

中国金融集成电路（IC）卡

借记/贷记规范

第一部分：卡片规范

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. 概述	5
6.1 功能概述	5
6.1.1 应用选择（强制）	5
6.1.2 应用初始化/读应用数据（强制）	5
6.1.3 脱机数据认证（可选）	5
6.1.4 交易处理限制（强制）	6
6.1.5 持卡人验证（强制）	6
6.1.6 终端风险管理（强制）	6
6.1.7 终端行为分析（强制）	6
6.1.8 卡片行为分析（强制）	7
6.1.9 联机处理（可选）	7
6.1.10 交易结束（强制）	7
6.1.11 发卡行到卡片的脚本处理（可选）	7
6.2 强制与可选功能	9
6.2.1 卡片功能需求	9
6.2.2 命令支持需求	10
7. 应用选择	11
7.1 卡片数据	11
7.2 终端数据	13
7.3 命令	13
7.4 建立候选应用列表	14
7.4.1 目录选择方式	14
7.4.2 AID列表选择方式	16
7.5 确定和选择应用	16
7.6 流程图	17
7.7 后续相关流程	18
8. 应用初始化	19
8.1 卡片数据	19
8.2 终端数据	20
8.3 命令	20
8.4 处理流程	20
8.5 前期相关处理	22
8.6 后续相关处理	22
9. 读应用数据	22
9.1 卡片数据	22
9.2 终端数据	23
9.3 命令	23

9.4	处理流程	23
9.5	前期相关处理	23
9.6	后续相关处理	23
10.	脱机数据认证	23
10.1	密钥和证书	24
10.2	决定脱机数据认证方法	24
10.2.1	卡片数据	24
10.2.2	处理流程	24
10.3	静态数据认证（SDA）	24
10.3.1	卡片数据	24
10.3.2	终端数据	26
10.3.3	命令	26
10.3.4	处理流程	26
10.4	动态数据认证（DDA）	26
10.4.1	卡片数据	26
10.4.2	终端数据	27
10.4.3	命令	28
10.4.4	处理流程	28
10.5	前期相关处理	29
10.6	后续相关处理	29
11.	处理限制	30
11.1	卡片数据	30
11.2	终端数据	31
11.3	处理流程	31
11.3.1	应用版本号检查	31
11.3.2	应用用途控制检查	31
11.3.3	应用生效日期检查	32
11.3.4	应用失效日期检查	32
11.4	前期相关处理	32
11.5	后续相关处理	32
12.	持卡人验证	32
12.1	卡片数据	33
12.2	终端数据	36
12.3	命令	36
12.4	处理流程	37
12.4.1	CVM列表处理	37
12.4.2	脱机明文PIN处理	37
12.4.3	其它CVM处理	41
12.5	前期相关处理	41
12.6	后续相关处理	41
13.	终端风险管理	41
13.1	卡片数据	41
13.2	终端数据	42
13.3	命令	42
13.4	处理流程	43

13.4.1	终端异常文件检查	43
13.4.2	商户强制交易联机	43
13.4.3	最低限额检查	43
13.4.4	随机交易选择	43
13.4.5	频度检查	43
13.4.6	新卡检查	43
13.5	前期相关处理	43
13.6	后续相关处理	44
14.	终端行为分析	44
14.1	卡片数据	44
14.2	终端数据	45
14.3	命令	46
14.4	处理流程	46
14.4.1	检查脱机处理结果	46
14.4.2	请求密文处理	46
14.5	前期相关处理	46
14.6	后续相关处理	46
15.	卡片行为分析	46
15.1	卡片数据	47
15.2	终端数据	49
15.3	命令	49
15.4	处理流程	49
15.4.1	卡片收到密文请求	49
15.4.2	卡片风险管理	49
15.4.3	卡片风险管理流程	51
15.5	卡片提供响应密文	54
15.5.1	卡片脱机拒绝交易	55
15.5.2	卡片请求联机操作	55
15.5.3	卡片脱机接受交易	56
15.5.4	复合动态数据认证/生成应用密文响应	56
15.6	流程图	57
15.7	前期相关处理	62
15.8	后续相关处理	63
16.	联机处理	63
16.1	卡片数据	63
16.2	联机响应数据	64
16.3	命令	64
16.4	处理流程	65
16.4.1	联机请求	65
16.4.2	联机响应	65
16.4.3	发卡行认证	65
16.5	流程图	66
16.6	前期相关处理	66
16.7	后续相关处理	67
17.	交易结束	67

17.1	卡片数据	67
17.2	终端数据	69
17.3	命令	70
17.4	结束操作概述	70
17.5	收到生成应用密文 (GENERATE AC) 命令	71
17.6	联机授权的交易	71
17.6.1	联机授权后请求AAC (拒绝)	72
17.6.2	联机授权后请求TC (接受)	73
17.7	请求联机操作, 但是联机授权没有完成	75
17.7.1	卡片风险管理	75
17.7.2	无法联机上送后的卡片响应	77
17.8	复合动态数据认证/生成应用密文响应	78
17.9	流程图	79
17.10	前期相关处理	85
17.11	后续相关处理	85
18.	脚本处理	85
18.1	卡片数据	85
18.2	终端数据	86
18.3	发卡行脚本操作中的密钥管理	86
18.4	认证响应数据	88
18.5	命令	88
18.6	处理流程	90
18.6.1	授权响应报文	90
18.6.2	卡片脚本处理	90
18.6.3	卡片安全报文	90
18.6.4	结果指示器	91
18.6.5	流程图	91
18.7	前期相关处理	92
18.8	后续相关处理	93
19.	卡片记录交易明细	93
19.1	交易明细记录文件	93
19.2	交易记录数据元	94
附录	1
A.	卡片数据元素定义	1
A.1	卡片和发卡行数据元描述	1
A.2	卡片和发卡行数据元需求	31
A.2.1	标签 (Tag)	31
A.2.2	需求	31
A.2.3	数据完整性 (备份)	31
A.2.4	修改能力	31
A.2.5	取回能力	31
A.2.6	静态或动态	31
A.2.7	秘密数据	31
A.2.8	ADF或DDF数据	31
A.2.9	数据需求表	32

A.2.10	数据需求表-条件号对应表	40
B.	命令规范—描述卡片支持的命令	41
B.1	发卡行脚本命令的基本处理原则	42
B.2	应用锁定（APPLICATION BLOCK）命令APDU	42
B.2.1	定义和范围	42
B.2.2	命令报文	42
B.2.3	命令报文的数据域	42
B.2.4	响应报文的数据域	42
B.2.5	响应报文返回的处理状态	43
B.3	应用解锁（APPLICATION UNBLOCK）命令APDU	43
B.3.1	定义和范围	43
B.3.2	命令报文	43
B.3.3	命令报文的数据域	43
B.3.4	响应报文的数据域	43
B.3.5	响应报文返回的处理状态	43
B.4	卡片锁定（CARD BLOCK）命令APDU	44
B.4.1	定义和范围	44
B.4.2	命令报文	44
B.4.3	命令报文的数据域	44
B.4.4	响应报文的数据域	44
B.4.5	响应报文返回的处理状态	44
B.5	外部认证（EXTERNAL AUTHENTICATE）命令APDU	44
B.5.1	定义和范围	44
B.5.2	命令报文	45
B.5.3	命令报文的数据域	45
B.5.4	响应报文的数据域	45
B.5.5	响应报文返回的处理状态	45
B.6	生成应用密文（GENERATE AC）命令APDU	46
B.6.1	定义和范围	46
B.6.2	命令报文	46
B.6.3	命令报文的数据域	47
B.6.4	响应报文的数据域	47
B.6.5	响应报文返回的处理状态	48
B.7	取数据（GET DATA）命令APDU	48
B.7.1	定义和范围	48
B.7.2	命令报文	49
B.7.3	命令报文的数据域	50
B.7.4	响应报文的数据域	50
B.7.5	响应报文返回的处理状态	50
B.8	取处理选项（GET PROCESSING OPTIONS）命令APDU	50
B.8.1	定义和范围	50
B.8.2	命令报文	50
B.8.3	命令报文的数据域	50
B.8.4	响应报文的数据域	51
B.8.5	响应报文返回的处理状态	51

B.9	内部认证 (INTERNAL AUTHENTICATE) 命令APDU	51
B.9.1	定义和范围	51
B.9.2	命令报文	51
B.9.3	命令报文的数据域	52
B.9.4	响应报文的数据域	52
B.9.5	响应报文返回的处理状态	52
B.10	PIN修改/解锁 (PIN CHANGE/UNBLOCK) 命令APDU	52
B.10.1	定义和范围	52
B.10.2	命令报文	52
B.10.3	命令报文的数据域	53
B.10.4	响应报文的数据域	54
B.10.5	响应报文返回的处理状态	54
B.11	设置数据 (PUT DATA) 命令APDU	54
B.11.1	定义和范围	54
B.11.2	命令报文	55
B.11.3	命令报文的数据域	55
B.11.4	响应报文的数据域	55
B.11.5	响应报文返回的处理状态	56
B.11.6	SW2	56
B.12	读记录 (READ RECORD) 命令APDU	56
B.12.1	定义和范围	56
B.12.2	命令报文	57
B.12.3	命令报文的数据域	57
B.12.4	响应报文的数据域	57
B.12.5	响应报文返回的处理状态	57
B.13	选择 (SELECT) 命令APDU	58
B.13.1	定义和范围	58
B.13.2	命令报文	58
B.13.3	命令报文数据域	59
B.13.4	应答报文数据域	59
B.13.5	应答报文状态码	60
B.14	修改记录 (UPDATE RECORD) 命令APDU	60
B.14.1	定义和范围	60
B.14.2	命令报文	61
B.14.3	命令报文的数据域	61
B.14.4	响应报文的数据域	61
B.14.5	响应报文返回的处理状态	61
B.15	校验 (VERIFY) 命令APDU	62
B.15.1	定义和范围	62
B.15.2	命令报文	62
B.15.3	命令报文的数据域	64
B.15.4	响应报文的数据域	64
B.15.5	响应报文中的处理状态	64
C.	安全报文	64
C.1	安全报文格式	64

C.2	报文完整性和认证 (MACing)	64
C.2.1	MAC位置	64
C.2.2	MAC长度	64
C.2.3	MAC密钥生成	64
C.2.4	MAC计算	64
C.3	数据加密	66
C.3.1	数据加密密钥计算	66
C.3.2	加密数据的结构	66
C.3.3	数据加密计算	67
C.3.4	数据解密计算	67
C.4	生成过程密钥	68
C.5	命令中的安全报文	69
D.	认证密钥和算法	69
D.1	数据源	69
D.2	生成TC, AAC和ARQC	69
D.3	生成授权响应密文ARPC	70
D.4	密钥分散方法	72
E.	支持的密文版本	73
F.	算法标识	74

图 表

图表 6-1:	交易流程图例子	8
图表 7-1:	卡片目录结构例子	15
图表 7-2:	使用目录方式进行应用选择	17
图表 7-3:	使用AID列表选择方式进行应用选择	18
图表 8-1:	应用初始化流程图	21
图表 12-1:	检查PIN尝试计数器	38
图表 12-2:	脱机明文PIN处理	40
图表 15-1:	卡片行为分析处理流程图 (1)	57
图表 15-2:	卡片行为分析处理流程图 (2)	58
图表 15-3:	卡片行为分析处理流程图 (3)	59
图表 15-4:	卡片行为分析处理流程图 (4)	60
图表 15-5:	卡片行为分析处理流程图 (5)	61
图表 15-6:	卡片行为分析处理流程图 (6)	62
图表 16-1:	联机处理流程图	66
图表 17-1:	交易结束处理流程图	71
图表 17-2:	交易流程图 (1)	80
图表 17-3:	交易流程图 (2)	81
图表 17-4:	交易流程图 (3)	82
图表 17-5:	交易流程图 (4)	83
图表 17-6:	交易流程图 (5)	84
图表 18-1:	MAC密钥的生成和使用	87
图表 18-2:	安全报文加密密钥的生成和使用	88
图表 18-3:	发卡行脚本处理流程图	92

图表 C-1: 使用双长度DEA密钥计算MAC的算法.....	66
图表 C-2: 用双长度DEA密钥进行数据加密.....	67
图表 C-3: 使用双长度DEA密钥进行数据解密.....	68
图表 D-1: TC/AAC/ARQC的生成算法。.....	70
图表 D-2: 生成ARPC的算法.....	72
图表 D-3: 密钥分散.....	72
图表 D-4: 使用UDK执行卡片认证.....	73

表 格

表格 6-1: 卡片功能需求.....	9
表格 6-2: 命令支持需求.....	10
表格 7-1: 应用选择——卡片数据.....	12
表格 7-2: 应用选择——终端数据.....	13
表格 7-3: AID匹配例子.....	16
表格 8-1: 应用初始化——卡片数据.....	19
表格 8-2: 应用初始化——终端数据.....	20
表格 9-1: 读应用数据——卡片数据.....	22
表格 9-2: 读应用数据——卡片文件.....	23
表格 10-1: 脱机数据认证——卡片数据.....	24
表格 10-2: SDA中使用的卡片数据.....	25
表格 10-3: 脱机数据认证——DDA卡片数据.....	27
表格 10-4: 脱机数据认证——DDA处理中卡片内部数据元.....	27
表格 10-5: 脱机数据认证——终端数据.....	27
表格 11-1: 处理限制——卡片数据.....	30
表格 11-2: 处理限制——终端数据.....	31
表格 11-3: 应用用途控制（AUC）.....	32
表格 12-1: CVM列表处理——卡片数据.....	33
表格 12-2: CVM列表例子.....	35
表格 12-3: 脱机PIN处理——卡片数据.....	36
表格 12-4: PIN处理——终端数据.....	36
表格 13-1: 终端风险管理——卡片数据.....	41
表格 13-2: 终端风险管理——终端数据.....	42
表格 14-1: 终端行为分析——卡片数据.....	44
表格 14-2: 请求密文处理——卡片数据.....	45
表格 14-3: 检查脱机处理结果——终端数据.....	45
表格 14-4: 请求密文处理——终端数据.....	45
表格 15-1: 卡片行为分析——卡片数据.....	47
表格 15-2: 卡片行为分析——终端数据.....	49
表格 15-3: 卡片风险管理检查.....	50
表格 15-4: 卡片响应第一个生成应用密文命令.....	55
表格 16-1: 生成应用密文响应——卡片数据.....	63
表格 16-2: 决定发卡行认证——卡片数据.....	63
表格 16-3: 联机处理，发卡行认证——卡片数据.....	64
表格 16-4: 联机处理——终端数据.....	64

表格 17-1: 交易结束——卡片数据.....	67
表格 17-2: 生成应用密文命令响应.....	68
表格 17-3: 交易结束——终端使用的卡片数据.....	69
表格 17-4: 交易结束——终端数据.....	69
表格 18-1: 发卡行脚本处理——卡片数据.....	85
表格 18-2: 发卡行脚本处理——终端数据.....	86
表格 18-3: 发卡行脚本处理——联机响应数据.....	88
表格 A-1: 卡片和终端的数据元描述.....	1
表格 A-2: 数据需求.....	32
表格 A-3: 条件号对应条件.....	40
表格 B-1: APPLICATION BLOCK命令报文.....	42
表格 B-2: APPLICATION UNBLOCK命令报文.....	43
表格 B-3: CARD BLOCK命令报文.....	44
表格 B-4: EXTERNAL AUTHENTICATE命令报文.....	45
表格 B-5: 生成应用的密文类型.....	46
表格 B-6: GENERATE AC命令报文.....	46
表格 B-7: GENERATE AC引用控制参数.....	46
表格 B-8: GENERATE AC响应报文数据域格式1.....	47
表格 B-9: 密文信息数据编码.....	47
表格 B-10: 使用GET DATA命令访问的静态数据.....	48
表格 B-11: GET DATA命令报文.....	49
表格 B-12: GET PROCESSING OPTIONS命令报文.....	50
表格 B-13: GET PROCESSING OPTIONS响应报文数据域格式.....	51
表格 B-14: INTERNAL AUTHENTICATE命令报文.....	51
表格 B-15: PIN CHANGE/UNBLOCK命令报文.....	52
表格 B-16: 使用PUT DATA命令修改的数据.....	55
表格 B-17: PUT DATA命令报文.....	55
表格 B-18: PUT DATA命令的警告响应码.....	56
表格 B-19: READ RECORD命令报文.....	57
表格 B-20: READ RECORD命令引用控制参数.....	57
表格 B-21: READ RECORD响应报文数据域.....	57
表格 B-22: SELECT命令报文.....	58
表格 B-23: SELECT命令引用控制参数.....	58
表格 B-24: SELECT命令的可选参数.....	58
表格 B-25: 选择PSE的应答报文 (FCI).....	59
表格 B-26: 选择DDF的应答报文 (FCI).....	59
表格 B-27: 选择ADF的应答报文 (FCI).....	60
表格 B-28: UPDATE RECORD命令报文.....	61
表格 B-29: UPDATE RECORD命令引用控制参数.....	61
表格 B-30: UPDATE RECORD命令的警告响应码.....	61
表格 B-31: UPDATE RECORD命令的错误响应码.....	62
表格 B-32: VERIFY命令报文.....	62
表格 B-33: VERIFY命令参考数据定义 (P2).....	63
表格 D-1: TC/AAC/ARQC数据元顺序.....	69
表格 E-1: 生成TC/AAC和ARQC的数据.....	73

1. 引言

《中国金融集成电路（IC）卡借记/贷记应用卡片规范》从卡片角度根据交易流程描述了芯片卡和终端在 PBOC 借记贷记交易中相关的技术细节，包括卡片内部处理细节、所使用数据元、卡片支持的指令集等。

2. 范围

《中国金融集成电路（IC）卡借记/贷记应用卡片规范》适用于由银行发行或接受的金融借记/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）卡文件

