终端行为分析

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

## 7.2.6 持卡人验证

### 7.2.6.1 描述

持卡人验证用来确保持卡人是合法的，卡片不是丢失的或被盗的。

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

支持的持卡人验证方法有：

- 脱机明文 PIN 验证
- 联机 PIN 验证
- 签名
- CVM 失败
- 无需 CVM
- 签名与脱机明文 PIN 验证组合
- 身份证件验证

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

终端从卡片规定的持卡人验证方法列表中选择要采用的持卡人验证方法。持卡人验证方法列表中的选择准则可包括交易类型（取现或消费）、交易金额、以及终端性能。如果持卡人验证失败，持卡人验证方法列表也会指定终端的行为。

### 7.2.6.2 卡片数据

终端将表格 7.2.6-1 和表格 7.2.6-2 中描述的卡片数据用于持卡人验证方法列表处理。这些卡数据元及其用法的详细说明请参阅《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 A，卡和发卡行数据元表。

表格 7.2.6-1：持卡人验证方法列表处理—卡片数据

数据元	说明
应用交互特征（AIP）	包含一个指示器，标明卡片是否支持持卡人验证。此指示器必须设置为“1”。
持卡人验证方法（CVM）列表	卡片应用持卡人验证方法列表先后顺序。卡片可以包含多种的持卡人验证方法列表以用于不同的环境，比如国际和国内交易。持卡人验证方法列表包含以下部分： <ul style="list-style-type: none"><li>● 金额 X—可能在持卡人验证方法使用条件中用到的金额</li><li>● 金额 Y—可能在持卡人验证方法用法条件中用到的第二个金额</li><li>● 持卡人验证方法条目—持卡人验证方法列表可能包括不止一个条目，每个条目包含以下子域：</li></ul>

子域	说明
持卡人验证方法代码	如果持卡人验证失败，即指定要采取的行动。可以选择处理下一个持卡人验证方法或中止持卡人验证处理。
持卡人验证方法类型	持卡人验证方法要执行的类型，例如脱机密码验证。
持卡人验证方法条件	当要用到持卡人验证方法条目时的条件，例如，如果终端支持该持卡人验证方法类型（脱机密码）。
请参阅《中国集成电路（IC）卡借记/贷记卡片规范》持卡人验证一章，发卡行怎样定义持卡人验证方法的例子。	

表格 7.2.6-2：脱机密码验证处理—卡片数据

数据元	说明
应用缺省行为（ADA）	如果脱机密码重试次数超限，卡片用该数据元来决定要采取怎样的行动。
卡片验证结果（CVR）	包含卡片为下列情况设置的指示器： <ul style="list-style-type: none"> <li>• 执行了脱机密码验证</li> <li>• 脱机密码验证失败</li> <li>• 密码重试次数超限</li> <li>• 因密码重试次数超限，应用锁定</li> </ul>
密码重试次数计数器	剩余的脱机密码重试次数。每次持卡人脱机密码验证失败时，密码重试次数计数器都减 1。如果持卡人输入与存储在卡中参考密码一致的密码或重置密码重试次数计数器的脚本命令执行成功，密码重试次数计数器被重置为密码重试次数上限。
密码重试次数上限	针对某一应用，发卡行指定的所能允许的连续输入错误密码的最大次数。
参考密码	持卡人密码，储存在卡片的安全位置。

### 7.2.6.3 终端数据

下表中描述的终端数据用于持卡人验证处理。这些数据元及其用法的详细说明请参阅《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 A，卡片和发卡行数据元表。

表格 7.2.6-3：持卡人验证处理—终端数据

数据元	说明
加密个人密码（PIN）数据	在密码键盘加密交易密码用于联机验证。
个人密码（PIN）键盘保密密钥	密码键盘使用的用来加密输入的脱机密码的保密密钥，且读卡机用它来给加密密码解密。当密码键盘和读卡机没有集成为一个不受外界干预的一体设备，这个密钥是必须的。此密钥和用于脱机加密密码的密钥不同。
终端性能	标明了终端支持的持卡人验证方法。
终端校验结果（TVR）	在终端校验结果里为下列情况设置指示器： <ul style="list-style-type: none"> <li>• 持卡人验证不成功</li> <li>• 未被认可的持卡人验证方法</li> <li>• 密码输入次数超限</li> <li>• 需要密码输入而没有密码键盘或密码键盘不能工作</li> <li>• 需要密码输入，有密码键盘但密码没有输入</li> <li>• 输入联机密码</li> </ul>
交易个人密码（PIN）	包含持卡人为密码验证输入的数据。

### 7.2.6.4 命令

以下命令用于脱机密码处理：

#### GET DATA

终端用这条命令从卡片获取密码重试计数器以便决定在先前的交易中密码输入次数是否超限，或接近超限。

GET DATA 命令包含了密码重试计数器标签。如果密码输入计数器在一个私有数据文件内，卡就将一个错误响应返回给 GET DATA，于是终端避开检查密码输入次数计数器，继续脱机密码验证处理。