- 《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
密码 Cryptogram	加密运算的结果
金融交易 Financial Transaction	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
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	应用认证密码(Application Authentication Cryptogram)
AAR	应用授权参考(Application Authorization Referral)
AC	应用密码(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	授权响应密码(Authorization Response Cryptogram)
ARQC	授权请求密码(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	Europe 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. 概述

本章概述了 PBOC 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。

6.1 功能概述

下面是 PBOC 借记/贷记交易处理中用到的功能。有些强制功能中的某些步骤是可选。没有标注强制的功能是可选，是否执行要由卡片或终端中的参数决定。

6.1.1 应用选择（强制）

面对一张 PBOC 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。

6.1.2 应用初始化/读应用数据（强制）

在选择了 PBOC 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流程。

6.1.3 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，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。

6.1.4 交易处理限制（强制）

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，货物，服务或返现。

6.1.5 持卡人验证（强制）

持卡人认证可以用来确保持卡人是合法而且卡片没有遗失或被盗。终端使用一个卡片中的卡片认证方式（CVM）列表数据决定认证的执行方式。CVM 列表建立了持卡人认证方式优先级别，根据终端能力和交易特性提示用户采用特定的持卡人认证方式。如果持卡人认证方式是脱机 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认证。

如果卡片不支持 CVM 处理，或卡片中不存在 CVM，终端可能使用一个缺省的 CVM。

CVM处理失败
IC卡进行的明文PIN验证
联机加密PIN验证
IC卡进行的明文PIN验证和签名（纸上）
签名（纸上）
出示证件
无需CVM

6.1.6 终端风险管理（强制）

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。

6.1.7 终端行为分析（强制）

终端行为分析根据脱机数据认证，交易处理限制，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（IACs）数据域中设置。支付系统的规则在终端行为代码（TACs）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：接受交易是交易证书（TC），联机是授权请求密文（ARQC），拒绝是应用认证密文（AAC）。终端请求中指明交易是否符合执行 CDA。

6.1.8 卡片行为分析（强制）

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。TC 可以作为一个交易“证据”当一个持卡人质疑一笔交易的时候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。

6.1.9 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联机卡片认证（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。

传回终端的授权响应报文包括一个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，校验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。

6.1.10 交易结束（强制）

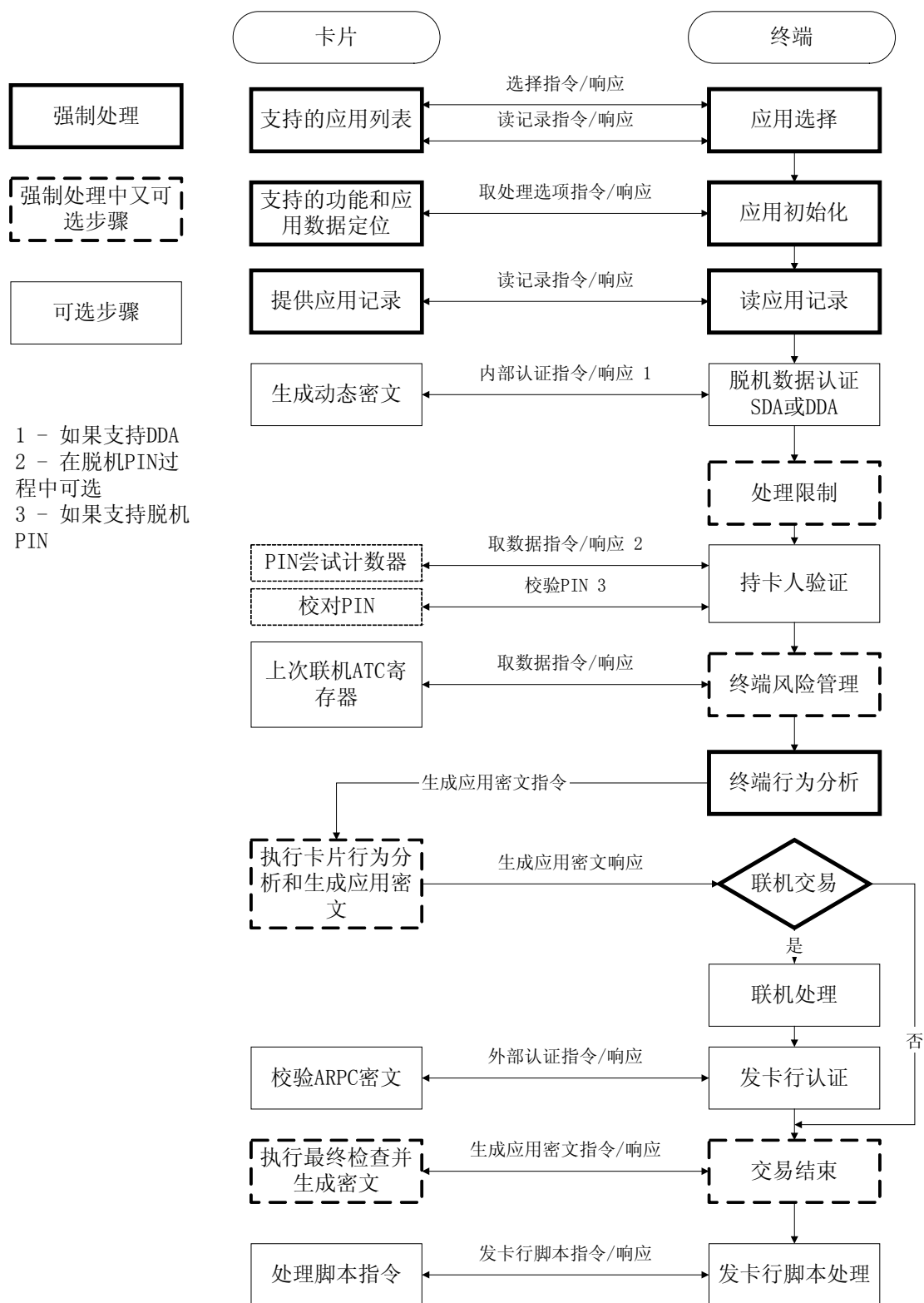
卡片和终端执行最后的交易结束处理。一个发卡行接受的交易可能因为发卡行认证结果和卡片中的发卡行编码参数而被修改为拒绝。卡片使用交易处理结果、发卡行认证结果和发卡行编码规则决定是否重新设置基于卡片的计数器和指示器（位）。卡片接受交易生成 TC，拒绝交易生成 AAC。

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。

6.1.11 发卡行到卡片的脚本处理（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，卡片执行安全校验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，修改脱机 PIN 值。



图表 6-1：交易流程图例子

6.2 强制与可选功能

6.2.1 卡片功能需求

PBOC 借记/贷记卡片必须支持下表中列出的强制功能。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。

表格 6-1：卡片功能需求

功能	卡片支持
应用选择	强制 (EMV)
● 目录选择方式	可选 (EMV) 强制 (PBOC借记/贷记)
● 直接选择方式	强制 (EMV)
应用初始化	强制 (EMV)
读应用纪录	强制 (EMV)
脱机数据认证	可选 (EMV)
● SDA	可选 (EMV) 有条件——如果支持DDA (PBOC借记/贷记)
● 标准DDA	可选 (EMV) 有条件——如果支持CDA (PBOC借记/贷记)
● 复合DDA/应用密文生成	可选 (EMV)
处理限制	强制 (EMV)
● 应用版本号检查	强制 (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	强制 (EMV)
持卡人验证	可选 (EMV) 需要 (VIS)
● 单独的CVMs	可选 (EMV) 需要 (VIS)
终端风险管理	可选 (EMV) 强制 (PBOC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) 不推荐但是不排除 (PBOC借记/贷记)

● 新卡检查	可选（PBOC借记/贷记）
终端行为分析	IACs可选（EMV）IACs需要（PBOC借记/贷记）
卡片行为分析	强制（EMV）
● 联机/脱机决定	强制（EMV）
● 脱机参考	可选（EMV）不支持（PBOC借记/贷记）
● 卡片风险管理	可选（EMV）强制（PBOC借记/贷记）在PBOC DC中有些卡片风险管理步骤是可选的（参见卡片规范第11章，卡片行为分析）
● 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（PBOC借记/贷记）
联机处理	
● 联机能力	强制（EMV）
● 发卡行认证	可选（EMV）
交易结束	强制（EMV）
发卡行到卡片脚本处理	可选（EMV）
● 安全报文	如果支持脚本一些形式是强制的（EMV） 推荐的形式（PBOC借记/贷记）

6.2.2 命令支持需求

卡片支持的PBOC CC/DC的命令在下表中描述。

表格 6-2：命令支持需求

命令	卡片支持
应用锁定 APPLICATION BLOCK	应用锁定能力可选，如果支持，推荐使用应用锁定命令（PBOC借记/贷记）
应用解锁 APPLICATION UNBLOCK	应用解锁能力可选，如果支持，推荐使用应用解锁命令（PBOC借记/贷记）
卡片锁定 CARD BLOCK	卡片锁定是推荐功能，卡片锁定命令是一种方法（PBOC借记/贷记）
外部认证	有条件的——如果支持发卡行认证（EMV）

EXTERNAL AUTHENTICATE	
生成应用密文 GENERATE APPLICATION CRYPTOGRAM	强制（EMV）
取数据 GET DATA	可选（EMV） 强制（PBOC借记/贷记）
取处理选项 GET PROCESSING OPTIONS	强制（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	解锁PIN——可选，如果支持脱机。可以使用的方法是PIN修改/解锁（PBOC借记/贷记） PIN修改——可选，必须在发卡行控制的环境下（PBOC借记/贷记）
设置数据 PUT DATA	可选（PBOC借记/贷记）
读纪录 READ RECORD	强制（EMV）
选择 SELECT	强制（EMV）
修改纪录 UPDATE RECORD	可选（PBOC借记/贷记）
校验 VERIFY	有条件的——如果支持脱机PIN（EMV）

7. 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：

1. 终端建立终端和卡片都支持的应用列表
2. 从列表中确定一个应用来处理交易。

7.1 卡片数据

应用选择使用的卡片数据元和简单描述在下表中列出。附录A卡片和发卡行数据元表中有这些数据元以及他们的使用的详细描述。

表格 7-1：应用选择——卡片数据

数据元	描述
应用标识符（AID）	<p>AID由注册的应用提供者标识（RID）和专用应用标识符扩展（PIX）组成。它标识了在ISO/IEC 7816-5中描述的应用。</p> <p>如果一张卡片中有超过一个应用使用相同的AID, 卡片AID必须要有一个后缀。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。</p>
应用定义文件（ADF）	<p>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</p> <p>FCI模板</p> <p>-DF名字</p> <p>-FCI专有模板</p> <p>应用标签</p> <p>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必须为1）</p> <p>PDOL（可选。）</p> <p>语言优先级（可选）</p> <p>发卡行代码表索引（可选。如果应用首选名称存在）</p> <p>应用首选名称（可选）</p> <p>FCI发卡行自定义数据（可选）</p>
应用基本文件（AEFs）	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。ADF的FCI中和ADF目录入口的强制数据
应用首选名称	<p>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。</p> <p>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。</p>
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必须要持卡人确认才能选择
目录定义文件（DDF）	<p>定义其下目录结构的文件，DDF的FCI：</p> <p>FCI模板</p> <p>-DF名称</p> <p>-FCI专有模板</p> <p>目录文件的短文件标识符SFI</p> <p>FCI发卡行自定义数据（可选）</p>

目录文件	一个文件，列出了目录下的DDFs和ADFs。在选择后，使用READ RECORD命令对它进行访问
文件控制信息（FCI）	SELECT命令的响应信息，选择不同类型的文件，响应信息不同
发卡行编码表索引	根据ISO8859，指明在终端显示应用首选名称时使用的编码表
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，入口格式由EMV定义。
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 EMV保留 11-20 支付系统专用 21-30 发卡行专用

7.2 终端数据

应用选择使用的终端数据在下表中描述。终端数据的详细描述可参考终端规范。

表格 7-2：应用选择——终端数据

数据元	描述
AID	AID由注册的应用提供者标识（RID）和专用应用标识符扩展（PIX）组成。它标识了在ISO/IEC 7816-5中描述的应用。参见表格 7-1：应用选择——卡片数据中的描述。
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

7.3 命令

选择（SELECT）

选择命令在附录B中有详细描述。

终端发送 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，语言优先级。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）

命令可以有如下 SW1 SW2 返回状态码：

- 9000——SELECT 命令成功返回
- 6A82——卡片不支持目录选择方式（命令中包括支付系统环境名称）和文件未找到

- 6A82——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（命令包含 AID）
- 6A81——卡片锁定或命令不支持
- 6283——应用锁定

如果卡片包括一个 PDOL，PDOL 作为 FCI 的一部分包括在 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）

READ RECORD 命令在附录B中有详细描述。

当使用目录选择方式时，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 可以有如下列返回值：

- 9000——成功执行
- 6A83——记录号不存在

7.4 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。

- 目录选择方式是卡片和终端都强制要求的。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应用加入候选列表中
- AID 列表选择方式是卡片和终端都强制要求的。终端为每一个终端支持的应用发送一个 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。

7.4.1 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：

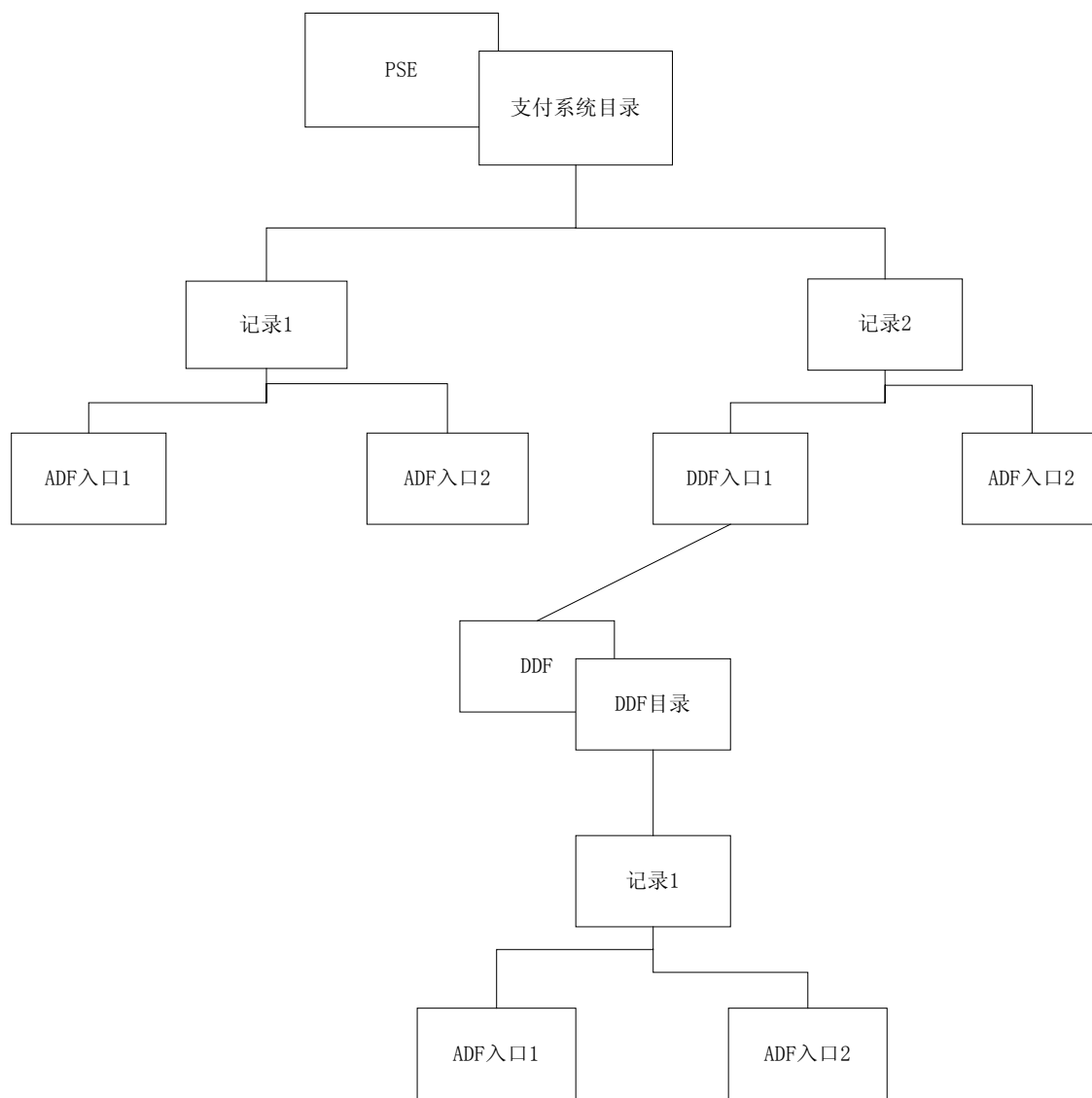
1. 卡片接收一个来自终端的 SELECT 命令，请求选择 PSE（文件名“1PAY.SYS.DDF01”）。
 - 如果卡片锁定或者 SELECT 命令不支持，卡片响应 SW1 SW2=“6A81”。
 - 如果卡片中没有 PSE，卡片响应 SELECT 命令指出文件不存在（SW1 SW2=“6A82”）
 - 如果 PSE 锁定，卡片响应“6283”
 - 如果 PSE 找到，卡片响应“9000”返回 PSE 的 FCI。
2. 如果 PSE 找到，卡片接受终端发出的表明短文件标识和记录号的 READ RECORD 命令，卡片对每一个 READ RECORD 命令响应请求的记录内容和返回状态码 SW1 SW2=“9000”。当请求的记录不存在，卡片返回 SW1 SW2=“6A83”。
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 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 READ RECORD 命令返回请求的记录和状态码“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下图所示：

1. 从支付系统目录读记录 1。
2. 检查 ADF 入口 1 或 2 中的 AID 是否和终端 AIDs 匹配。如果匹配，加入候选列表。
3. 从支付系统目录读记录 2。
4. 选择记录 2 中入口 1 指出的 DDF 目录
5. 读 DDF 目录文件中的记录 1。
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。
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。
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。
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。

图表 7-1：卡片目录结构例子



7.4. 2AID列表选择方式

从卡片的角度来看，AIDs 列表选择方式包括下列步骤：

1. 卡片收到终端发来 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 匹配的例子在下表中显示。

表格 7-3：AID匹配例子

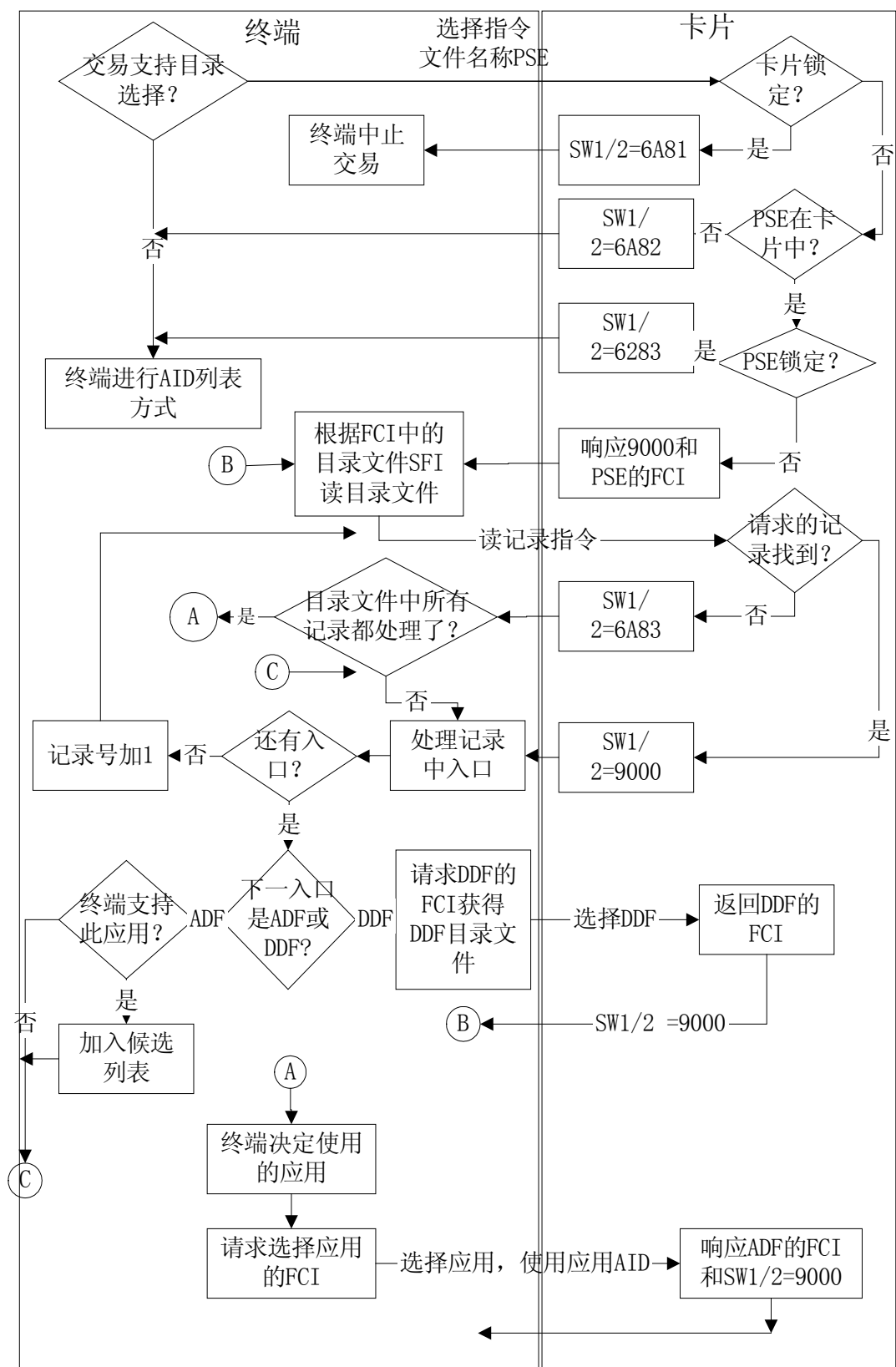
终端AID	终端应用	卡片AID	卡片应用
	PBOC		PBOC 借记
	PBOC		PBOC贷记

- 如果 AID 匹配，卡片响应 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，卡片响应状态码 SW1 SW2= “6A82” 指明应用没找到。
 - 如果卡片锁定或不支持 SELECT 命令，卡片响应状态码 SW1 SW2= “6A81” 指明交易应被中止。
2. 如果匹配的卡片 AID 长度比终端 AID 长，卡片在 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二个 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 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。

7.5 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 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”。

7.6 流程图



图表 7-2：使用目录方式进行应用选择

终端发送取处理选项（GET PROCESSING OPTIONS）命令给卡片，如果在应用选择时 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。

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。

8. 应用初始化

在应用初始化处理中，终端通过发送 GET PROCESSING OPTIONS 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。

8.1 卡片数据

应用初始化处理使用的卡片数据在下表中列出。

表格 8-1：应用初始化——卡片数据

数据元	描述
应用文件定位器（AFL）	<p>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：</p> <ul style="list-style-type: none"> ● 字节1——短文件标识符（一个文件的数字标签） ● 字节2——第一个要读出的记录号 ● 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指出的是第一条要读的记录号
应用交互特征（AIP）	<p>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）。</p> <p>AIP在个人化时必须被写入卡中用来指明支持终端风险管理和持卡人验证</p>
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）	PBOC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

8.2 终端数据

在应用初始化处理中使用的终端数据在下表中列出。

表格 8-2: 应用初始化——终端数据

数据元	描述
交易明细（9F65）	交易明细内容。当发卡行要求记录交易明细时会在PDOL中指定此数据元，在GPO指令中由终端提供给卡片。
PDOL中定义的其它数据	PDOL中指定的来自终端的其它数据

注：阴影部分的数据是VIS定义的PDOL处理需要的数据

8.3 命令

取处理选项（GET PROCESSING OPTIONS）

终端使用 GET PROCESSING OPTIONS 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。

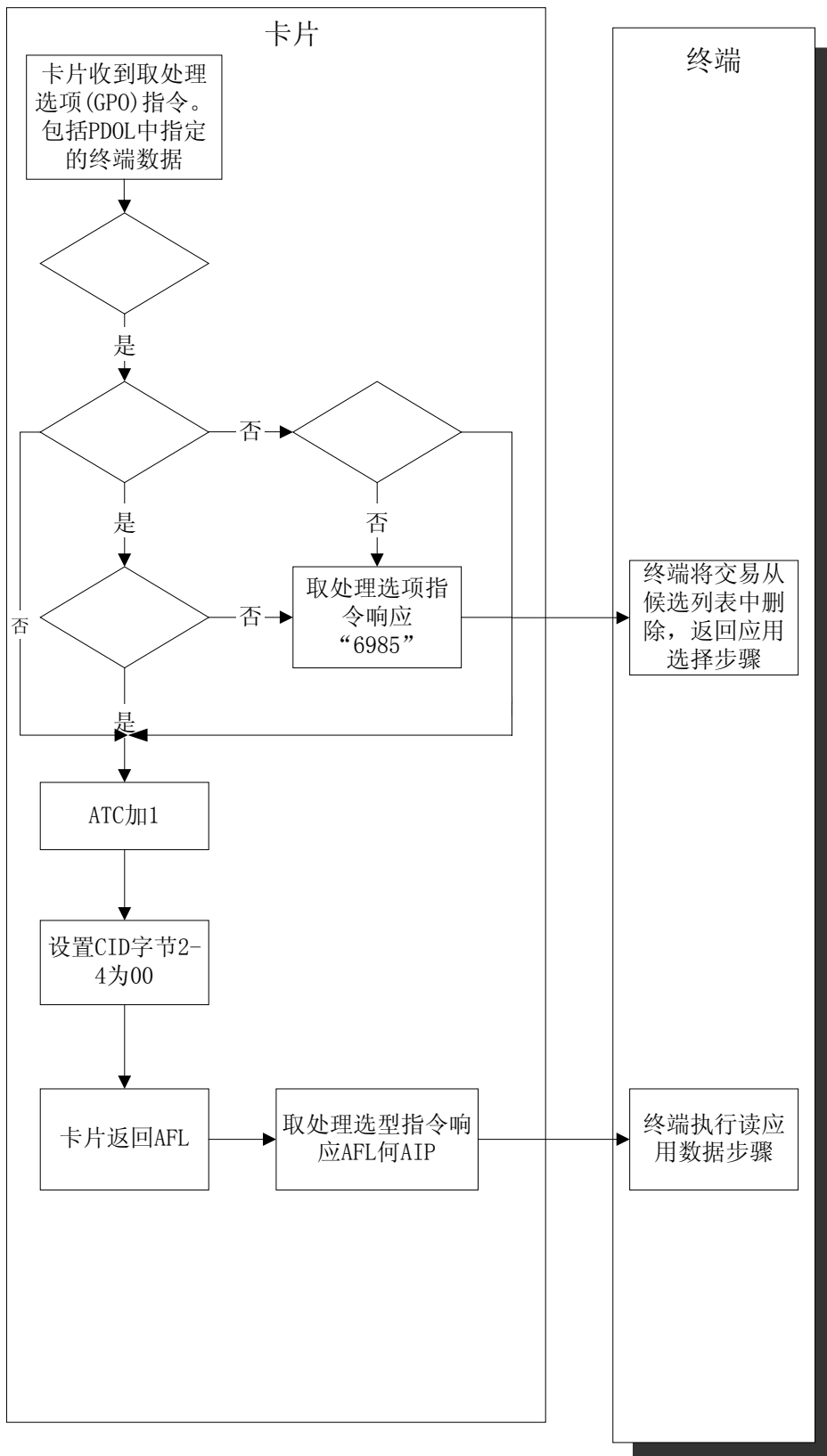
命令编码见附录B。

8.4 处理流程

卡片收到终端发送的 GET PROCESSING OPTIONS 命令后，卡片：

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。
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。
3. 如果自定义限制检查通过，卡片
 - a) ATC 加 1
 - 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

下图显示了应用初始化处理流程图。



图表 8-1：应用初始化流程图

8.5 前期相关处理

应用选择

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

8.6 后续相关处理

应用选择

如果地域限制或其它限制生效，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 GET PROCESSING OPTIONS 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那些数据用于脱机数据认证。

脱机数据认证

终端使用卡片在 GET PROCESSING OPTIONS 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 GET PROCESSING OPTIONS 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 GET PROCESSING OPTIONS 命令的响应信息中的 AIP 决定卡片是否支持发卡行认证。

9. 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 的必须数据。

9.1 卡片数据

下表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。

表格 9-1：读应用数据——卡片数据

数据元	描述
应用文件定位器（AFL）	<p>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：</p> <ul style="list-style-type: none">● 文件的短文件标识符（SFI）● 第一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。从文件中第一个开始读取的记录号开始计算。

下表中列出读取卡片中应用基本文件记录的数据。

表格 9-2：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

9.2 终端数据

卡片在此步骤中不使用终端数据。

9.3 命令

读纪录（READ RECORD）

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。

9.4 处理流程

卡片收到终端发送的 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 READ RECORD 命令读出。

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

使用 READ RECORD 命令读出的数据参见附录A.2。

9.5 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。

9.6 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。

10. 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必须支持脱机数据认证，卡片是否支持是可选的。

10.1 密钥和证书

在安全规范“6.1 密钥和证书”中描述。

10.2 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。

10.2.1 卡片数据

终端用来决定是否执行 SDA 或 DDA 的卡片数据在下表中列出。

表格 10-1：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： <ul style="list-style-type: none">● 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

10.2.2 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。

10.3 静态数据认证（SDA）

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。

10.3.1 卡片数据

终端在 SDA 处理中使用的卡片数据在下表中列出。

表格 10-2：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。定义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算法中恢复发卡行公钥证书。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）	<p>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：</p> <p>应用交互特征AIP（如果支持DDA）</p> <p>应用生效日期</p> <p>应用失效日期</p> <p>应用主账号</p> <p>应用主账号序列号</p> <p>应用用途控制AUC</p> <p>持卡人验证方法（CVM）列表</p> <p>发卡行行为代码——缺省</p> <p>发卡行行为代码——拒绝</p> <p>发卡行行为代码——联机</p> <p>发卡行国家代码（“5F28”）</p> <p>如果应用中签名的数据不是唯一，卡片必须支持多个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。</p> <p>如果发行后的卡片有修改签名数据的能力，则卡片必须支持修改SAD的能力。</p>
SDA标签列表	如果AIP也要签名，SDA标识列表包括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。

下表中是和 SDA 相关的卡片内部数据。

表格 10-3：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。

10.3.2 终端数据

在 SDA 过程中，卡片不需要终端数据。

10.3.3 命令

SDA 操作没有使用命令。

10.3.4 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。详细描述见安全规范 6.2 静态数据认证（SDA）。概括的描述如下：

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

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

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。

10.4 动态数据认证（DDA）

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。

PBOC 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，同时验证一个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。

10.4.1 卡片数据

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

表格 10-4：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。PBOC里规定：1字节为IC卡动态数据长度；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。PBOC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INTERNAL AUTHENTICATION命令生成的签名。

在 DDA 处理中，卡片内部使用的数据元在下表中列出。

表格 10-5：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
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

10.4.2 终端数据

下表列出 DDA 处理中卡片使用的来自终端的数据。

表格 10-6：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

10.4.3 命令

10.4.3.1 内部认证（INTERNAL AUTHENTICATE）命令

在标准 DDA 处理过程中，终端发送 INTERNAL AUTHENTICATE 命令。命令包括了 DDOL 或缺省 DDOL 中指定的终端动态数据。

当卡片收到 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。

10.4.3.2 生成应用密文（GENERATE APPLICATION CRYPTORAM（AC））命令

终端在卡片行为分析处理步骤中发送第一次 GENERATE AC 命令，下面两种情况满足一种，交易执行 CDA：

- 卡片的 CDOL 数据中指定终端性能数据并且送回卡片的此数据表明支持 CDA 而且卡内的 AIP 数据表明卡片也支持 CDA
- CDOL 中没有终端性能数据而且生成应用密文命令中参数 P1 的第 6 位为“1”，表明执行 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。

10.4.4 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 处理的详细描述在安全规范 6.3 动态数据认证（DDA）。下面是一个概括性的描述。

10.4.4.1 标准动态数据认证（DDA）

标准 DDA 的处理有以下步骤

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

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

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。

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。详细描述见安全规范 2.3.5 标准动态数据认证。
- 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。

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：

- a) 使用 IC 卡公钥解密动态签名恢复数据元哈希值。
- b) 使用动态数据元重新计算哈希。
- c) 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。

10.4.4.2 复合动态数据认证/应用密文生成（CDA）

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。

10.5 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认证数据（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。

10.6 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”。

11. 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。

11.1 卡片数据

在处理限制过程中使用的卡片数据在下表中列出。

表格 11-1：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	EMV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。

11.2 终端数据

在处理限制过程中使用的终端数据在下表中列出。

表格 11-2：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

11.3 处理流程

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

11.3.1 应用版本号检查

终端比较卡片和终端中的应用版本号看是否一样。

11.3.2 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：

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必须为“1”表明请求的服务允许进行。

举例：如果是一个现金交易，AUC 中“国内现金交易有效”指示位必须为“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必须为“1”表明请求的服务允许进行。

举例：如果是一个现金交易，AUC 中“国际现金交易有效”指示位必须为“1”。

2. ATM 检查

如果终端设备为 ATM，AUC 中 ATMs 有效位必须为“1”。如果终端设备不是 ATM，AUC 中“除 ATM 外的终端有效”位必须为“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”。

下表是 AUC 的编码格式，如果指示位的值为“1”说明支持此用途。

表格 11-3: 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

11.3.3 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。

11.3.4 应用失效日期检查

应用失效日期检查是强制的。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。

11.4 前期相关处理

读应用数据

终端使用 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。

11.5 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。

12. 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。

12.1 卡片数据

下表描述了 CVM 列表处理过程中终端使用的卡片数据。

表格 12-1：CVM列表处理——卡片数据

数据元	描述
应用货币码	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和金额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

<p>持卡人验证方式列表（CVM List）</p>	<p>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：</p> <ul style="list-style-type: none"> ● 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： <table border="1"> <thead> <tr> <th>子集</th><th>描述</th></tr> </thead> <tbody> <tr> <td>CVM代码</td><td>指出如果这个CVM失败，是执行下一CVM还是认为CVM失败</td></tr> <tr> <td>CVM类型</td><td>CVM的类型有： <ul style="list-style-type: none"> ●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 ●不需要CVM（认为CVM通过） ●CVM处理失败（认为CVM失败） ●出示证件 </td></tr> <tr> <td>CVM条件</td><td>此CVM的使用条件，包括： <ul style="list-style-type: none"> ●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 <p>注意：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）</p> </td></tr> </tbody> </table>	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： <ul style="list-style-type: none"> ●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 ●不需要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： <ul style="list-style-type: none"> ●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 <p>注意：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）</p>
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： <ul style="list-style-type: none"> ●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 ●不需要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： <ul style="list-style-type: none"> ●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 <p>注意：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）</p>								

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 列表内容参考下表：

表格 12-2：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	
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
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-不需要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下表中描述。

表格 12-3: 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尝试次数计数器	<p>指明PIN的剩余尝试次数。卡片使用GET DATA命令返回PIN尝试计数器（可选）。在校验命令中返回给终端。</p> <p>当PIN校验不成功，计数器减一，直到校验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校验时，此计数器应存在卡片中。</p> <p>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，此数据必须可以由GET DATA命令读出。否则此数据不应由终端通过GET DATA命令读取。</p>
脱机PIN	卡片脱机PIN被安全的保存在卡片中。
卡片认证结果（CVR）	<p>包括下列内容的指示位：</p> <ul style="list-style-type: none">● 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