## VERIFY

用于脱机明文密码

VERIFY 命令包括持卡人输入的密码并开始卡片对这个密码与储存在卡上的参考密码的比较。

卡片的响应指出下列情况中的一种：

- 密码匹配
- 密码不相符，且密码重试的剩下次数是“n”。如果“n”等于“0”，则在当前交易中，密码输入次数已经超过了
- 先前交易中，密码输入次数就已超过了

如果卡片和终端支持脱机密码处理，则它们支持 VERIFY 命令。

### 7.2.6.5 处理流程

持卡人验证处理分成两部分：卡片的持卡人验证方法列表处理与执行持卡人验证。

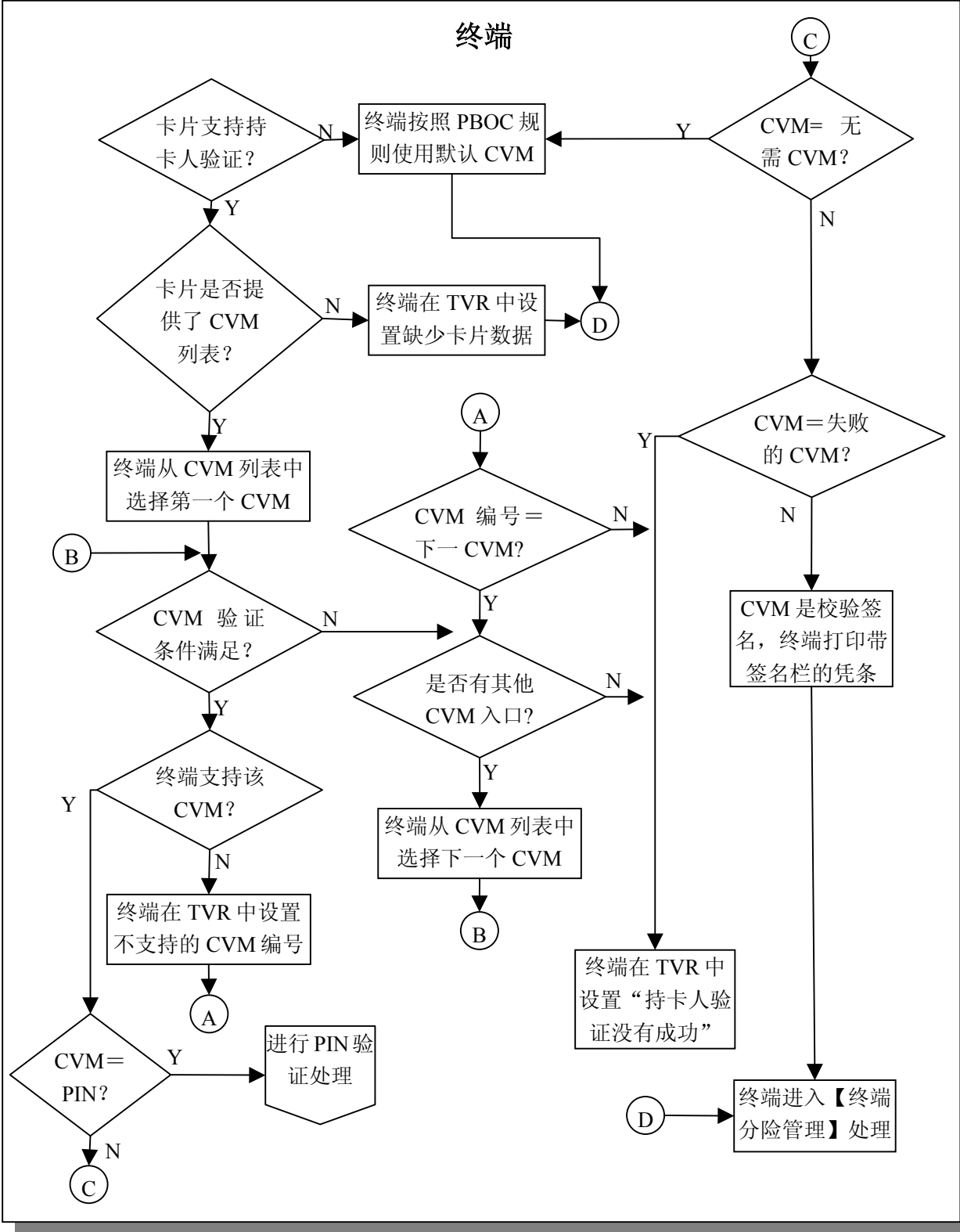
#### 7.2.6.5.1 持卡人验证方法列表（CVM）处理

卡片在持卡人验证方法列表处理中，除了给终端提供持卡人验证方法列表以及其他必需数据外，不起别的作用。

终端执行下列步骤：

1. **决定是否执行持卡人验证**—如果卡片支持持卡人验证（如应用交互特征所说明），且读取应用数据时，卡片提供一个持卡人验证方法列表，那么终端就继续持卡人验证。反之，终端将执行中国集成电路（IC）卡为终端指定的持卡人验证方法。如果没有指定，终端就进行终端风险管理。
2. **处理持卡人验证列表条目**—由持卡人验证方法列表中的第一个条目开始，终端执行以下行为：
  - a. 检查持卡人验证条件是否符合。如果不符合，终端进行下一个持卡人验证方法列表条目。
  - b. 如果持卡人验证方法不被认可或不受支持，终端将不被认可的持卡人验证方法在终端验证结果里设置为“1”。认为持卡人验证不成功。
  - c. 执行指定的持卡人验证方法。
  - d. 如果持卡人验证不成功（例如脱机密码校验失败），终端进行持卡人验证方法条目里持卡人验证方法代码中指定的行为。如果持卡人验证方法代码是“进行下一个持卡人验证方法，”终端就进行下一个持卡人验证方法列表条目。如果是“持卡人验证失败，”终端就在终端验证结果里设置持卡人验证不成功标志“1”并进行终端风险管理。
  - e. 如果持卡人验证成功，终端进行终端风险管理。
3. **如果终端到达了持卡人验证方法列表的末端还没有一个成功的持卡人验证，则持卡人验证处理失败**—终端在终端验证结果里设置持卡人验证不成功标志“1”并进行终端风险管理。

7.2.6.5.2 持卡人验证方法列表（CVM）处理流程图



图表 7-8：持卡人验证方法列表处理流程图

### 7.2.6.5.3 持卡人验证处理

#### 7.2.6.5.3.1 脱机明文 PIN 验证

脱机密码验证处理中，卡片将持卡人输入的交易密码与卡里储存的参考密码对比以做检查。不同于联机密码，脱机密码不包括在联机授权报文中。如果交易联机进行，脱机密码验证结果就包括在联机授权报文中。终端可用 GET DATA 命令向卡片请求密码重试次数计数器，如果卡片不支持传送密码重试次数计数器，终端要求继续输入密码。如果返回的密码重试次数计数器为零（没有剩余密码重试次数），则脱机密码验证失败。如果返回的密码输入次数计数器为一，则终端显示“最后一次尝试”。

如果允许密码重试，终端要求持卡人在密码键盘上输入密码。如果密码键盘和读卡机没有集成为一个不收外界干预的整体设备，密码就被密码键盘保密密钥加密并由读卡机解密。VERIFY 命令将持卡人输入的交易密码从读卡机以明文方式传递给卡。

卡将交易密码与卡里储存的参考密码加以对比。

- 如果它们匹配，卡片将返回一个指示器，显示脱机密码已被验证，持卡人验证完成。
- 如果不相配，卡片密码重输次数计数器递减并返回一个显示剩余密码重输次数的指示器。

如果没有剩余密码重输次数，脱机密码验证失败。

如果还有密码重输次数剩余，终端要求持卡人重新输入密码，重复校验过程。

#### 7.2.6.5.3.2 联机 PIN 验证

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

联机密码处理流程不在本规范中描述。

#### 7.2.6.5.3.3 签名

当选择签名作为持卡人验证方法时，终端打印一张附有给持卡人签名档的收据。

#### 7.2.6.5.3.4 不需要持卡人验证

当持卡人验证方法是“不需要持卡人验证”时，持卡人验证成功。

#### 7.2.6.5.3.5 持卡人验证失败

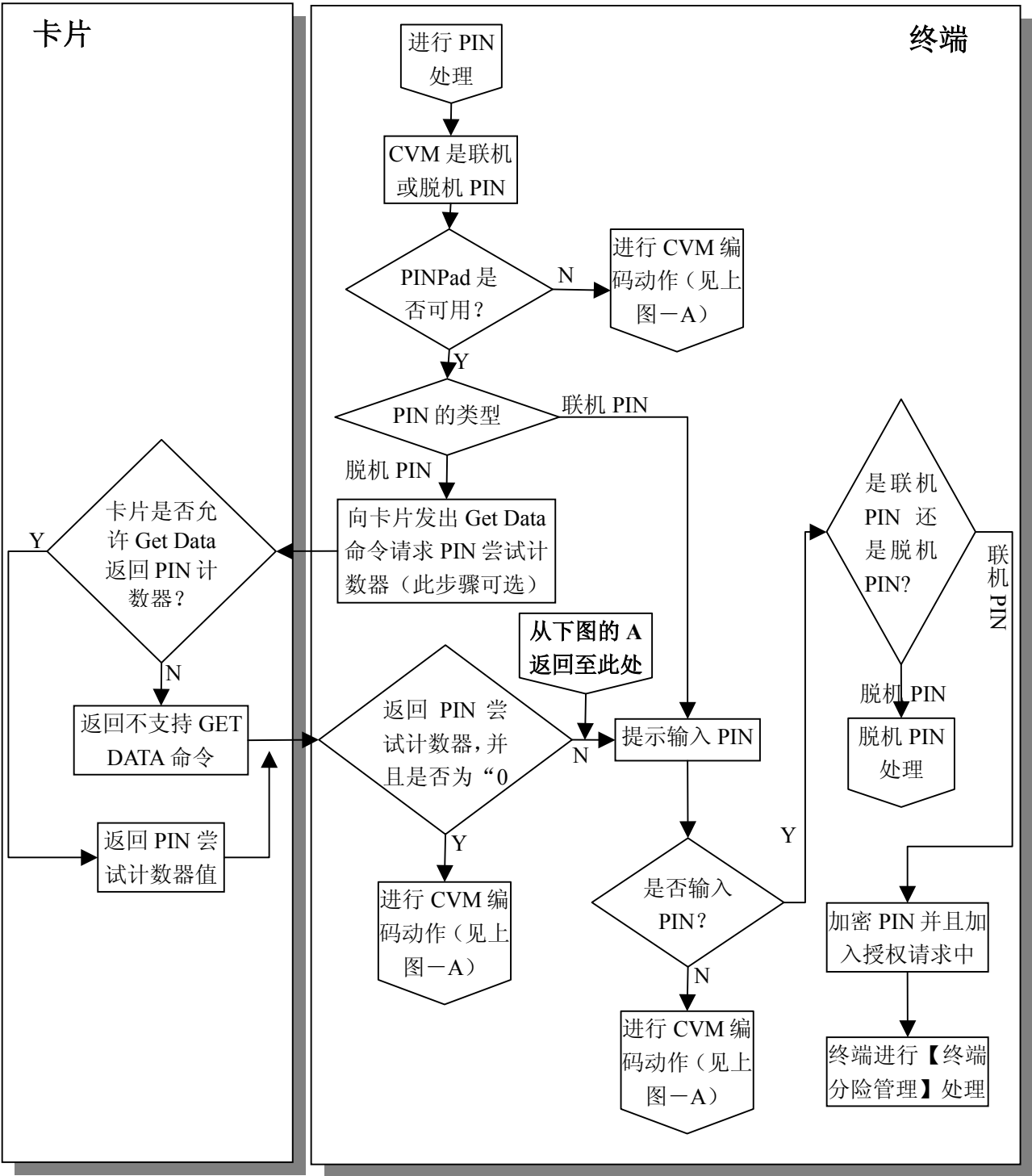
当持卡人验证方法是“持卡人验证失败”时，认为持卡人验证处理失败。

下面两张流程图概述了密码验证处理流程。

#### 7.2.6.5.3.6 持卡人证件验证

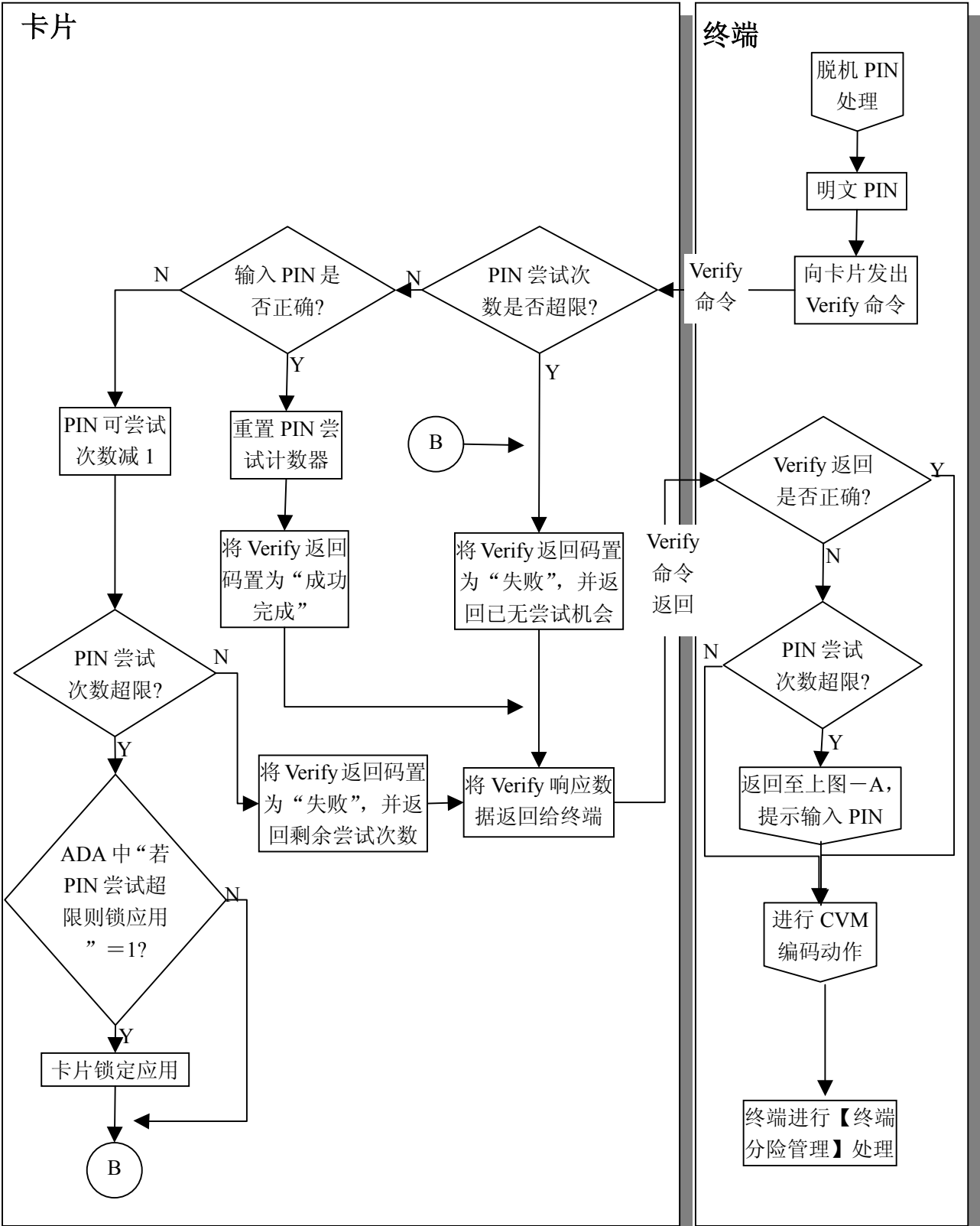
终端提示持卡人出示身份证件，并将卡片中得到的证件类型和证件号码显示给服务员，进行持卡人身份比对验证。