12.2 终端数据

下表列出了终端使用的数据

表格 12-4: PIN处理——终端数据

数据元	描述
交易PIN	持卡人输入的PIN

12.3 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 尝试次数计数器的值，可选。
如果卡片不支持用 GET DATA 命令返回 PIN 尝试次数计数器，卡片返回“6A88”。
- 校验（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 VERIFY 命令。

命令的响应状态码 SW1 SW2 可能有如下返回值：

- “9000” 校验成功
- “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，本次交易第一次处理 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 VERIFY 命令时返回

12.4 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。

12.4.1 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。

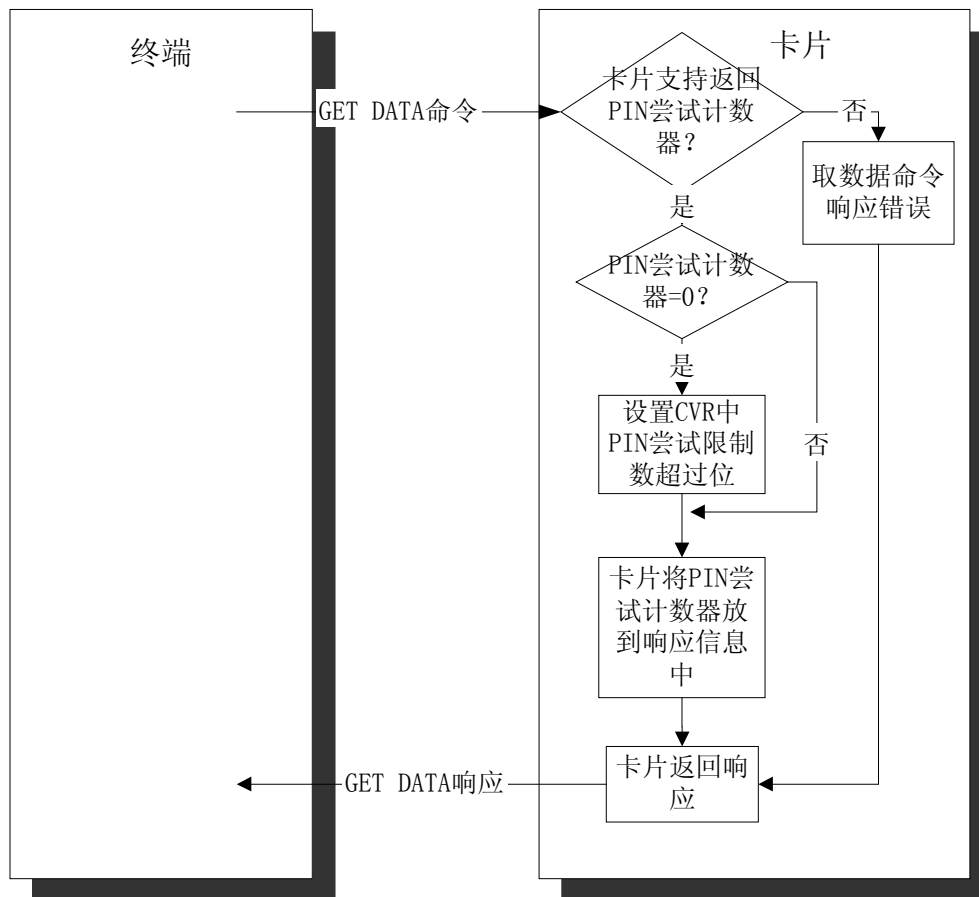
12.4.2 脱机明文PIN处理

当一个 PIN 传送给卡片后，卡片的处理：

1. 检查 PIN 尝试次数计数器

在终端决定要输入一个脱机 PIN 以后，终端可以发送一个 GET DATA 命令获取 PIN 尝试次数计数器值。

- a) 如果卡片支持使用取数据命令返回 PIN 尝试次数计数器，卡片：
 - 如果 PIN 尝试次数计数器为“0”，设置 CVR 中“PIN 尝试限制数超过”位为“1”。
 - 在 GET DATA 命令的响应信息中返回 PIN 尝试次数计数器。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 GET DATA 命令返回 PIN 尝试次数计数器，卡片要返回“6A88”。



图表 12-1：检查PIN尝试计数器

2. 接收校验（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 VERIFY 命令。当卡片收到 VERIFY 命令，卡片要设置 CVR 中“脱机 PIN 验证执行”位为“1”。

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：

- 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 尝试次数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”

- 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：

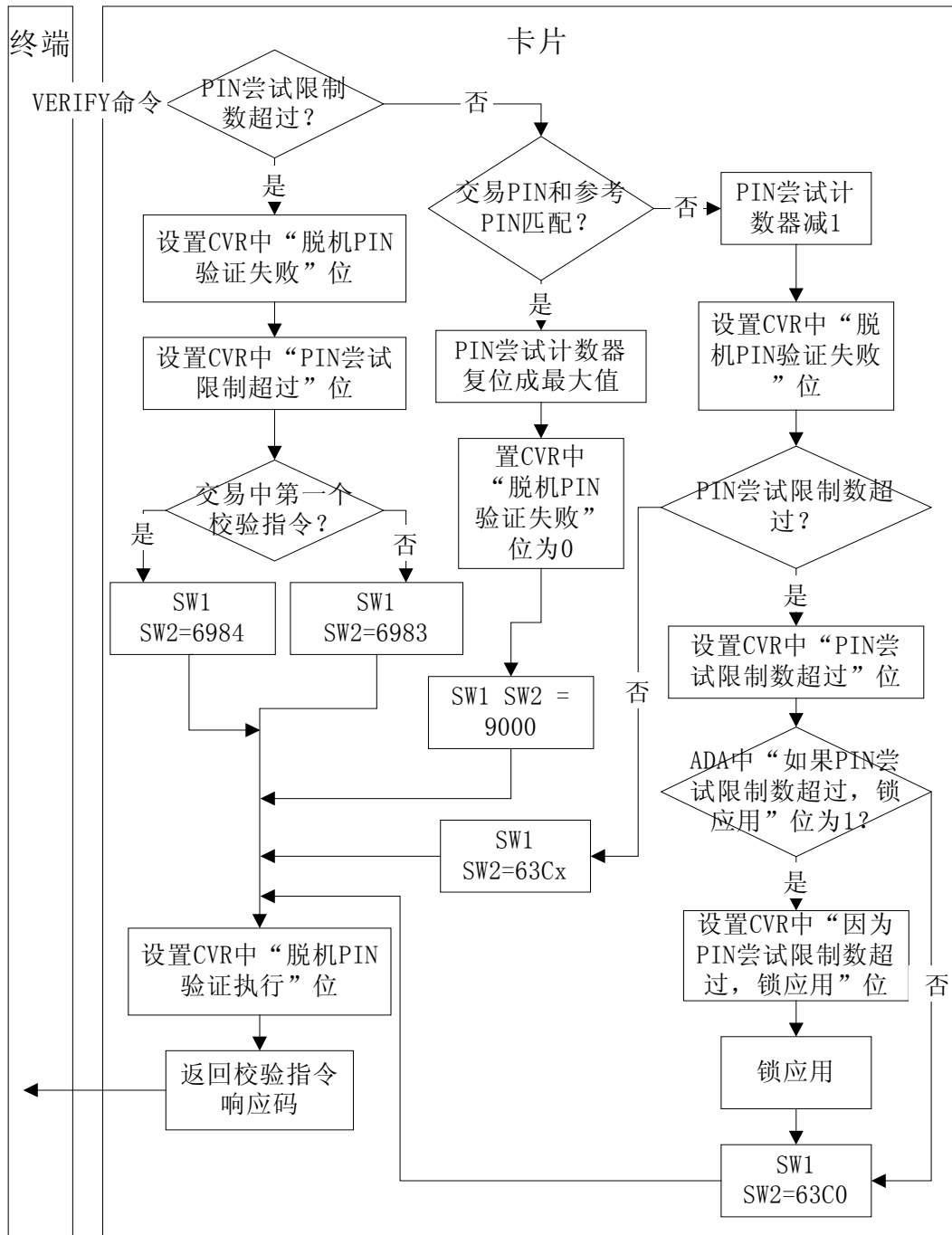
-设置 CVR 中 “PIN 尝试限制数超过” 位为 “1”

-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。

-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 VERIFY 命令 “63Cx”，x 表示剩余的尝试次数。



图表 12-2：脱机明文PIN处理

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 VERIFY 命令。

如果在 PIN 尝试次数减为零之前 PIN 校验成功，卡片：

- PIN 尝试次数计数器重置为最大值（PIN 尝试限制数）
- 设置 CVR 中“脱机 PIN 校验失败”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 VERIFY 命令

。

12.4.3 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。

12.5 前期相关处理

应用初始化

在 GET PROCESSING OPTIONS 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、持卡认证件类型、CVM 列表和其它处理 CVM 列表需要的卡片数据。

12.6 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 的校验结果，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。

13. 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。

13.1 卡片数据

终端在终端风险管理处理中使用的卡片数据在下表中列出：

表格 13-1：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
应用交易序号计数器（ATC）	当卡片中建立应用时被初始化，由应用维护
上次联机应用交易序号（ATC）寄存器	上次联机授权成功时的ATC值。 如果卡片强制要求发卡行认证，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。

13.2 终端数据

终端风险管理中使用的终端数据在下表中列出。

表格 13-2：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帐号和交易金额，并可选包含应用主帐号顺序号和交易日期。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

13.3 命令

取数据（GET DATA）命令

如果终端中上次联机应用交易序号值和应用交易序号值不存在，终端发送 GET DATA 命令从卡片中读取上次联机应用交易序号（ATC）寄存器和应用交易序号计数器（ATC）。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 PBOC 专用数据元并不能返回给终端。此时卡片响应 SW1 SW2=“6A88”。

GET DATA 命令，见附录 B

13.4 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：

13.4.1 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。

13.4.2 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。

13.4.3 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。

13.4.4 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。

13.4.5 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，终端发送阿 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。

注意：卡片在卡片行为分析处理时可以执行类似的处理。

13.4.6 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 GET DATA 命令给卡片读出上次联机 ATC 寄存器值。

注意：卡片在卡片行为分析处理时可以执行类似的处理。

13.5 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）

13.6 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

14. 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：

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（IACs）以及终端中定义的终端行为代码（TACs）。
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。

14.1 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下表中列出。

表格 14-1：终端行为分析——卡片数据

数据元	描述
-----	----

卡片行为代码（IACs）	<p>IACs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：</p> <p>IAC-拒绝</p> <p>和对应的TVR中的条件如果满足，则交易拒绝</p> <p>IAC-联机</p> <p>和对应的TVR中的条件如果满足，则交易联机</p> <p>IAC-缺省</p> <p>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</p>
--------------	---

IACs 数据建议作为静态脱机数据认证用数据。

下表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。

表格 14-2：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）

14.2 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下表中列出。

表格 14-3：检查脱机处理结果——终端数据

数据元	描述
终端行为代码（TACs）	<p>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：</p> <ul style="list-style-type: none"> ● TAC-拒绝 <p>收单行设置能够导致脱机拒绝的TVR条件位。</p> <ul style="list-style-type: none"> ● TAC-联机 <p>收单行设置能够导致交易联机的TVR条件位。</p> <ul style="list-style-type: none"> ● TAC-缺省 <p>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。</p>

终端在请求应用密文时使用的终端数据元在下表中列出。

表格 14-4：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，在生成应用密文命令中使用。
交易证书（TC）哈希结果	可选。作为输入数据使用GENERATE AC命令送入卡片

14.3 命令

生成应用密文（GENERATE APPLICATION CRYPTOGRAM（AC））

终端使用 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。当 CDOL1 中包含终端能力数据标签并且从终端返回终端能力数据值和卡片中的 AIP 表明两者都支持 CDA，则执行 CDA。

卡片处理 GENERATE AC 命令并响应。

具体的命令编码见附录B。

14.4 处理流程

14.4.1 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。

14.4.2 请求密文处理

在请求密文处理过程中，终端发送一个 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。（下一章：卡片行为分析）

14.5 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。

14.6 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。

15. 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 PBOC 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。

15.1 卡片数据

下表列出了在卡片行为分析处理过程中使用的卡片数据。

表格 15-1：卡片行为分析——卡片数据

数据元	描述
应用密文	<p>生成应用密文命令的响应信息。</p> <ul style="list-style-type: none"> ● 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）	<p>列出在第一个生成应用密文命令中，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：</p> <ul style="list-style-type: none"> ● 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，本地货币加第二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，本地货币加第二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 <p>CDOL1中包含的数据不能重复。</p>
卡片认证结果（CVR）	PBOC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）	PBOC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）	PBOC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）	PBOC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）	PBOC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	PBOC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	PBOC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）	PBOC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二货币的脱机交易总金额
累计脱机交易金额限额（双货币）	PBOC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	用来将第二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，第一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： <ul style="list-style-type: none"> ● 发卡行认证执行并失败 ● 发卡行认证强制但没执行
发卡行认证指示位	指明卡片支持的发卡行认证是强制还是可选的指示位
发卡行国家代码（“9F57”）	PBOC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”）	PBOC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尝试次数计数器	记录PIN剩余的尝试次数
第二应用货币代码	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。

15.2 终端数据

下表列出在卡片风险管理处理中是使用的终端数据。

表格 15-2：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
终端认证结果（TVR）	终端记录脱机处理结果的一系列指示器。

15.3 命令

生成应用密文（GENERATE AC）命令

终端使用生成应用密文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。具体描述在安全规范脱机数据认证部分中。

15.4 处理流程

15.4.1 卡片收到密文请求

卡片收到终端发来的 GENERATE AC 命令。命令的数据部分包括 CDOL1 中卡片指定的终端数据。

表格 15-1列出了 CDOL1 中支持卡片风险管理需要的数据。

15.4.2 卡片风险管理

下表总结了所有卡片风险管理检查，并标明这些检查是否强制或可选，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 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。

表格 15-3：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强制但是没有执行）	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二货币，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

15.4.3 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。

15.4.3.1 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

注意：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”。

15.4.3.2 上次交易发卡行认证失败（或强制未执行）检查

如果卡片AIP中表明支持发卡行认证，则必须执行此检查。如果上次交易发卡行认证（1）失败或（2）强制（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”。

15.4.3.3 上次交易静态数据认证（SDA）失败检查

如果支持SDA，此检查强制执行。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”。

15.4.3.4 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”。

15.4.3.5 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”。

15.4.3.6 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 PBOC 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

15.4.3.7 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”。

15.4.3.8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”。

15.4.3.9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”。

15.4.3.10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二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、第二应用货币代码、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二应用货币代码，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：
 - 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”。

15.4.3.11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：

- 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”。

注意：如果卡片要求发卡行认证强制执行，除非发卡行认证成功，否则上次联机 ATC 寄存器值一直为零。

15.4.3.12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。

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
- 卡片没有收到过校验命令
- PIN 尝试次数计数器已经为零

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。

15.5 卡片提供响应密文

根据卡片风险管理的结果，卡片响应 GENERATE AC 命令。卡片的响应可能会修改终端在 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

下表列出了修改原则。

表格 15-4：卡片响应第一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 中第一个生成应用密文响应 TC，AAC 或 ARQC 指示位，卡片还设置 CVR 中“还没有请求第二个生成应用密文”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。

15.5.1 卡片脱机拒绝交易

当交易被脱机拒绝，卡片用 AAC 响应 GENERATE AC 命令，在响应之前，卡片：

- 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”
 - 注意：在 CID 中，“服务不被允许”原因代码比其它原因代码优先
- 2. 检查在 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”
- 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

15.5.2 卡片请求联机操作

当交易联机上送做授权，卡片用 ARQC 响应 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”。

注意：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）

15.5.3 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二应用货币代码，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 GET PROCESSING OPTIONS 命令传送到卡片中。关于卡片交易明细的内容在 19 章中有详细描述。

15.5.4 复合动态数据认证/生成应用密文响应

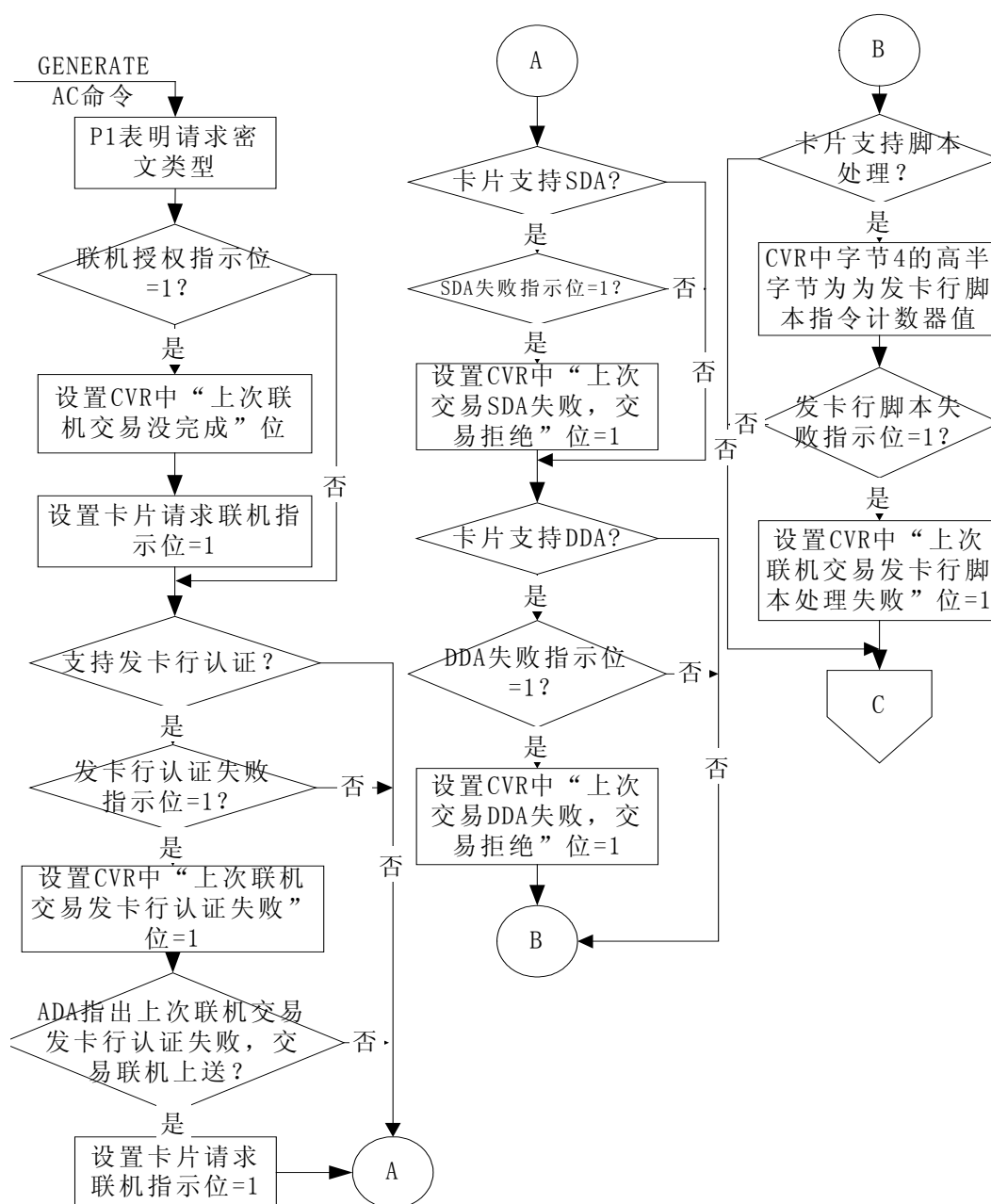
下面列出的情况有一项发生，卡片执行 CDA：

- 卡片的 CDOL1 中包括终端能力数据标签，而且终端回送的终端能力数据和卡片中的应用交互特征（AIP）中都标明支持 CDA。
- 卡片的 CDOL1 中不包括终端能力数据标签，终端发送的生成应用密文命令中的 P1 参数中 CDA 位为“1”。

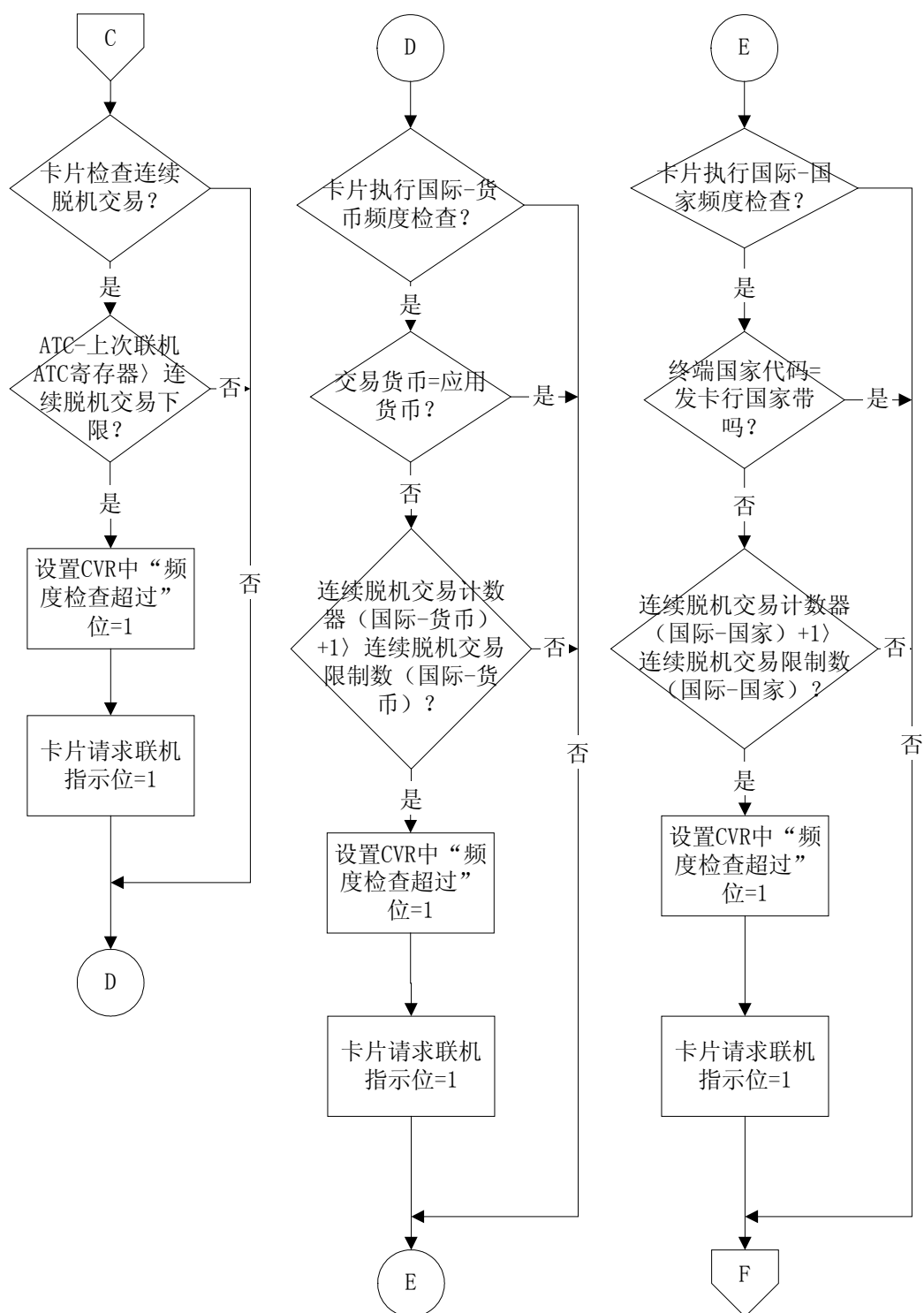
卡片：

1. 按照上面的描述执行卡片风险管理，生成应用密文
2. 如果卡片响应 AAC，没有特殊处理
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，详见安全规范 6.3.6。归纳为下面 4 个步骤：
 - 在安全规范中 6.3.6 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 GENERATE AC 指令响应中包括签名的动态应用数据。