7.2.6.5.3.7 PIN 验证处理流程图（2-1）



图表 7-9: PIN 验证处理流程图（1）

7.2.6.5.3.8 PIN 验证处理流程图（2-2）



图表 7-10: PIN 验证处理流程图（2）

7.2.6.6 前期相关处理

初始化应用处理

从卡片中获取应用交互特征（AIP），指示卡片是否支持持卡人验证。

读取应用数据

终端从卡片中读取持卡人验证方法列表以及其他持卡人验证处理中使用的数据。

7.2.6.7 后续相关处理

终端行为分析

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

卡片行为分析

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

联机处理

授权请求报文中含有包括脱机密码校验结果在内的持卡人验证结果，发卡行的授权决定中应该考虑这些结果。联机授权报文里不包括脱机密码。

完成

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

发卡行到卡脚本命令处理

PIN CHANGE/UNBLOCK 命令可以用于重新设置密码重试次数计数器，使其与密码重试次数上限相等，并改变参考密码。

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

7.2.7 终端风险管理

7.2.7.1 描述

终端风险管理为大额交易提供了发卡行认证，并确保芯片交易能够周期性地联机以防止在脱机环境中也许无法觉察的风险。

虽然发卡行被强制要求应用交互特征（AIP）中将终端风险管理位设置成 1 以触发终端风险管理，但终端应该执行终端风险管理而不必考虑卡片的设置情况。

7.2.7.2 卡片数据

下表列出并描述了终端风险管理中使用的卡片数据元。这些数据元及其用法的详细说明请参阅《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 A，卡片和发卡行数据元表。

表格 7.2.7-1：终端风险管理—卡数据

数据元	说明
应用主帐号（PAN）	终端异常文件检查时使用的有效的持卡人帐号。
应用交易序号（ATC）	自卡片个人化以后处理的交易数量，在终端频度检查中使用。
最后的联机交易序号寄存器	最后一次联机的交易序号值。如果卡片要求终端进行终端频度检查或新卡检查，则这个数据元以及下面所列出的数据元都必须提供。
连续脱机交易下限	如果终端可以联机，该数据元（标签“9F14”）是发卡行定义的在交易必须联机



	之前所允许的最大连续脱机交易笔数，它用于终端频度检查。
连续脱机交易上限	该数据元（标签“9F23”）是发卡行定义的在脱机交易必须被拒绝之前所允许的最大连续脱机交易笔数。它用于终端频度检查。

### 7.2.7.3 终端数据

下表列出并描述了终端风险管理中使用的终端数据元。这些数据元及其用法的详细说明请参阅《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 A，卡片和发卡行数据元表。

表格 7.2.7-2：终端风险管理—终端数据

数据元	说明
授权金额	该数字数据元存储了当前交易金额（不包括调帐交易）。用于最低限额检查。
用于偏置随机选择的 最大目标百分数	用于随机选择交易联机处理。
用来随机选择的 目标百分数	用于随机选择交易联机处理。
终端最低限额	该数据元（标签“9F1B”）表示与应用标识符相关联的终端最低限额。用于最低限额检查和随机选择交易联机处理。
终端校验结果 (TVR)	记录终端脱机处理结果的一系列指示器。它们用来记录终端风险管理检查的结果。
偏置随机选择 阈值	用于随机选择交易联机处理的数值。
交易日志	为防止分开销售，终端可能记录了已批准交易的日志。此日志至少包含了应用主帐号和交易金额，并可选择地包含了应用主帐号顺序号和交易日期。要存储和维护的交易日志数量不在本规范规定范围内。如果有此日志，则它可被用于终端最低限额检查。
交易状态信息 (TSI)	标明终端执行的功能，联机授权和清算报文中不提供此数据元，终端用它来表示已经执行了终端风险管理。

### 7.2.7.4 命令

#### GET DATA

如果先前终端没有读取，则终端用 GET DATA 命令从卡片中读取最后一次联机交易的序号寄存器和应用交易序号（ATC）。

### 7.2.7.5 终端异常文件检查

如果出现终端异常文件，终端就检查卡上的主帐号（PAN）是否列在终端异常文件上。

如果卡号列在终端异常文件中，终端在终端验证结果（TVR）中设置“卡号出现在终端异常文件中”的位为“1”。

### 7.2.7.6 商户强制交易联机

在可以联机的终端，商户可以将终端设置为交易应该联机处理。

如果商户强制交易联机，终端将终端验证结果（TVR）中“商户强制交易联机”的位设置成“1”。

### 7.2.7.7 最低限额检查

执行最低限额检查，可以使超过终端最低限额的交易执行联机授权。

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

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

#### 7.2.7.8 随机交易选择

可以支持脱机和联机交易的终端会随机选择交易进行联机处理。

如果随机选择了一个交易，终端会标注在终端验证结果中。此处理的例子请参阅《中国集成电路（IC）卡借记/贷记应用终端规范》终端风险管理一章。

#### 7.2.7.9 终端频度检查

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

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

终端发送 GET DATA 命令向卡申请最后的联机交易序号寄存器与交易计数器（ATC）。卡在命令响应中返回这些数据元。

终端将 ATC 与最后联机交易的序号寄存器对比：

- 如果 ATC 减去最后联机交易的序号寄存器大于连续脱机下限值，终端将终端验证结果中“超过连续脱机下限”的位设置成“1”。
- 如果 ATC 减去最后联机交易的序号寄存器大于连续脱机上限值，终端将终端验证结果中“超过连续脱机上限”的位设置成“1”。

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

#### 7.2.7.10 新卡检查

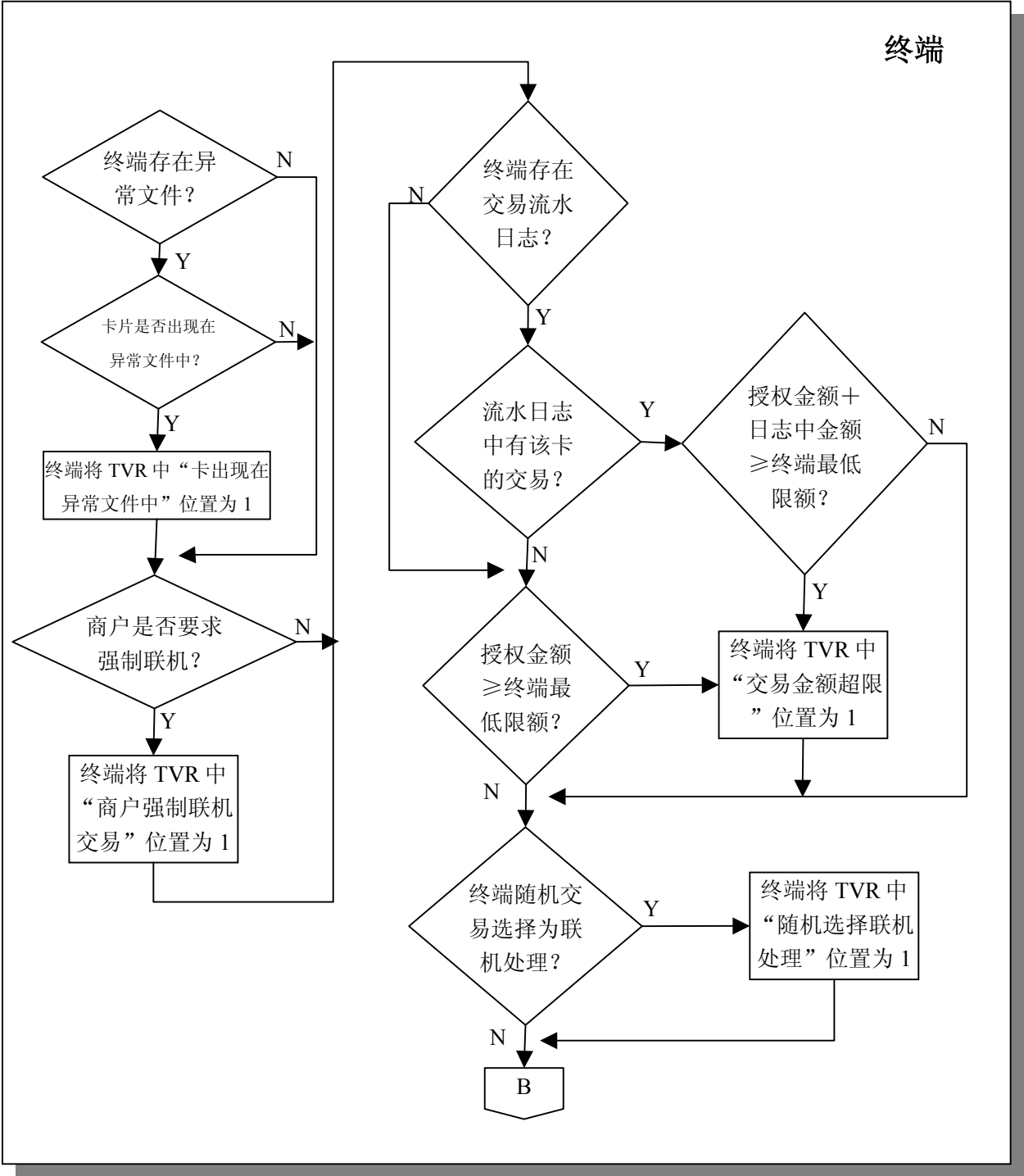
在终端所做的新卡检查中，如果存在连续脱机上限值和连续脱机下限值，终端就检查最后联机交易序号寄存器（如果卡提供的话）。根据发卡行认证结果和卡片参数，交易被联机批准后，该寄存器被重新复位。