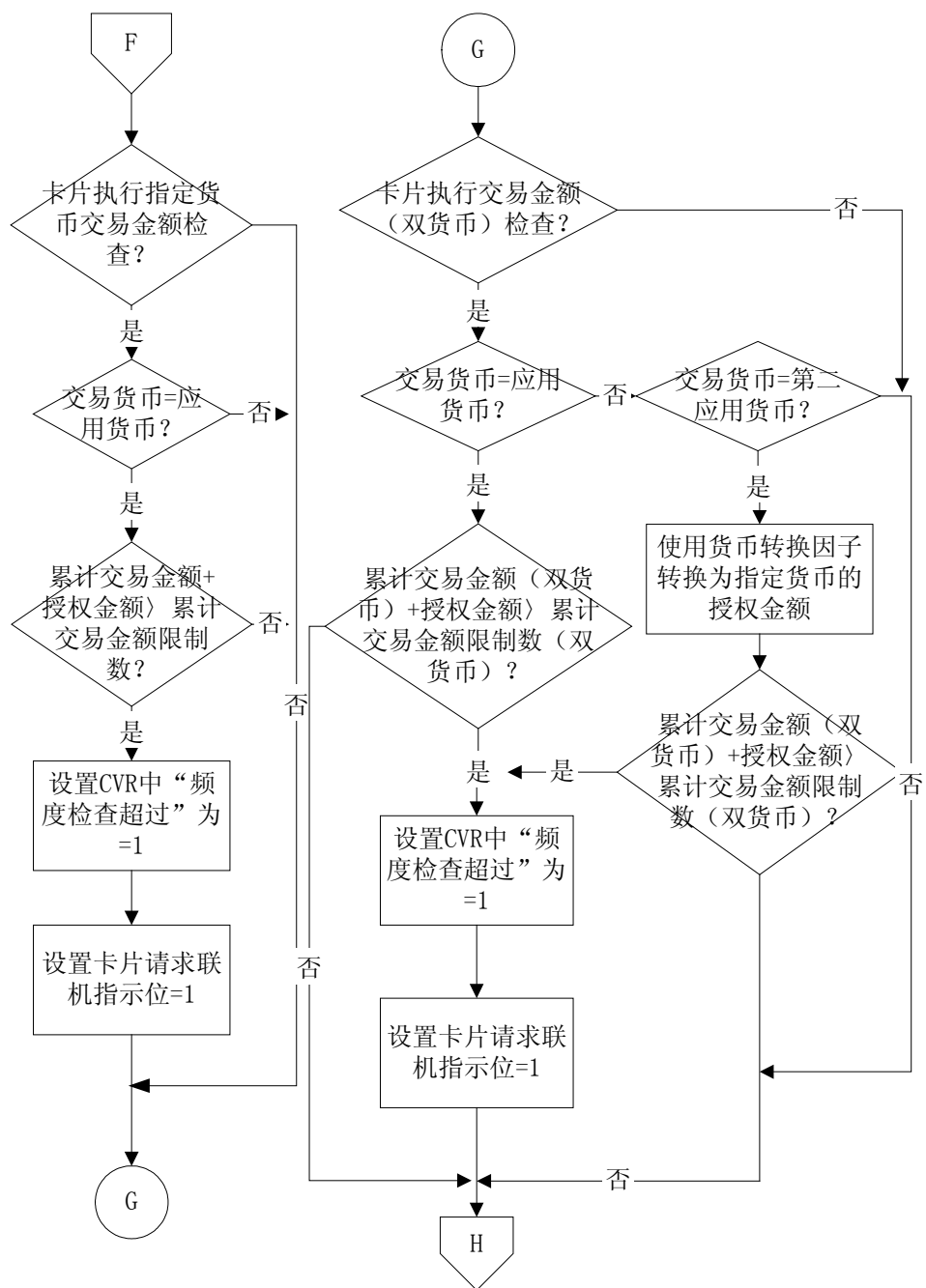
15.6 流程图



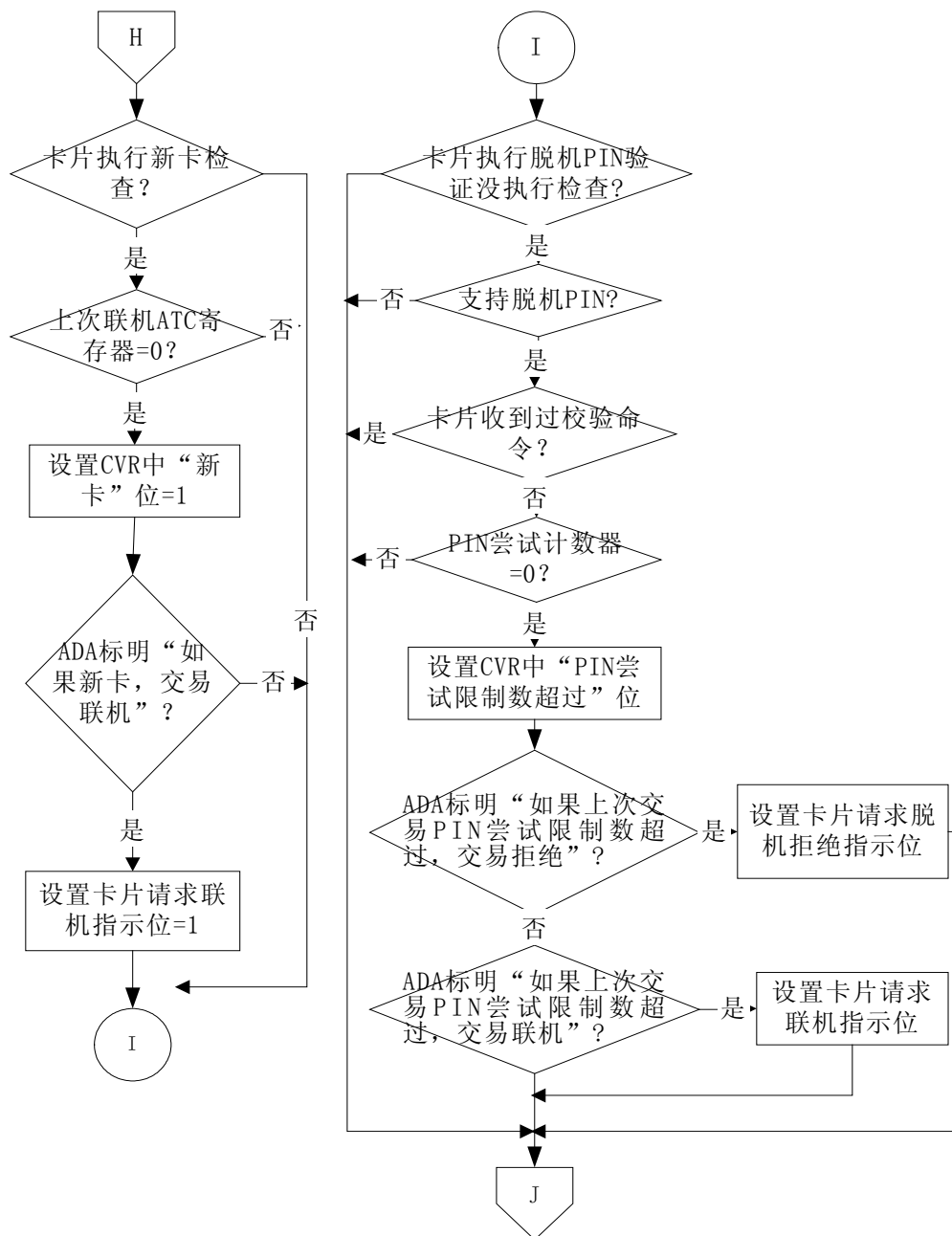
图表 15-1：卡片行为分析处理流程图（1）



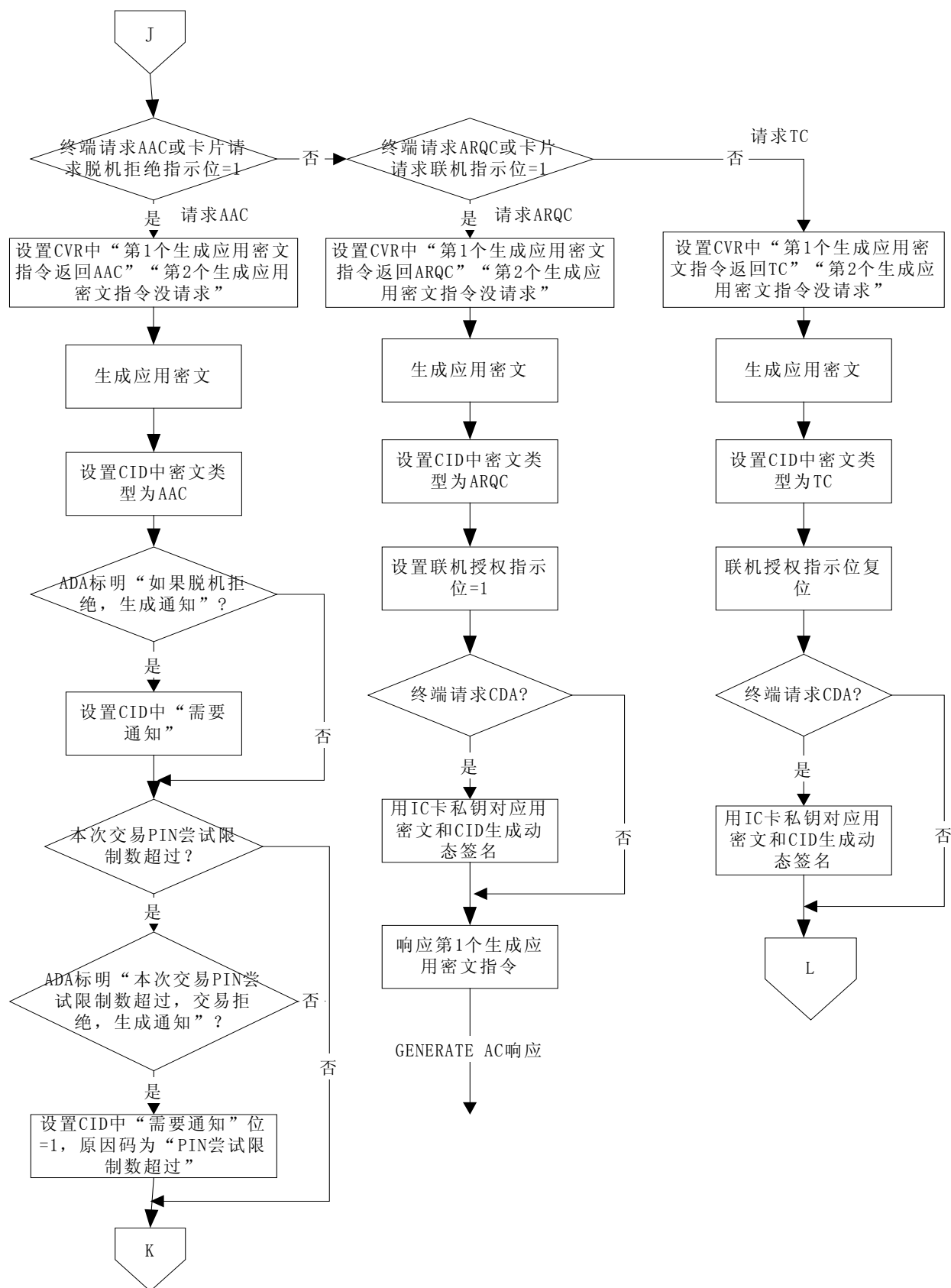
图表 15-2：卡片行为分析处理流程图（2）



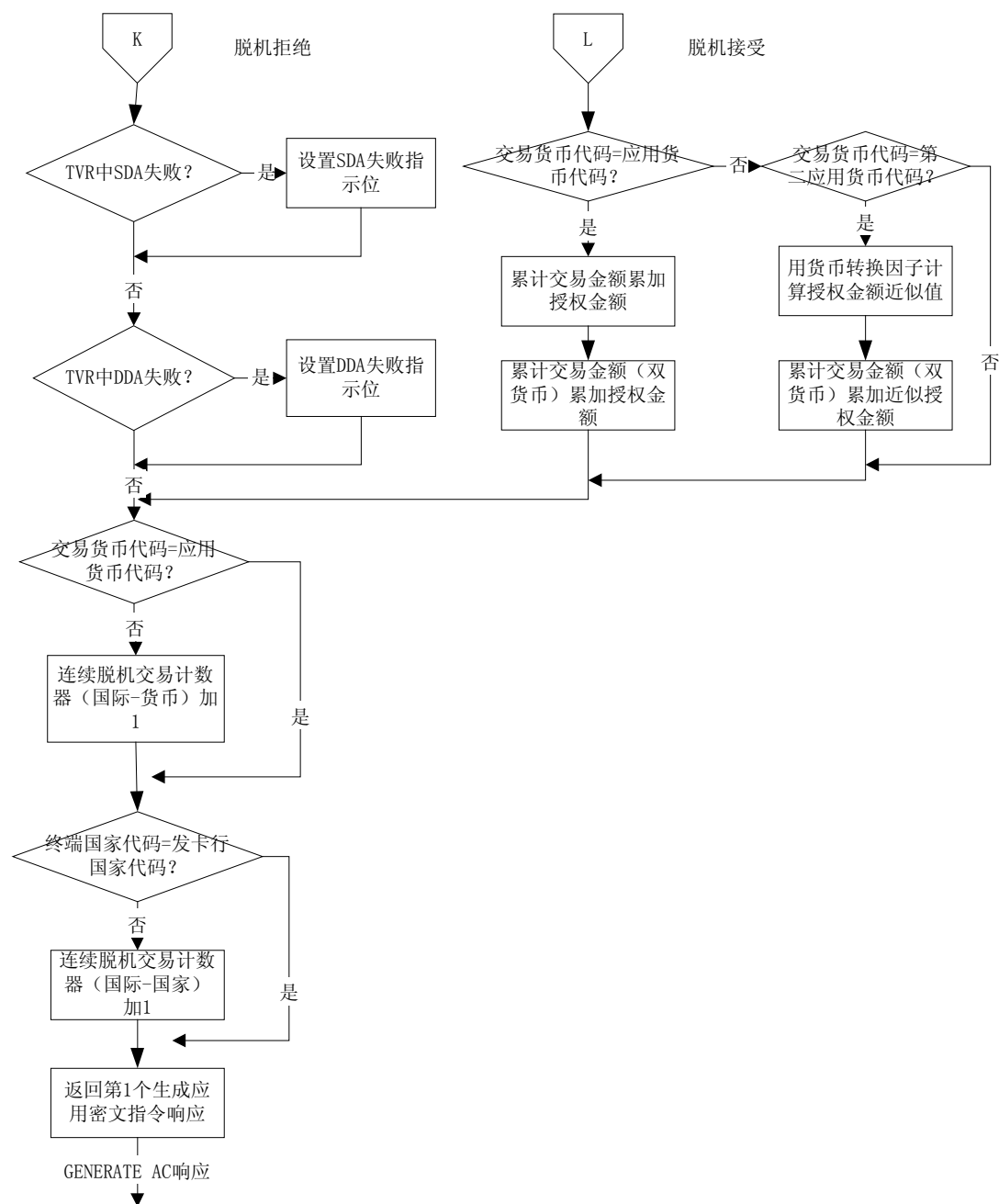
图表 15-3：卡片行为分析处理流程图（3）



图表 15-4：卡片行为分析处理流程图（4）



图表 15-5：卡片行为分析处理流程图（5）



图表 15-6：卡片行为分析处理流程图（6）

15.7 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

终端发送第一个 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。

15.8 后续相关处理

联机处理

终端根据生成应用密文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。

16. 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。

这一章描述卡片联机处理功能。

16.1 卡片数据

下表列出了在联机处理过程中终端使用的卡片数据。

表格 16-1：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PBOC强制数据，用来把PBOC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： <ul style="list-style-type: none">● 长度指针● 分散密钥索引● 密文版本信息● 卡片验证结果（CVR）● 发卡行自定义数据（可选）

下表列出了在收到联机请求后，终端使用的卡片数据

表格 16-2：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 12-3 列出了在发卡行认证处理中卡片用到的数据

表格 16-3：联机处理，发卡行认证——卡片数据

数据元	描述
授权请求密文（ARQC）	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）
卡片认证结果（CVR）	CVR包括了下列和发卡行认证相关的标记： <ul style="list-style-type: none"> ● 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

16.2 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下表列出。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。

表格 16-4：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。

16.3 命令

外部认证（EXTERNALAUTHENTICATE）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。

16.4 处理流程

联机处理由三部分组成：联机请求处理，联机响应处理和发卡行认证。卡片只在发卡行认证过程中有操作。

16.4.1 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。

16.4.2 联机响应

在联机响应处理中，卡片不进行操作。

16.4.3 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：

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”。
 - 返回状态码 SW1 SW2=“6985”。
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。
3. 使用第一次 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。
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：

1. 设置发卡行认证失败指示位为“0”。
2. 外部认证命令响应“9000”。

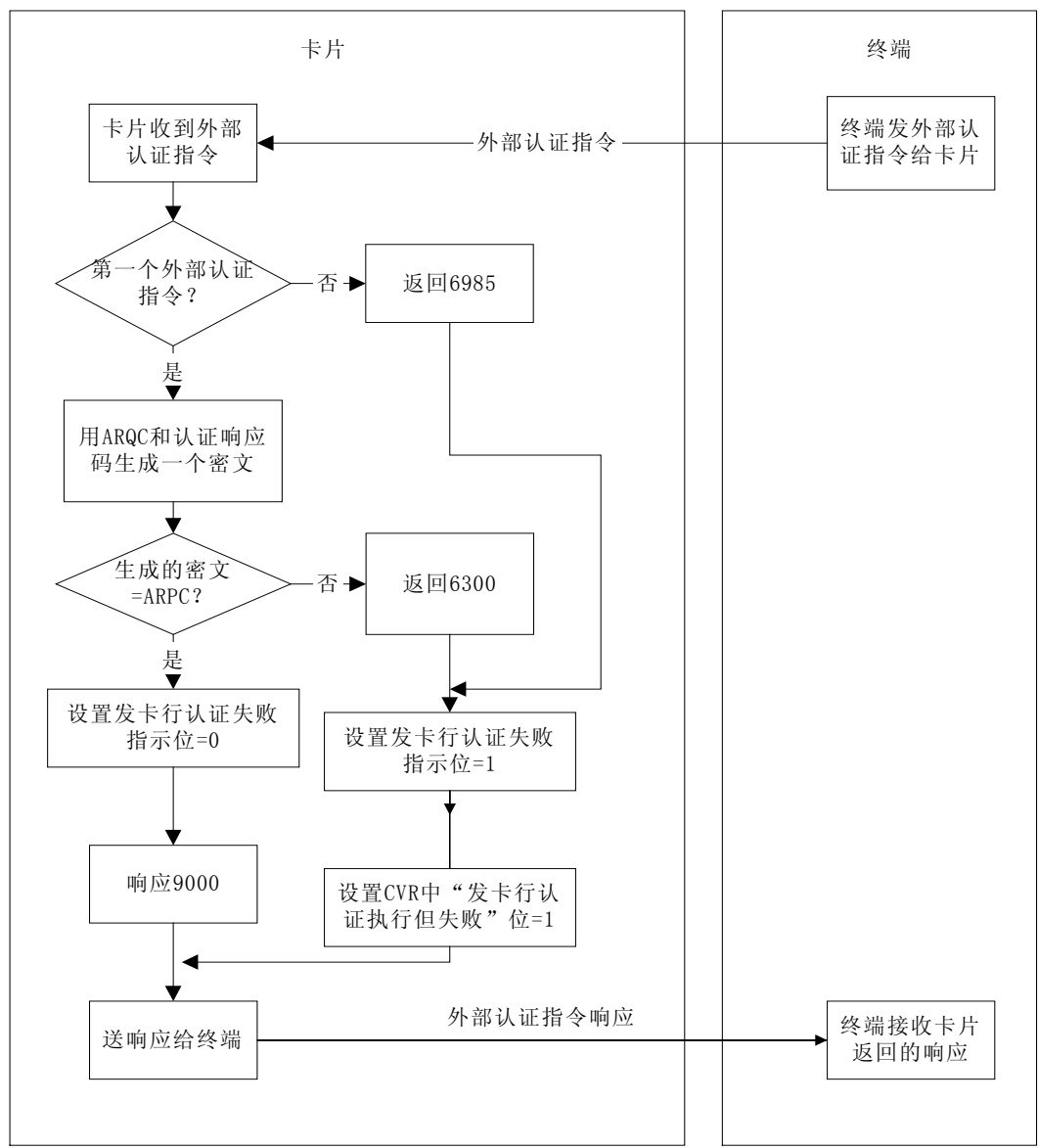
如果发卡行认证失败，卡片：

1. 设置发卡行认证失败指示位为“1”。
2. 设置 CVR 中“发卡行认证执行但失败”位为“1”
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，卡片在处理第二个 GENERATE AC 命令时，要检查发卡行认证是否执行以及是否成功。

16.5 流程图



图表 16-1：联机处理流程图

16.6 前期相关处理

应用初始化

卡片在 GET PROCESSING OPTIONS 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

第一条 GENERATE AC 命令里，卡片响应应用密文。

16.7 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。

17. 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。

17.1 卡片数据

下表列出卡片在交易结束处理过程中使用的数据。

表格 17-1：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）	PBOC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）	PBOC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	PBOC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）	PBOC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）和第二应用货币的脱机交易总金额。如果是第二应用货币，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	PBOC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	用来将第二应用货币转换成应用指定货币的汇率值。第二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	标明发卡行认证是强制还是可选。 如果发卡行认证是强制的，卡片必须受到并成功处理一个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）	PBOC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。
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。
第二应用货币代码	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	PBOC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。

下表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。

表格 17-2：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一个非对称数字签名中
发卡行应用数据	包含用来上送给发卡行的自定义应用数据，包括CVR
● 卡片认证结果（CVR）	● PBPC专用数据元。表明当前和上次交易的脱机处理结果

下表列出了在交易结束处理过程中终端使用的卡片数据

表格 17-3：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）	<p>列出在第二个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，下面列出的数据必须在CDOL2中用于交易结束处理：</p> <ul style="list-style-type: none"> ● 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） <p>CDOL中的数据元不能重复</p>

17.2 终端数据

下表列出了在交易结束处理过程中卡片使用的终端数据。

表格 17-4：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	<p>表明交易处理结果，提交给卡片。</p> <ul style="list-style-type: none"> ● 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）
终端认证结果（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

17.3 命令

生成应用密文（GENERATE APPLICATION CRYPTOGRAM (AC)) 命令

终端发第二个 GENERATE AC 命令给卡片请求第二个应用密文。

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），应用密文和发卡行自定义数据。自定义数据中包括记录处理结果的 CVR。

第二次发 GENERATE AC 命令。见附件B。

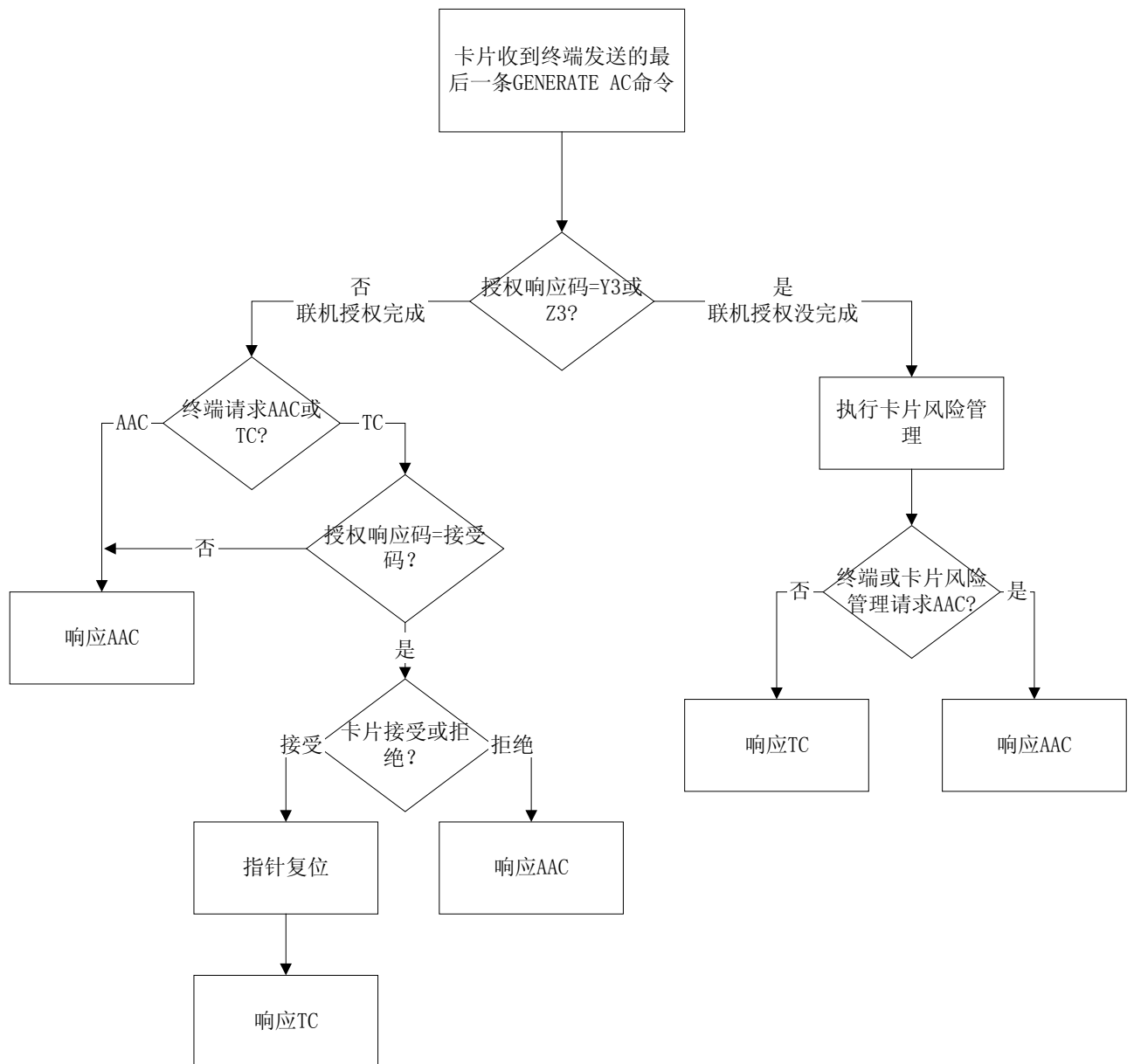
17.4 结束操作概述

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。

下图是结束处理的过程图。



图表 17-1：交易结束处理流程图

17.5 收到生成应用密文（GENERATE AC）命令

卡片在收到第二次 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17.6和请求联机，但是联机授权没有完成的交易17.7。

17.6 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,则终端提示操作员打电话请求授权,根据发卡行授权结果（批准或拒绝）请求相应的密文。如果终端不支持参考,则终端请求 AAC

-其它值表明发卡行拒绝。终端要请求交易拒绝。

- 检查第二个生成应用密文命令中的 P1 参数:

-如果 P1 表明请求 TC（接受交易）而且认证响应码表明发卡行接受或推荐,执行交易接受处理。详细描述在 17.6.2 联机授权后请求 TC（接受）中描述。

-如果 P1 表明请求 AAC（拒绝交易）或者认证响应码表明发卡行拒绝,执行交易拒绝处理。详细描述在17.6.1联机授权后请求 AAC 中描述。

17.6.1 联机授权后请求AAC（拒绝）

当第二个 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“第二个 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”
- 如果发卡行认证强制（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:（1）不支持,或者（2）可选而且没有执行,或者（3）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
- 响应第二个 GENERATE AC 命令

17.6.2 联机授权后请求TC（接受）

当第二个 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”
 - 发卡行认证强制但是没有执行，但是 ADA 中“如果发卡行认证强制但没有 ARPC 收到，交易拒绝位”为“0”

执行卡片接受交易的后续步骤，详细描述在 17.6.2.1 收到 TC 请求后卡片接受交易中。

- **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”
 - 发卡行认证强制但是没有执行，但是 ADA 中“如果发卡行认证强制但没有 ARPC 收到，交易拒绝位”为“1”

执行卡片拒绝交易的后续步骤，详细描述在 17.6.2.2 收到 TC 请求后卡片拒绝交易中。

17.6.2.1收到TC请求后卡片接受交易

当卡片接受交易，卡片：

1. 设置 CVR 中“第二个 GENERATE AC 命令返回 TC”位为“1”
2. 设置 CID 中密文类型为 TC
3. 根据发卡行认证的状态复位计数器
 - a) 如果发卡行认证（1）失败，或者（2）强制但是没有执行，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

- 如果发卡行认证强制但是没有执行：

-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（1）成功，或者（2）可选而且没有执行，或者（3）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）

- 修改上次联机 ATC 寄存器的值为当前交易 ATC。

4. 生成应用密文

5. 卡片记录交易明细，明细的内容在交易初始化阶段，通过 GET PROCESSING OPTIONS 命令传送到卡片中。关于卡片交易明细的内容在 19 章中有详细描述。

6. 响应第二个 GENERATE AC 命令

17.6.2.2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“第二个 GENERATE AC 命令返回 AAC”位为“1”

- 如果支持发卡行认证而且是强制的，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 失败指示器
 - DDA 失败指示器
 - 发卡行脚本命令计数器
 - 发卡行脚本失败指示器

卡片：

- 生成应用密文
- 响应第二个应用密文生成命令

17.7 请求联机操作，但是联机授权没有完成

当发送的第二个 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，17.7.1 卡片风险管理中描述
- 响应终端，17.7.2 无法联机上送后的卡片响应

17.7.1 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，即使在第二个 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。

17.7.1.1 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 PBOC 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

17.7.1.2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。

17.7.1.3PIN尝试限制数超过

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，卡片没有收到过校验命令，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”

17.7.1.4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”。

17.7.1.5 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二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（如果使用第二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”。

17.7.2 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，卡片响应第二个 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“17.7.2.1 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“17.7.2.2 无法联机上送后，卡片接受交易”中描述。

17.7.2.1 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：
 - 第二个 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 GENERATE AC 命令

17.7.2.2 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：
 - 第二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二应用货币代码相同，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 GET PROCESSING OPTIONS 命令传送到卡片中。关于卡片交易明细的内容在 19 章中有详细描述。
- 响应生成应用密文命令

17.8 复合动态数据认证/生成应用密文响应

下面列出的情况有一项发生，卡片执行 CDA：

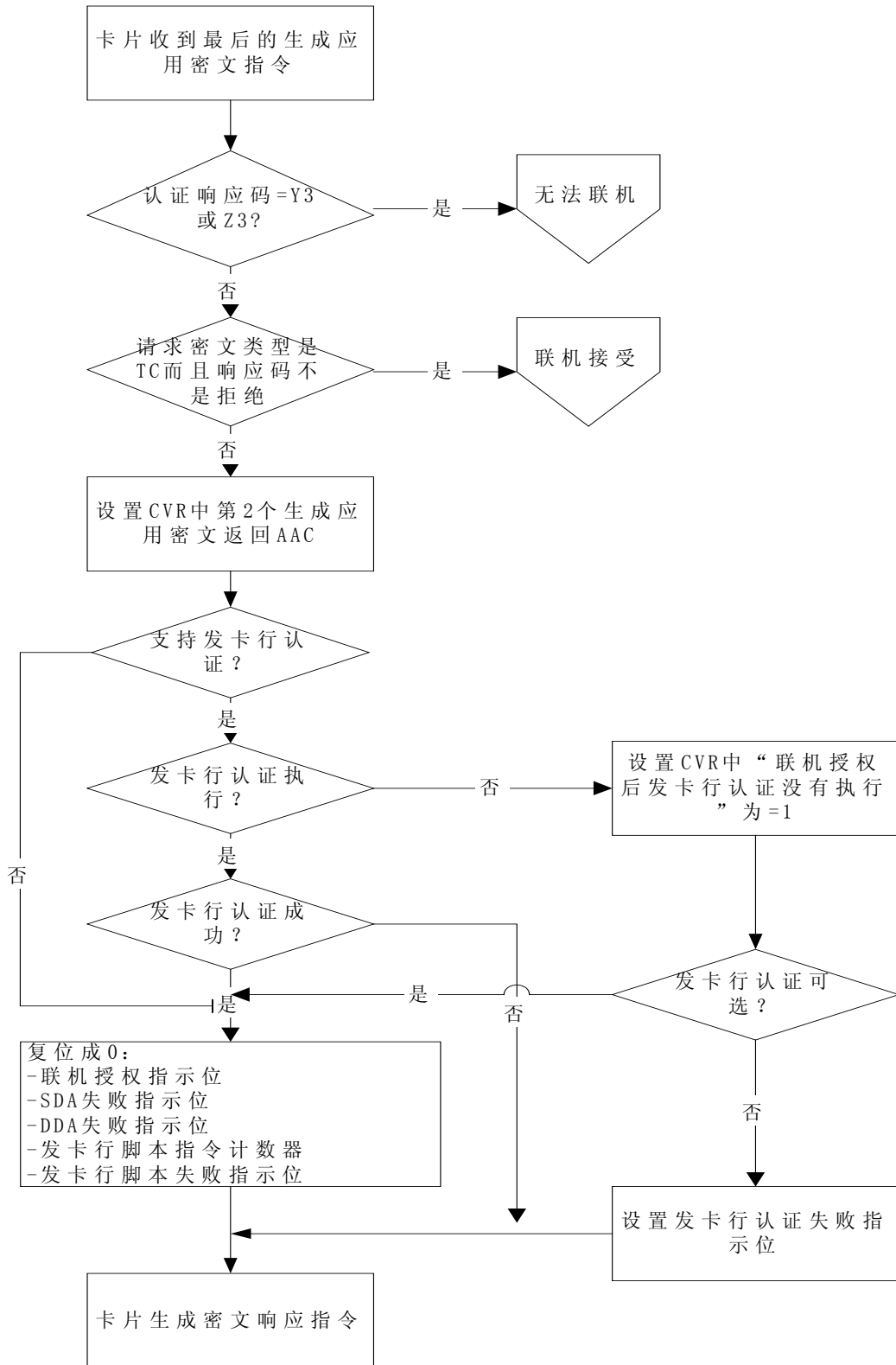
- 卡片的 CDOL2 中包括终端能力数据标签，而且终端回送的终端能力数据和卡片中的应用交互特征（AIP）中都标明支持 CDA。
- 卡片的 CDOL2 中不包括终端能力数据标签，终端发送的生成应用密文命令中的 P1 参数中 CDA 位为“1”。

卡片：

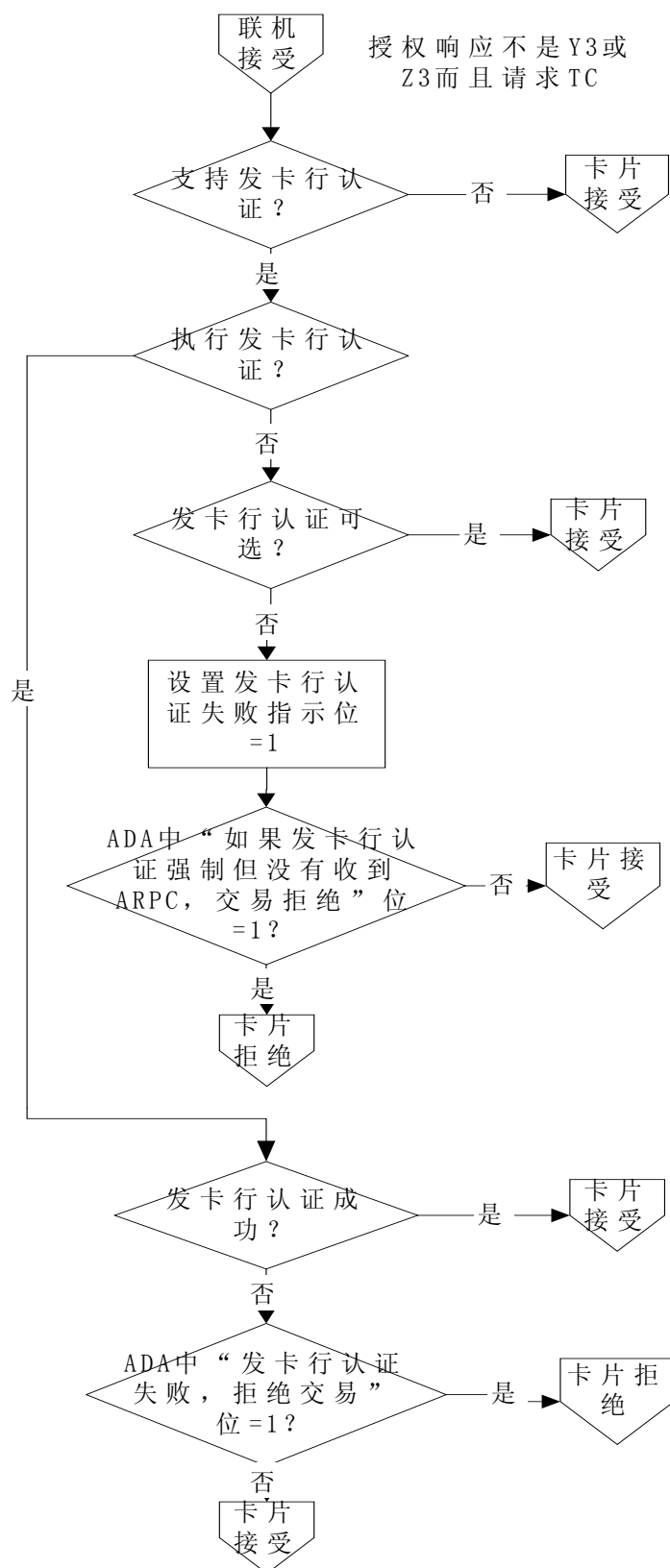
1. 按照上面的描述，生成应用密文
2. 如果卡片响应 AAC，没有特殊处理
3. 如果卡片响应 TC，卡片响应的应用密文作为签名动态应用数据用 IC 卡私钥做签名，步骤如下：
 - a) 设置 CVR 中“DDA 执行”位为“1”。此步骤在步骤 1 生成应用密文之前执行。
 - b) 使用应用密文生成一个动态密文，详见安全规范 6.3.6。归纳为下面 4 个步骤：
 - 按照安全规范中 6.3.6 中描述组织数据。数据包括 IC 卡动态数据（包括 IC 卡动态数长度，IC 卡动态数，密文信息数据和应用密文等）。
 - 用上述数据做一个哈希计算
 - 将哈希包括到签名的动态应用数据中
 - 使用 IC 卡私钥对签名的动态应用数据作签名
 - c) 响应 GENERATE AC 指令信息中包括签名的动态应用数据