终端发送 GET DATA 命令向卡片申请最后联机交易的序号（如果该数据元并未出现在终端里）。卡片用最后联机交易的序号寄存器作为对 GET DATA 命令的响应。

终端检查最后联机交易序号，如果序号为 0，终端将 TVR 中的“新卡”位置设为“1”。

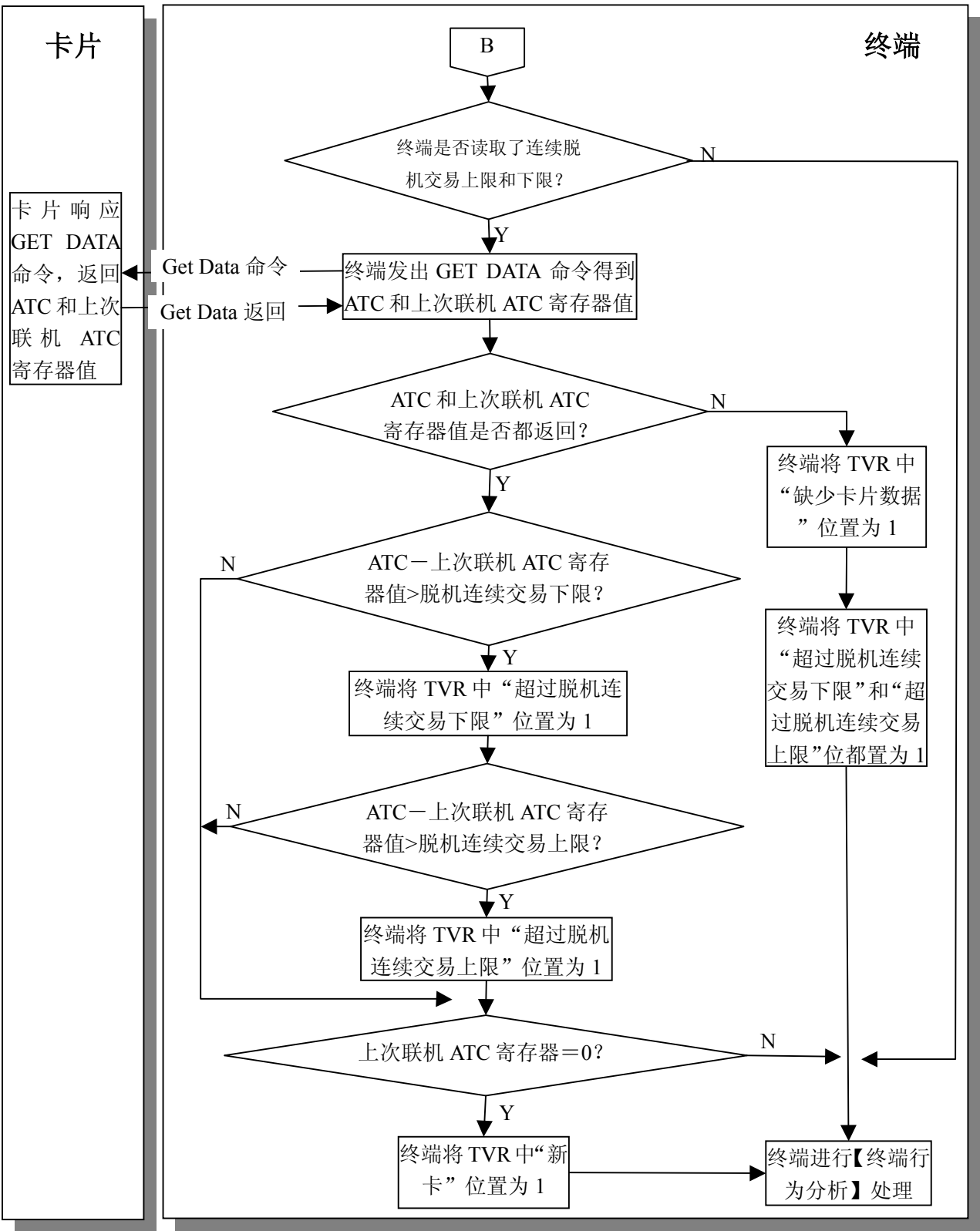
**注意：**卡片行为分析中，卡片也可以执行相似的新卡检查。

7.2.7.11 终端风险管理处理流程图（1）



图表 7-11：终端风险管理处理流程图(1)

7.2.7.12 终端风险管理处理流程图（2）



图表 7-12：终端风险管理处理流程图(2)

7.2.7.13 前期相关处理

读取应用数据

下列数据从卡片中读取：

- 主帐号用于检查终端异常文件。
- 如果卡上存在连续脱机交易上限值和下限值，它们用于终端频度检查。

7.2.7.14 后续相关处理

终端行为分析

终端根据卡片和终端的设置来决定采取怎样的行动，如果：

- 卡片在终端异常文件上
- 商户强制交易联机
- 超过了最低限额
- 交易被随机选择进行联机处理
- 频度检查金额或笔数超限
- 新卡

7.2.8 终端行为分析

7.2.8.1 描述

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

终端行为分析牵涉到两个步骤：

1. **检查脱机处理结果**—终端检查由终端记录在终端校验结果里的脱机处理结果，决定交易要请求联机授权、脱机批准，还是脱机拒绝。此过程考虑了卡片中发卡行定义的规则，即发卡行行为代码（IACs）以及终端的 PBOC 定义的规则，即终端行为代码（TACs）。
2. **请求密文处理**—终端要求一个来自卡片的密文。

终端行为分析中，脱机批准或申请联机处理的决定并不是最终的。作为卡行为分析的结果（参考 7.2.9），卡片可以不考虑终端的决定，但脱机拒绝的决定是不可以忽略的。

7.2.8.2 卡片数据

下表中所描述是先前从卡片收到并在终端行为分析中使用的卡片数据元。这些元及其用法的详细说明请参阅《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 A，卡片和发卡行数据元表。

表格 7.2.8-1：检查脱机处理结果—卡片数据

数据元	说明
发卡行行为代码（IACs）	发卡行行为代码是三种数据元，即发卡行行为代码-拒绝，发卡行行为代码-联机，发卡行行为代码-缺省。每个发卡行行为代码由一系列与终端校验结果（TVR）中的比特位相对应的比特位组成。 <ul style="list-style-type: none"><li>● 发卡行行为代码-拒绝位设置为“1”反映了交易被脱机拒绝的终端验证结果条件</li><li>● 发卡行行为代码-联机位设置为“1”代表需要联机授权条件</li><li>● 发卡行行为代码-缺省位设置为“1”是当联机处理不可行时脱机拒绝所需的条件</li></ul> 类似的终端行为代码（TACs）在终端里定义。

表格 7.2.8-2：要求密文处理—卡片数据

数据元	说明
卡片风险管理数据对象列表 1	卡片风险管理数据对象列表 1 包含了终端数据对象的标签和长度，卡片需要用它们来生

(CDOL1)	成第一个应用密文，以及进行其他处理。
---------	--------------------

### 7.2.8.3 终端数据

这些数据元及其用法的详细说明请参阅《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 A，卡片和发卡行数据元表。

表格 7.2.8-3：检查脱机处理结果—终端数据

数据元	说明
终端行为代码（TACs）	终端行为代码是三种数据元，即终端行为代码-拒绝，终端行为代码-联机，终端行为代码-缺省。和发卡行行为代码相似，每个终端行为代码由一系列与终端校验结果（TVR）中的比特位相对应的比特位组成。 <ul style="list-style-type: none"> <li>终端行为代码-拒绝比特位设置为“1”反映了交易被脱机拒绝的终端验证结果条件</li> <li>终端行为代码-拒绝比特位设置为“1”代表了联机授权条件</li> <li>终端行为代码-缺省比特位设置为“1”是当联机处理不可行时脱机拒绝所需的条件</li> </ul>
终端验证结果（TVR）	终端验证结果是在交易处理期间被用来代表脱机处理结果而设置的一系列比特位。

表格 7.2.8-4：要求密文处理—终端数据

数据元	说明
终端数据元	在卡片风险管理数据对象列表 1 中得以详细说明的终端数据元包括在 GENERATE APPLICATION CRYPTOGRAM（AC）命令中。

### 7.2.8.4 命令

#### GENERATE APPLICATION CRYPTOGRAM（AC）

终端发送 GENERATE AC 命令向卡申请一个应用密文。如果执行复合动态数据验证/应用密文生成，终端也会出现此命令。

该命令指明了下列应用密文中的一种：

- 交易证书（TC）——用于批准
- 应用认证密文（AAC）——用于拒绝
- 授权请求密文（ARQC）——进行联机

此命令也包括卡在卡风险管理数据对象列表 1 里要求的终端数据对象。

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

### 7.2.8.5 处理流程

终端行为分析处理有两个步骤：

- 脱机处理结果的检查
- 请求密文处理

#### 7.2.8.5.1 检查脱机处理结果

终端检查脱机处理的结果以决定是否交易需要联机、被脱机批准，或被脱机拒绝。这个过程中使用了卡片中发卡行定义的规则（发卡行行为代码）以及终端里中国集成电路（IC）卡定义的规则（终端行为代码）。《中国集成电路（IC）卡借记/贷记应用终端规范》的终端行为分析中有一个例子：发卡行行为代码和终端行为代码（IAC）如何与终端校验结果（TVR）共同使用以决定交易处理过程。

#### 7.2.8.5.2 请求密文处理

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

- 脱机批准——TC（交易证书）

- 进行联机授权——ARQC（授权请求码）
- 脱机拒绝——AAC（应用认证密码）

如果执行复合动态数据验证/应用密文生成，终端也会出现此命令。

#### 7.2.8.6 前期相关处理



## 读取应用数据

## 脱机数据认证，处理限制，持卡人验证及终端风险管理

44



发卡行行为代码和终端行为代码共同使用来决定交易处理。

7.2.8.7 后续相关处理

卡片行为分析

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

7.2.9 卡片行为分析

7.2.9.1 描述

卡行为分析允许发卡行执行频度检查以及其他的卡片内部的风险管理。本节描述的 PBOC 所专有的卡片风险管理特性包括如下检查：

- 上次交易的行为
- 新卡
- 交易频度计数器

7.2.9.2 卡片数据

下表列出并描述了卡行为分析中用到的卡数据元。关于这些数据元及其用途的详细描述参见《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 A，卡片和发卡行数据元表。

表格 7.2.9-1：卡片行为分析—卡片数据

数据元	说明
应用密文	卡响应 GENERATE APPLICATION CRYPTOGRAM（AC）命令而返回的密文。 <ul style="list-style-type: none"><li>• 返回请求拒绝的应用认证密文称为 AAC</li><li>• 返回请求批准的交易证书称为 TC</li><li>• 联机处理申请的授权请求密文称为 ARQC</li></ul>
卡风险管理数据对象列表中要求的数据（CDOL1）	卡风险管理数据对象列表 1 中要求的数据。请参阅《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 E。

7.2.9.3 终端数据

卡片行为分析中没有使用终端数据。

7.2.9.4 命令

GENERATE APPLICATION CRYPTOGRAM（AC）

终端用在终端行为分析完成后向卡片发出第一次 GENERATE APPLICATION CRYPTOGRAM（AC）命令来要求卡片返回一个标明卡片授权响应结果的密文。在此命令中终端也可以标识是否要执行复合动态数据认证/应用密文（CDA）生成密文。

7.2.9.5 处理流程

终端行为分析之后，终端向卡发送 GENERATE AC 命令，向卡片提供在卡片风险管理数据对象列表（CDOL1）中要求的数据并请求一个应用密文。在7.2.8阐述了终端行为分析处理过程。

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

7.2.9.5.1 卡片风险管理

如果卡片支持并且要求的数据可用，则卡片执行下列卡片风险管理行为：

- 上次交易行为：
  - ✓ 联机授权未完成
  - ✓ 上次联机交易时，发卡行认证失败
  - ✓ 上次交易静态数据认证失败
  - ✓ 上次交易动态数据认证失败
  - ✓ 上次交易发卡行脚本命令执行情况
  - ✓ 上次交易密码重试次数超限
- 新卡检查
- 频度检查查看以下项目的脱机处理次数是否超限：
  - ✓ 全部连续脱机交易笔数
  - ✓ 根据货币种类统计的全部连续脱机国际交易笔数
  - ✓ 根据国家统计的全部连续脱机国际交易笔数
  - ✓ 指定货币的全部脱机交易累计金额
  - ✓ 指定货币和第二货币的全部脱机交易金额

7.2.9.5.2 卡片响应决定

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

- 卡片可以不考虑终端已批准脱机的决定，而申请联机授权或拒绝脱机
- 卡片可以不考虑终端申请联机授权的决定，而拒绝交易

表格 7.2.9-2：卡片行为分析 — 卡片对 GENERATE AC 命令的响应

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

7.2.9.5.2.1 标准 GENERATE AC 的响应

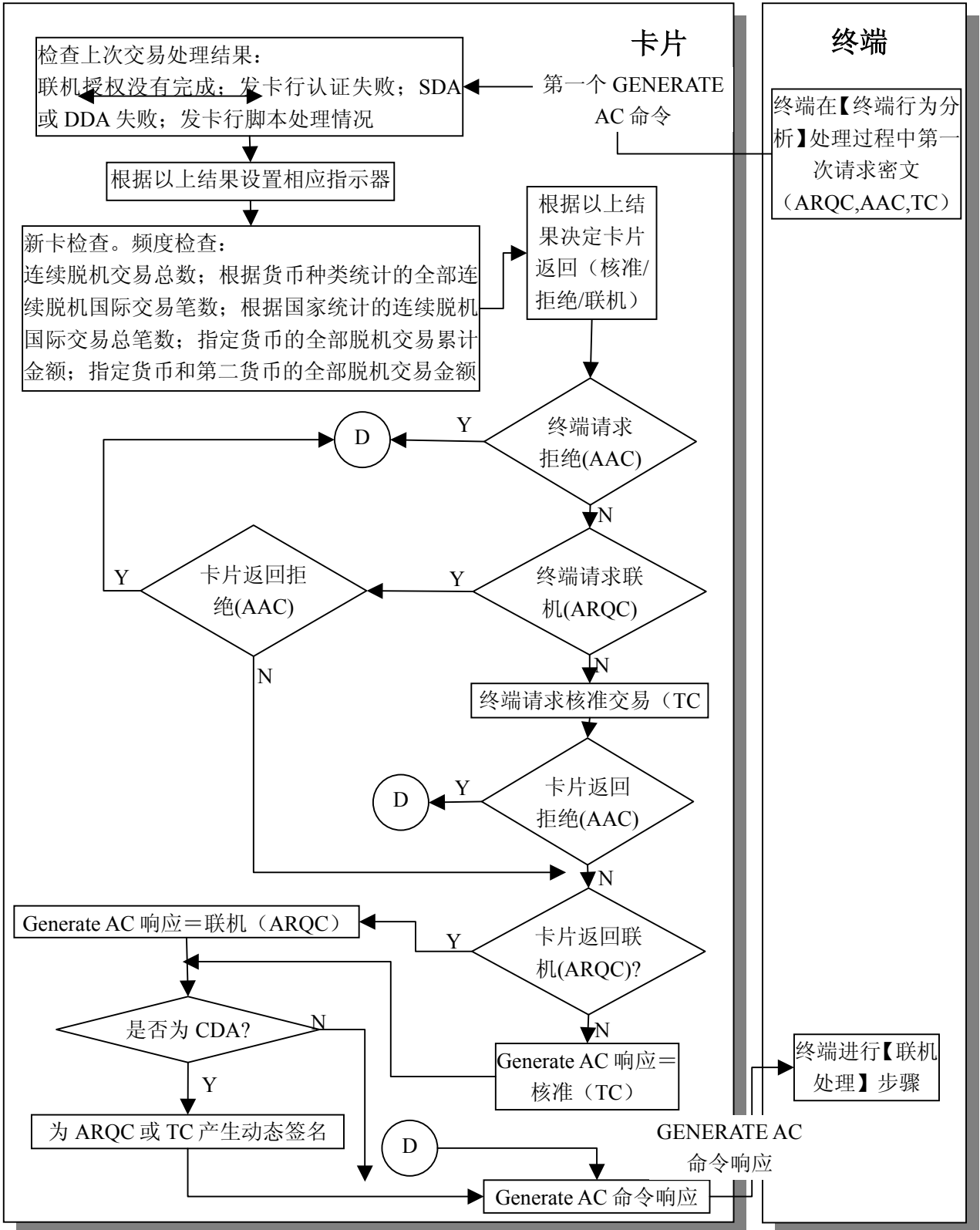
卡片利用终端和卡片提供的数据生成一个基于对称算法的密文。《中国集成电路（IC）卡借记/贷记应用卡片规范》附录 D 中详述了所要求的数据。《中国集成电路（IC）卡借记/贷记安全规范》中详述了密文生成过程中所需的对称密钥和算法。

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

7.2.9.5.2.2 复合动态数据认证/应用密文(CDA)生成的 GENERATE AC 响应

如果终端在 GENERATE AC 命令中表明将执行 CDA，并且卡片在 GENERATE AC 响应中返回的密文类型是核准（TC）或请求联机（ARQC），则卡片用 IC 卡私钥将应用密文、密文信息数据以及其他的数据加密。在 GENERATE AC 响应中，卡片将这签名数据返回给终端。

7.2.9.6 流程图



图表 7-14：卡片行为分析处理流程图

### 7.2.9.7 前期相关处理

#### 读取应用数据

终端从卡片读取卡片风险管理数据对象列表 1 (CDOL1)。

### 7.2.9.8 后继相关处理

#### 完成

如果要求联机处理，但终端无法将交易联机发送，则卡片和终端执行其他的处理来决定是核准脱机或拒绝交易。

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

卡也执行下列的卡风险管理检查，以决定最终的交易处理结果：

- 对于全部连续脱机交易（上限）的频度检查
- 新卡
- 没有执行脱机密码验证

### 7.2.10 联机处理

#### 7.2.10.1 描述

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

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

#### 7.2.10.2 卡片数据

终端所用到的卡片数据如下表所述：

表格 7.2.10-1：联机处理—终端使用的卡片数据

数据元	描述
Generate AC 命令返回数据	返回数据中包括： <ul style="list-style-type: none"><li>● 密文类型（如果交易需要联机授权，则是授权请求密文 ARQC）</li><li>● 应用密文（APPLICATION CRYPTOGRAM）</li><li>● 应用交易计数器（ATC）</li><li>● 发卡行应用数据</li></ul>
应用交互特征(AIP)	终端在应用初始化处理时从卡片得到 AIP，其中一位指明卡片是否支持发卡行认证。

在发卡行授权过程中卡片内部使用的数据如下：

表格 7.2.10-2：联机处理—卡片内部使用数据

数据元	描述
授权请求密文(ARQC)	由卡片在此交易的较早步骤产生。ARQC 和授权响应码将在授权响应密文（ARPC）确认处理中作为输入数据。
应用密文过程密钥（UDK）	是 ARPC 确认处理中使用的 DES 密钥，与产生 ARQC 使用的是同一密钥。
卡片验证结果（CVR）	如果发卡行认证失败，相应位将置为 1
发卡行认证失败指示器	如果发卡行认证失败该位将置为 1

### 7.2.10.3 终端数据

根据发卡行认证状态，终端需改变的数据元如下：

表格 7.2.10-3：联机处理—终端需改变数据

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

### 7.2.10.4 联机响应数据

下表是发卡行可能返回给收单行的响应数据，如果存在的话，收单行必须将数据传送给终端：

表格 7.2.10-4：联机处理—发卡行可能返回的响应数据

数据元	描述
发卡行认证数据	包括以下子项： <ul style="list-style-type: none"><li>● 授权响应密文（ARPC）：由发卡行主机系统产生的密文；</li><li>● 授权响应码：在产生 ARPC 时用到的响应码。</li></ul>
发卡行脚本	由发卡行发送给卡片的一些命令数据，用于更新卡片数据。

### 7.2.10.5 命令

联机处理过程中相关的命令如下：

#### 7.2.10.5.1 外部认证（External Authenticate）命令

如果执行了发卡行认证，终端应使用从发卡行请求到的发卡行认证数据通过外部认证（External Authenticate）命令验证授权响应密文（ARPC）的正确性。通过命令的返回可以知道认证是否通过。

### 7.2.10.6 处理流程

标准的联机处理包括联机请求、联机响应，如果需要，可以执行发卡行认证。如果已经执行 CDA，处理过程中还要包括动态数据的验证。

#### 联机请求

联机请求处理根据是否已经执行 CDA 而有所不同。

#### 执行 CDA

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

- 终端用恢复出的 IC 卡公钥解密动态密文，得到应用密文。
- 如果 HASH 值与终端 TVR 中的值不匹配，则 CDA 失败，并转至完成处理。
- 如果 HASH 值匹配，则进行标准联机处理。

#### 标准联机请求处理

如果卡片在 Generate AC 向终端返回 ARQC,同时终端具备联机能力，则终端发出联机授权报文。如果卡片没有返回 ARQC 或终端不具备联机能力，则转至完成处理步骤。

## 联机响应

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

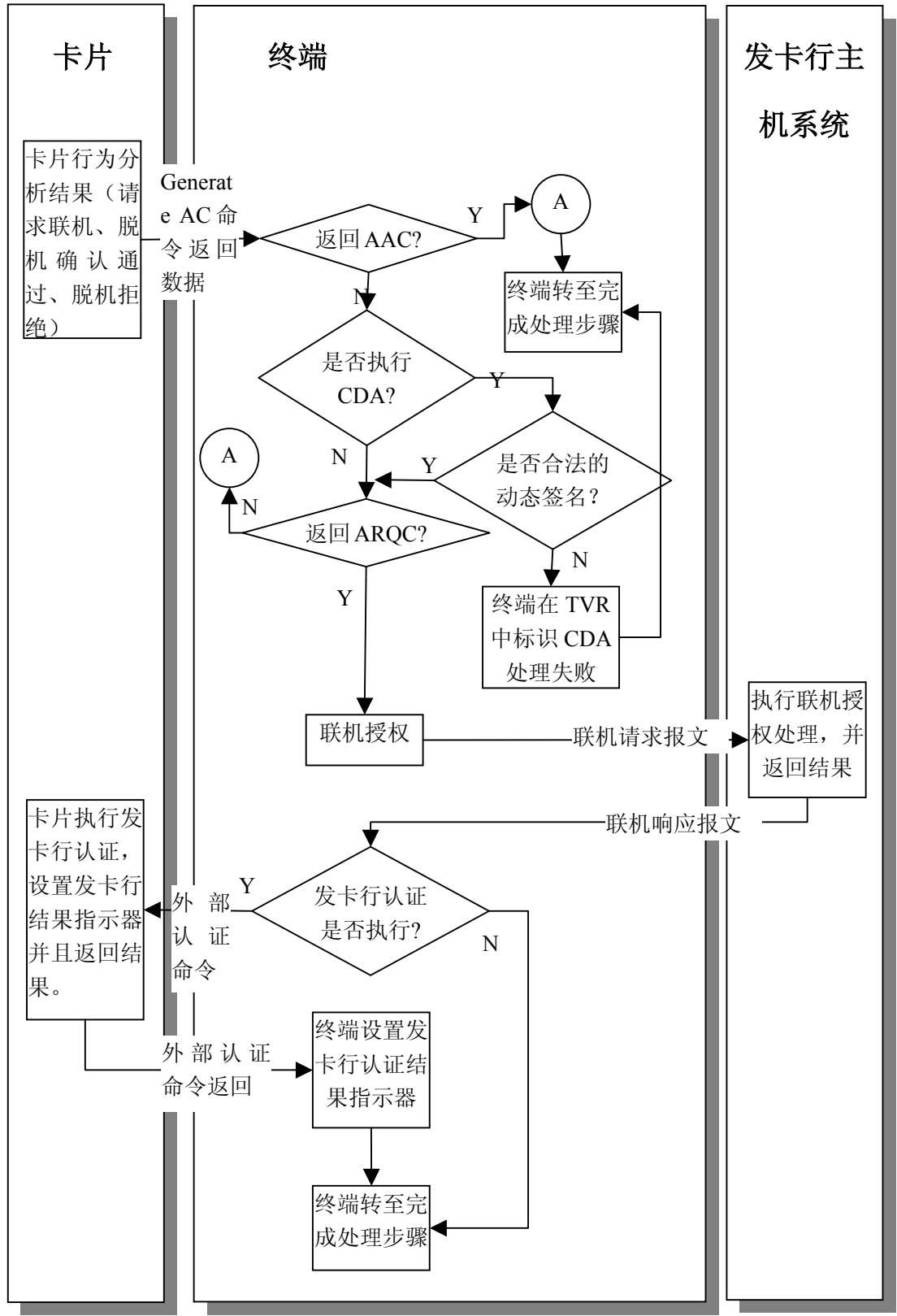
## 发卡行认证

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

卡片和终端都要记录发卡行认证结果：

- 卡片在卡片验证结(CVR)中设置发卡行认证结果以及发卡行认证失败标识，并且在外部认证命令（EXTERNAL AUTHENTICATE）响应报文中将结果返回给终端。
- 终端在进行完成处理之前，将在终端验证结果（TVR）中设置发卡行认证结果和交易状态信息（TSI）。

7.2.10.7 流程图



图表 7-15: 联机处理流程图

#### 7.2.10.8 前期相关操作

##### 卡片行为分析

如果经过卡片分析后需要联机授权，则卡片返回的密文类型为 ARQC。

#### 7.2.10.9 后续相关操作

##### 完成处理

在完成处理过程中，卡片参考发卡行认证结果和卡片参数交易如何处理以及是否重置相关指示器和计数器。

##### 发卡行脚本处理

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

#### 7.2.11 发卡行脚本处理

##### 7.2.11.1 描述

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

支持的脚本命令如下：

- 更改卡片参数
- 锁定/解锁应用
- 锁卡
- 重置 PIN 计数器
- 修改脱机 PIN

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

##### 7.2.11.2 脚本相关密钥

###### 7.2.11.2.1 报文认证码密钥（MAC KEY）

MAC Key 是用来产生和验证命令脚本 MAC 的。MAC 是包含在命令脚本中的密文，用于确认数据没有被篡改过（完整性），同时可以确认命令发出的发卡行是否是合法（发卡行认证）。MAC 处理过程中用到了三个密钥：

- MAC 主密钥（MAC MDK）：

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

- 卡片 MAC 子密钥（MAC UDK）：

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

- MAC 过程密钥：

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

###### 7.2.11.2.2 数据加密密钥

数据加密密钥用来加密脚本中的敏感数据，如脱机 PIN 等。数据加密用到三个密钥：

- 数据加密主密钥（ENC MDK）：

数据加密主密钥是发卡行唯一的双倍长对称密钥，用于产生卡片唯一数据加密密钥以及交易的



数据加密过程密钥。

- 卡片数据加密子密钥（ENC UDK）：

ENC UDK 是卡片个人化时由数据加密主密钥分散得到后写入卡片的双倍长对称密钥。用来产生数据加密过程密钥。

- 数据加密过程密钥：

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

### 7.2.11.3 卡片数据

脚本处理过程中卡片使用到的计数器和指示器如下表所示：

表格 7.2.11-1：发卡行脚本处理一卡片使用的计数器和指示器

数据元	描述
应用交易计数器 (ATC)	自卡个人化以后处理的交易计数器，在终端频度检查中用到。
卡片验证结果 (CVR)	根据本次和上次交易脱机处理结果进行设置的验证结果指示符。
发卡行脚本命令计数器	记录第二次生成应用密文后卡片收到的有安全报文的指令的个数。在下次交易中的结束处理步骤中可能被复位。
发卡行脚本失败指示器	如果脚本指令执行失败，指示位置“1”，失败的情况有： <ul style="list-style-type: none"><li>● 安全报文错误</li><li>● 安全报文通过但是指令执行失败</li><li>● 需要安全报文但是不存在</li></ul> 在下次交易中的结束处理步骤中可能被复位。

### 7.2.11.4 终端数据

发卡行脚本处理过程中终端用到的数据元如下表所示：

表格 7.2.11-2：发卡行脚本处理一终端使用的数据元

数据元	描述
发卡行脚本结果	记录卡片对发卡行脚本指令处理的结果，此结果要包括在清算报文和下次联机授权中。
终端验证结果 (TVR)	TVR 中包括和脚本有关的两个指示位 <ul style="list-style-type: none"><li>● 最后一个生成应用密文之前，发卡行脚本失败</li><li>● 最后一个生成应用密文之后，发卡行脚本失败</li></ul> PBOC 只支持在最后一个生成应用密文之后，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。

### 7.2.11.5 联机响应数据

表格 7.2.11-3：发卡行脚本处理一联机响应数据

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

### 7.2.11.6 命令

#### 7.2.11.6.1 应用锁定 (APPLICATION BLOCK)

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

#### 7.2.11.6.2 应用解锁 (APPLICATION UNBLOCK)

该命令将已被锁定的应用解锁。对于发卡行，应用解锁最好在专用设备上进行。

#### 7.2.11.6.3 锁卡 (CARD BLOCK)

卡片锁定将使卡片上所有的应用永久锁定。

#### 7.2.11.6.4 修改/解锁 PIN (PIN CHANGE/UNBOLCK)

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

#### 7.2.11.6.5 存数据 (PUT DATA)

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

#### 7.2.11.6.6 更新记录 (UPDATE RECORD)

修改记录命令用来修改文件中一条记录的内容。

### 7.2.11.7 处理流程

发卡行脚本处理包括发卡行脚本、命令执行、安全报文三方面。

#### 7.2.11.7.1 发卡行脚本

发卡行通过返回报文将发卡行脚本发送给收单方。

发卡行返回报文中如果包括标志“72”，标明在最终的 Generate AC 后需要执行发卡行脚本

#### 7.2.11.7.2 命令执行

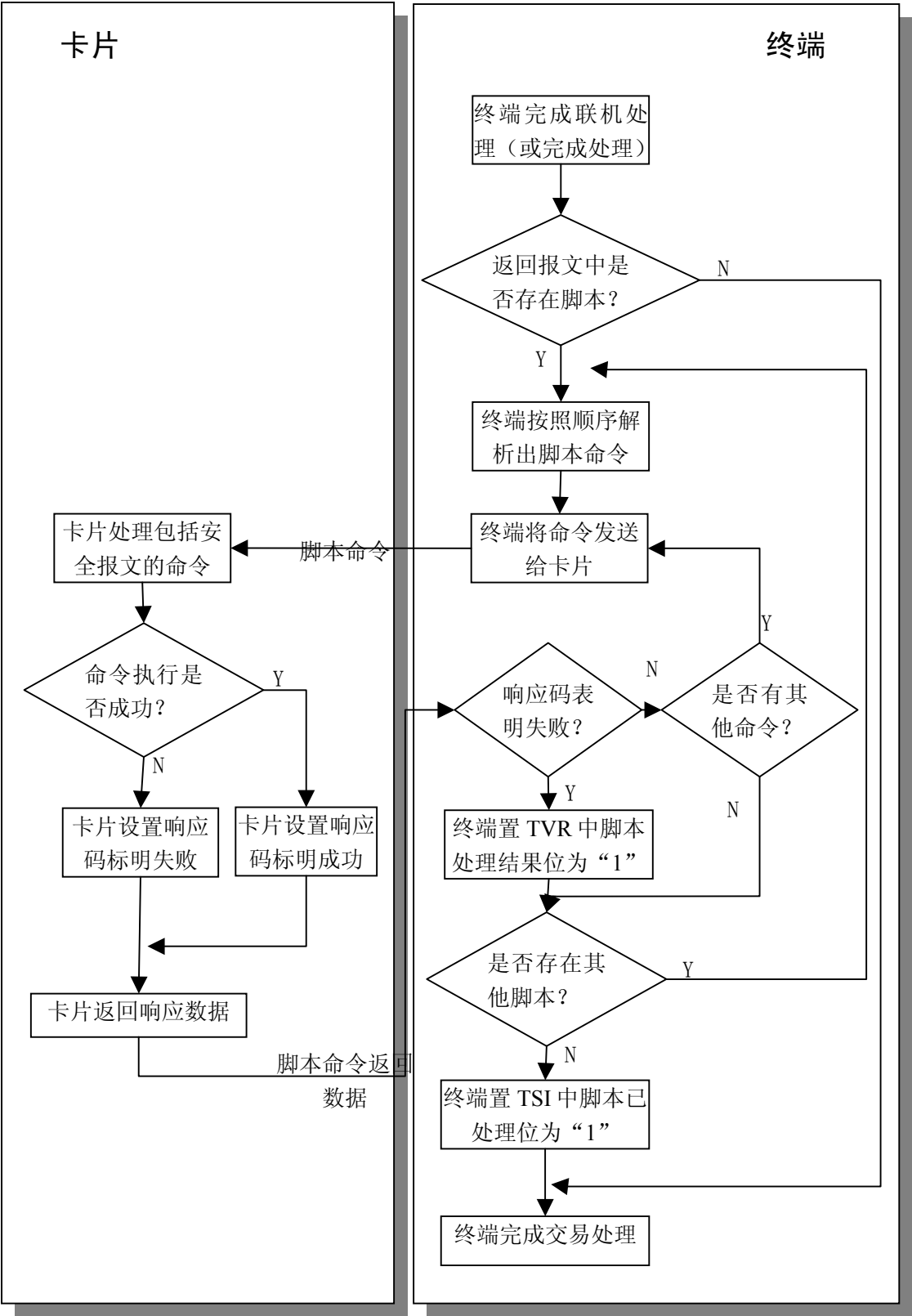
被推荐的发卡行脚本命令用来处理本章先前说明的那些功能。只有命令支持安全报文，而且安全报文得以成功执行的情况下，卡片才执行被请求的命令来更新包含在卡里的数据。

在处理发卡行脚本命令之前，发卡行需要先成功地执行一些发卡行认证方式。因为安全报文是一种发卡行认证方式，所以通过为命令成功地执行安全报文，也可以满足此要求。卡片发卡行承担着发卡行脚本命令组织。如果一个不同于发卡行的实体发起命令，也会发起同样的请求。

#### 7.2.11.7.3 安全报文

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

7.2.11.8 流程图



图表 7-16：发卡行脚本处理流程图

7.2.11.9 前期相关操作

联机处理

联机处理响应报文中可能包括需要在发卡行脚本处理过程中处理的发卡行脚本。

7.2.11.10 后续相关操作

卡片行为分析（下一交易）

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

完成处理（下一交易）

当下列任何一种情况发生时，卡片将重置发卡行脚本失败指示器和发卡行脚本计数器为“0”：

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

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

7.2.12 交易结束

7.2.12.1 描述

终端和卡片执行完成来结束交易处理，主要包括以下动作：

- 如果要求联机处理，但终端并不支持联机处理或联机授权无法完成，则终端和卡片通过其他的分析决定交易是否可以脱机完成或拒绝。
- 如果终端执行 CDA 失败，则终端按照以下方式处理：
  - ✓ 如果卡片请求 ARQC，则终端在第二次产生应用密文（Second Generate AC）时请求 AAC（拒绝密文）。
  - ✓ 如果卡片请求 TC 并且 CDA 执行失败，终端拒绝交易并返回响应码。
- 发卡行的联机确认结果有可能会因为发卡行认证结果和卡片的一些选项而变成拒绝交易。
- 交易处理过程中标识符和计数器会反应发生情况。
- 联机授权后，标识符和计数器可能会根据发卡行认证结果和卡片选项重置。

终端可以执行其他一些附加的功能以完成整个交易。例如打印凭条、记录交易数据等与本规范终端部分不冲突的功能。

7.2.12.2 卡片数据

完成处理时卡片内部使用到的部分数据如下表所示，其他数据元参见《中国金融集成电路（IC）卡借记/贷记应用卡片规范》：

表格 7.2.12-1：交易结束—卡片使用数据元

数据元	描述
应用默认动作 (ADA)	发卡行定义的指示位，指定在一些特殊条件下的卡片行为。
CDOL2	列出在第二个生成应用密文指令中，卡片要求终端传送的数据对象（标签和长度）。下列在 CDOL2 中的数据用于卡片风险管理检查： <ul style="list-style-type: none"><li>● 交易货币代码</li><li>● 终端国家代码</li><li>● 授权金额</li></ul>

	<ul style="list-style-type: none"> <li>● 授权响应码</li> </ul> 终端验证结果（TVR）
--	---

卡片对产生应用密文（Generate AC）命令响应数据如下表：

表格 7.2.12-2：交易结束—Generate AC 命令卡片响应数据

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

### 7.2.12.3 终端数据

在完成处理过程中终端使用到的数据元如下表：

表格 7.2.12-3：交易结束—终端使用数据

数据元	描述
认证响应码	表明交易处理结果，提交给卡片。
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

### 7.2.12.4 命令

#### GENERATE Application Cryptogram (AC)

终端发出第二次 Generate Application Cryptogram(AC)命令向卡片请求最终的应用密文，此处的 Generate AC 命令也可标识成需要执行复合动态数据认证/生成应用密文（CDA）执行。

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

指令参数 P1 指明终端请求的加密类型，EMV2000 4.0 的第三册资料的表 I—12 对此进行了详细描述。

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

### 7.2.12.5 处理流程

根据先前的交易处理中所发生的情况，完成处理期间终端可能处理不同的情况：

卡片行为分析结束后，卡片可能已经：

- 请求脱机确认（TC）或拒绝交易（AAC）；
- 请求联机授（ARQC）；

在联机处理时，联机授权可能已经：

- 成功完成；
- 由于终端或通讯原因未完成；

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

终端必须根据第一个 Generate AC 命令响应返回的 CID 以及 TVR 中显示的复合动态数据认证（CDA）结果决定交易最终结果：

表格 7.2.12-4: 交易结束—终端处理结果（脱机）

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

当卡片行为分析时第一个 Generate AC 命令返回 ARQC(要求联机)时:

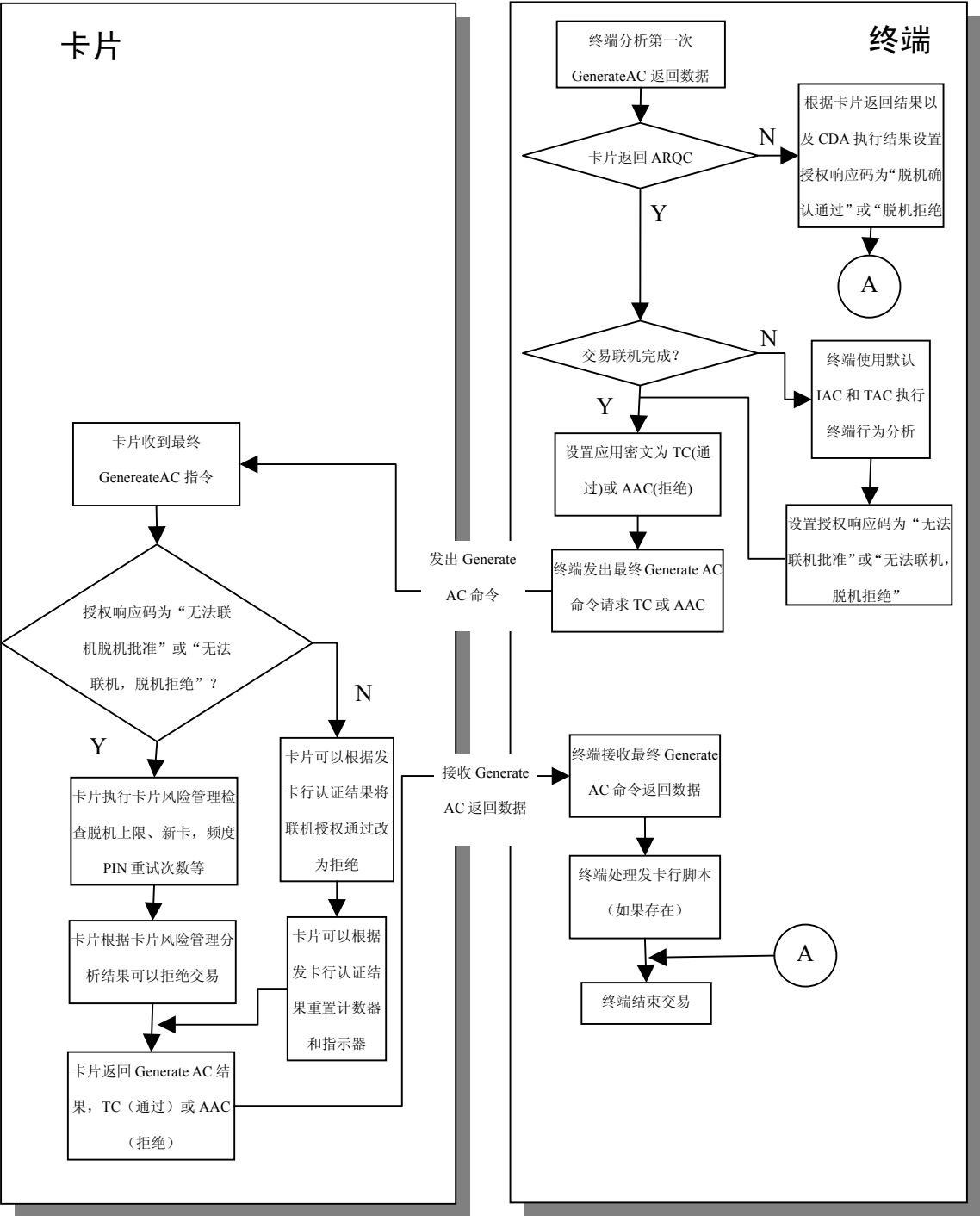
- 1、由于终端不支持或其他原因造成联机授权没有完成，终端向卡片发出第二个 Generate AC 命令请求产生 AAC 或 TC。
- 2、当联机授权完成，根据联机授权结果，终端向卡片发出第二个 Generate AC 命令请求 TC（确认通过）或 AAC（拒绝）。终端根据以下情况处理交易：

表格 7.2.12-5: 交易结束—终端处理结果（联机）

联机授权结果		终端向卡片请求数据	卡片返回	最终交易结果
未完成		AAC	AAC	拒绝
		TC	TC/AAC	核准/拒绝
完成	通过	TC	TC 或 AAC	除以下两种情况卡片返回 AAC(拒绝)，其他情况卡片返回 TC（核准）： 1. 发卡行认证失败，同时 ADA 中标识此种情况拒绝交易； 2. 发卡行认证为强制项，但未执行，同时 ADA 中标识此种情况拒绝交易。 注：如果拒绝交易，必须向发卡行发冲正交易
	拒绝	AAC	AAC	拒绝

当联机授权成功，但是终端向卡片发出第二个 Generate AC 命令执行失败，终端必须向发卡行发出冲正交易。

7.2.12.6 流程图



图表 7-17：交易结束处理流程图

7.2.12.7 前期相关操作

联机处理

如果卡片收到终端发出的外部认证（EXTERNAL AUTHENTICATE）命令，则卡片开始进行发卡行认证处理，同时设置指示器为发卡行认证已执行并标识成功或失败。这些指示器将在完成处理期间

被卡片用于卡片响应，并且决定哪些卡片计数器和指示器将被重置。

7.2.13 卡片交易明细记录

7.2.13.1 描述

在卡片个人化阶段，发卡行在建立交易记录文件的同时，还必须在 PDOL 中定义交易记录所需数据对象的列表（TL：9F6528）。

在应用选择阶段，卡片对 SELECT 命令的相应信息中包含了 PDOL 数据元。如果 PDOL 中包含“9F6528”内容（TL），则在下一条 GET PROCESSING OPTIONS 指令中，终端要把交易明细数据元的内容送给卡片，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，卡片将此内容加上卡片中应用交易计数器（ATC）一起保存到交易明细文件中。

如果发卡行发卡时没有建立交易明细文件，但是在 PDOL 中指定了交易记录数据元，则卡片不能记录交易明细。

交易结束时，如果卡片核准交易通过并返回 TC，卡片内部会记录此笔交易的交易明细供持卡人脱机查询。

交易明细是以循环记录文件形式保存在卡片的某一文件中，终端可以在读取应用数据阶段通过读记录（READ REOCD）命令从 AFL 中获得该文件的 SFI(数据元标签 9F63)，然后仍然通过读记录（READ RECORD）命令从此文件中逐条读取交易明细。

该交易明细文件的修改由卡片内部完成，终端只能对其进行读取操作。

7.2.13.2 数据格式

卡片交易明细中主要包括交易日期、交易时间、授权金额、其他金额、交易国家代码、交易货币代码、商户名称、应用交易计数器等，具体格式如下：

表格 7.2.13-1：卡片交易明细—数据格式

序号	位置	说明	长度（字节）	格式
1	1—4	交易日期	4	cn YYYYMMDD
2	5—7	交易时间	3	cn HHMMSS
3	8—11	授权金额	4	b
4	12—15	其他金额	4	b
5	16—17	终端国家代码	2	n3
6	18—19	交易货币代码	2	n3
7	20—39	商户名称	20	ans
8	40	交易类型	1	n2
9	41-42	应用交易计数器（ATC）	2	b

8. 安全、密钥和数字证书

此部分定义了 PBOC 借记/贷记应用过程中与安全相关的内容，包括：

- 1. 脱机静态数据认证
- 2. 脱机动态数据认证
- 3. AC 生成和发卡行认证
- 4. 安全报文

关于各步骤中安全具体要求与实现，请参考《中国金融集成电路（IC）卡借记/贷记应用安全规范》