17.9 流程图

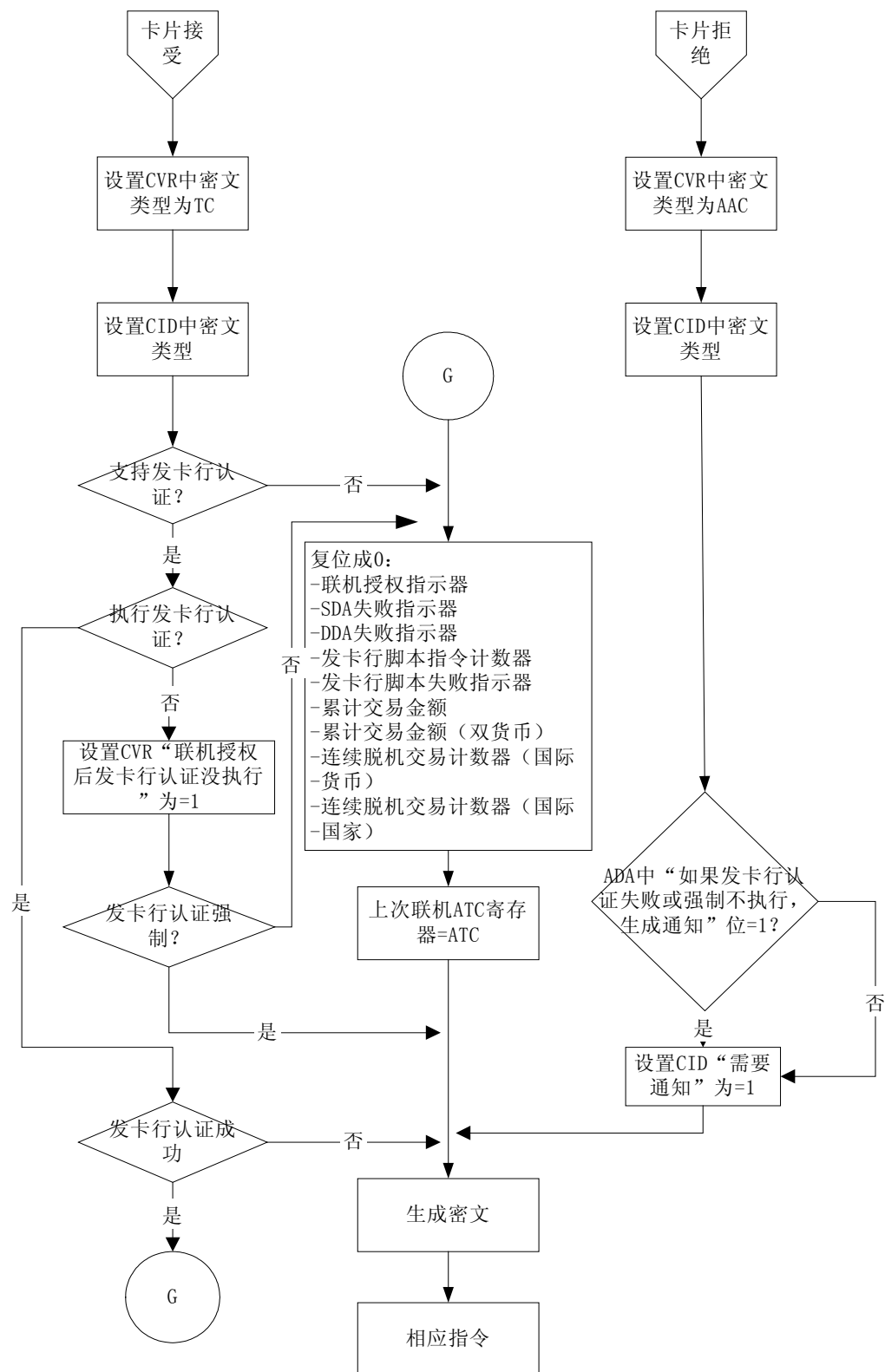
下图是卡片执行交易结束处理的流程图



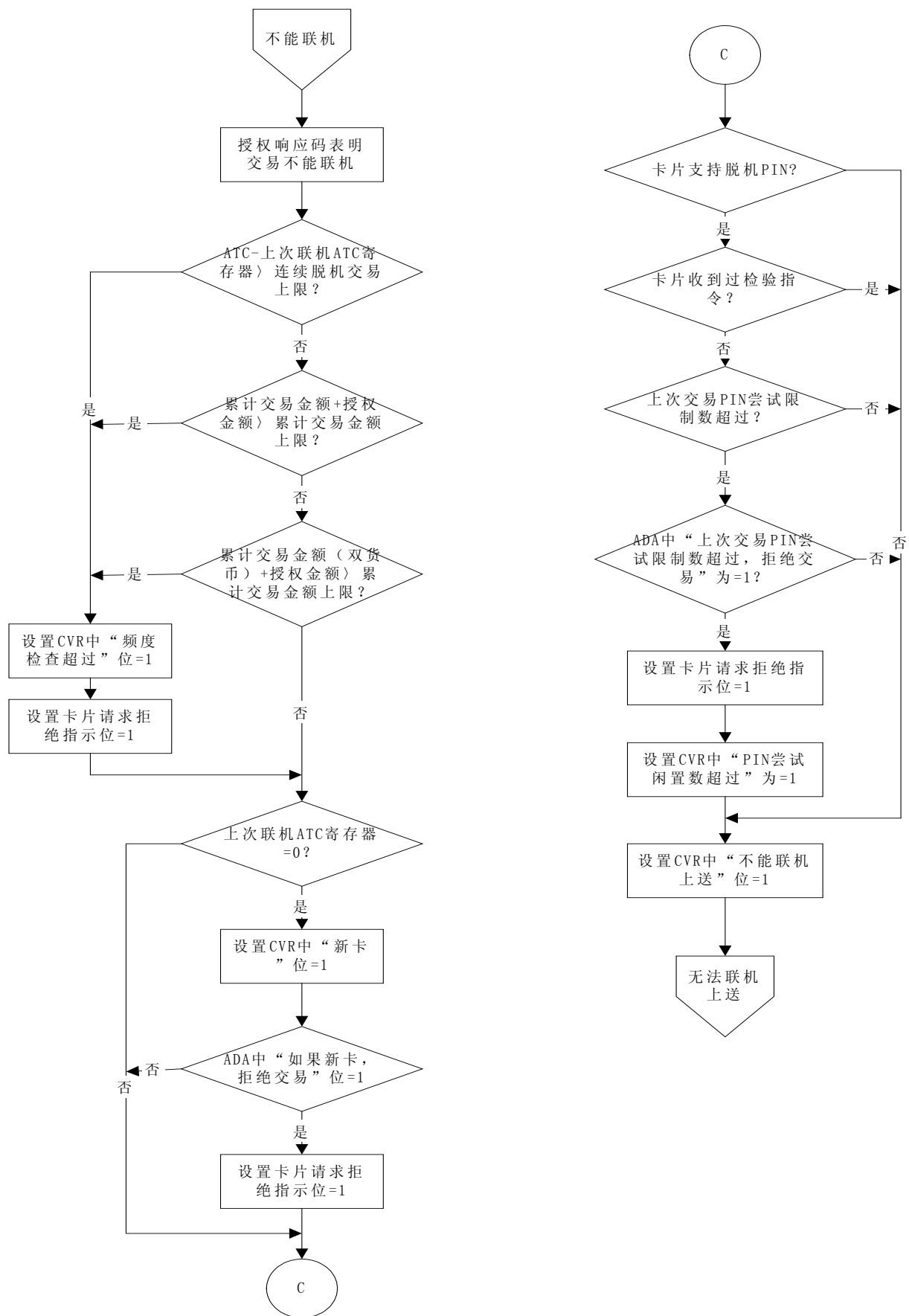
图表 17-2：交易流程图（1）



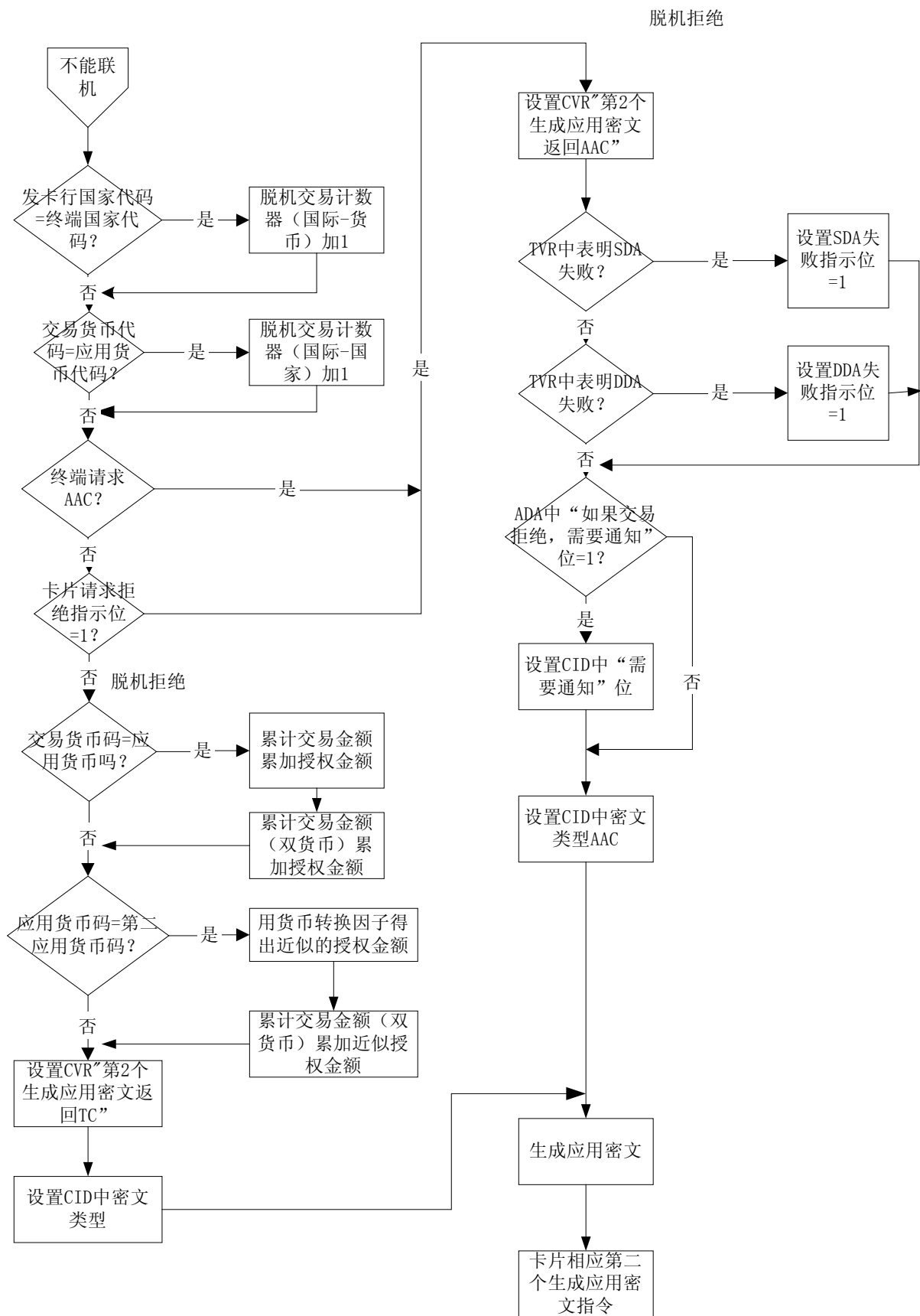
图表 17-3：交易流程图（2）



图表 17-4：交易流程图（3）



图表 17-5: 交易流程图 (4)



图表 17-6: 交易流程图 (5)

17.10 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二个 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”。

17.11 后续相关处理

卡片行为分析（后续交易）

在下次交易时，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。

18. 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。

18.1 卡片数据

下表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。

表格 18-1：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
卡片认证结果（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： <ul style="list-style-type: none">● 上次联机交易，第二次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	记录第二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	<p>在第二次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：</p> <ul style="list-style-type: none"> ● 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 <p>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。</p>

18.2 终端数据

下表列出了发卡行脚本处理过程中使用的终端数据

表格 18-2：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
终端认证结果（TVR）	<p>TVR中包括和脚本有关的两个指示位</p> <ul style="list-style-type: none"> ● 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 <p>PBOC 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</p>
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

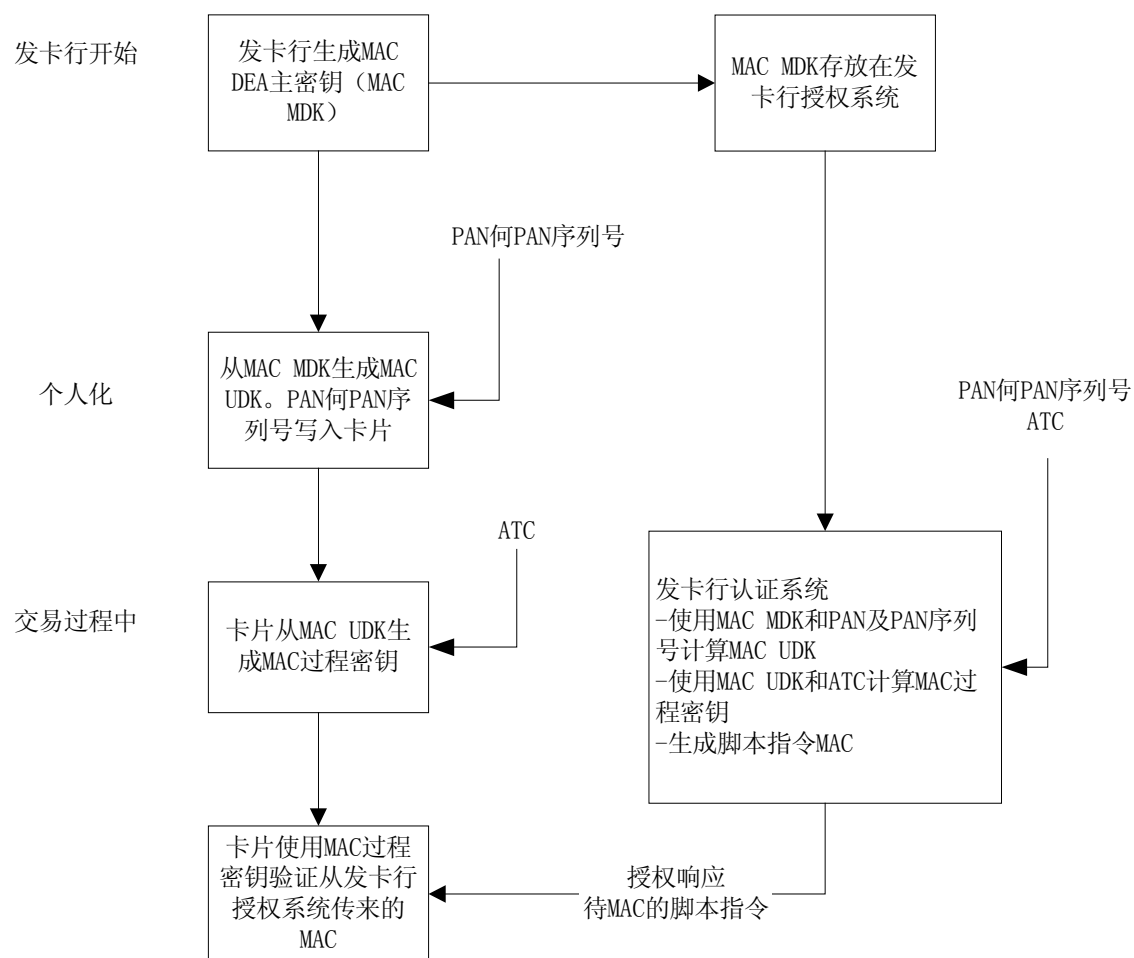
18.3 发卡行脚本操作中的密钥管理

安全报文认证（MAC）密钥

安全报文加密密钥

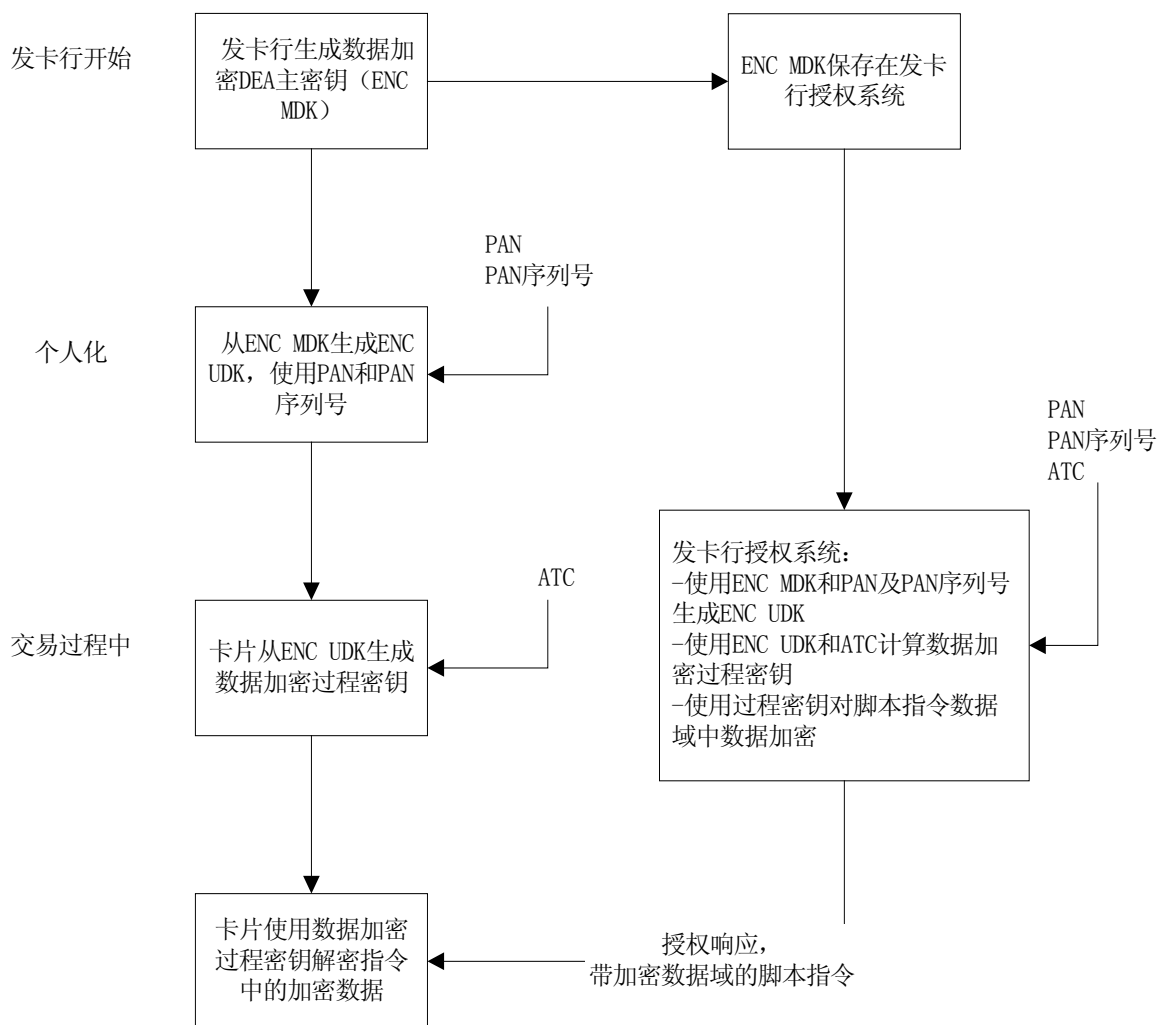
详细内容在安全规范中描述

下图是安全报文认证（MAC）密钥的生成和使用



图表 18-1：MAC密钥的生成和使用

下图是安全报文加密密钥的生成和使用



图表 18-2：安全报文加密密钥的生成和使用

18.4 认证响应数据

下表列出的是授权响应中发卡行脚本数据。

表格 18-3：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	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。

18.5 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

。命令的详细编码在附录 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，因此卡片必须对生成应用密文（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。在卡片对第一个 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必须进行的。也不需要第二个 GENERATE AC 命令。（如果由于一些原因，卡片在第二个 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 尝试次数计数器到最大值（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 尝试次数计数器复位成 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“18.6.3 卡片安全报文”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 值必须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 tag 的基本数据对象才允许使用此命令修改。

在本版本的规范中，下列数据可以使用 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

EMV 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 SF11-10 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

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

18.6 处理流程

18.6.1 授权响应报文

授权响应报文中的标签“72”表明，在第二个 GENERATEAC 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必须包全报文，参考18.6.3。

18.6.2 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，卡片不能拒绝在第二个生成应用密文命令之前送来的命令。

“18.6.4结果指示器”中描述了卡片中 PBOC 专有的指示位，记录在第二个 GENERATE AC 命令之后收到的发卡行脚本命令执行情况。

18.6.3 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。信息完整和认证发卡行可以使用 MAC，数据机密通过加密数据实现，例如 PIN 加密。

- **报文认证 (MACing)** ——报文认证 (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 生成和数据加密的详细描述在附录C。

18.6.4 结果指示器

卡片使用发卡行脚本命令计数器记录第二个 GENERATE AC 命令后收到的有安全报文的命令个数。

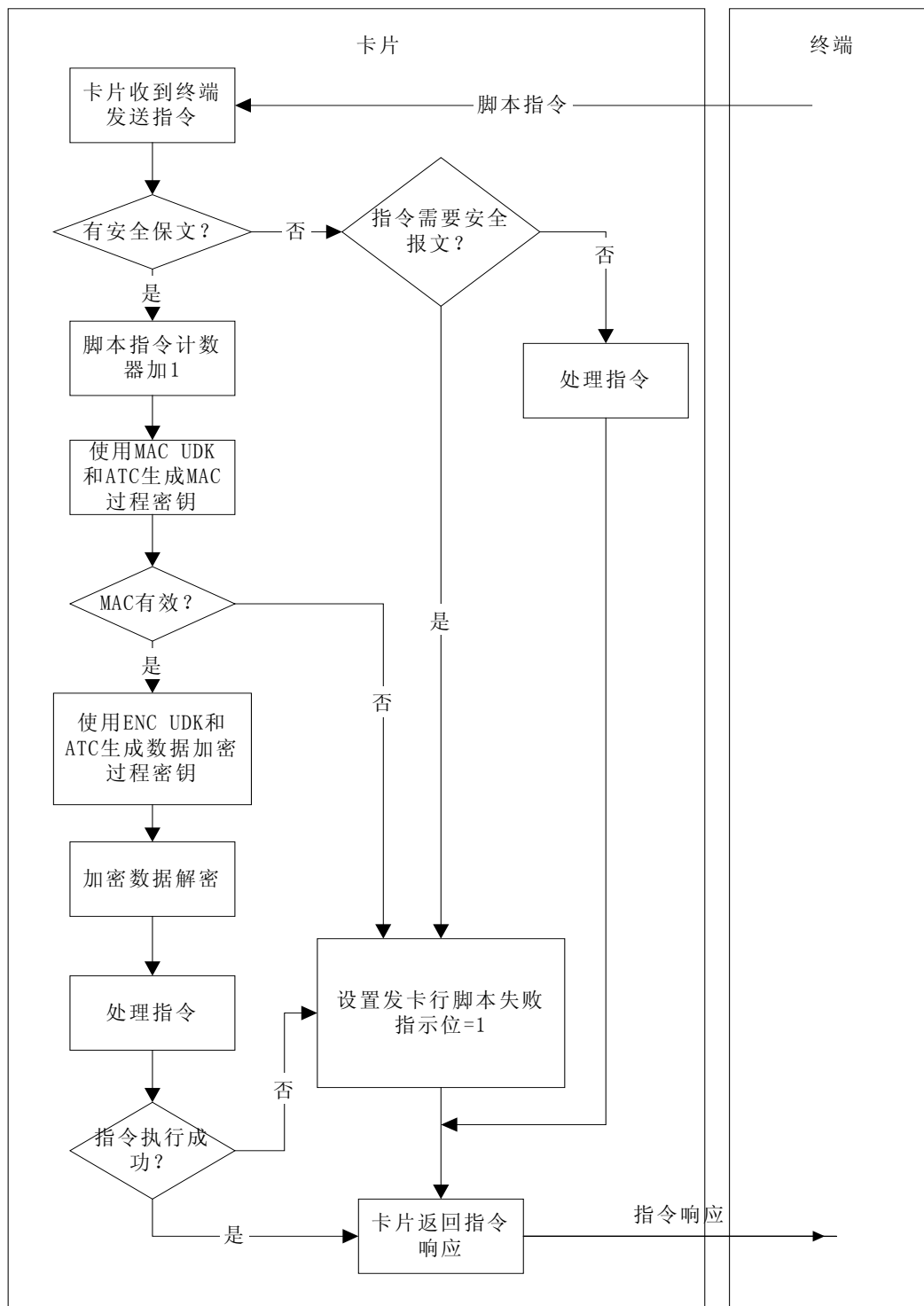
在卡片处理第二个 GENERATE AC 命令后收到的命令时，如果下面列出的错误出现一种，卡片设置发卡行脚本失败指示位为“1”：

- 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

一个不需要安全报文的命令执行失败时，不设置指示位。

18.6.5 流程图

下图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。



图表 18-3：发卡行脚本处理流程图

18.7 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。

18.8 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

19. 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。

19.1 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。记录长度为 42 字节，最小记录个数要求为 10 条记录。记录的内容在表 19-1 中列出：

表格 19-1：交易明细记录文件内容

数据	格式	长度（字节）
交易日期	YYYYMMDD	4
交易时间	HHMMSS	3
授权金额	b	4
其它金额	b	4
终端国家代码	n3	2
交易货币代码	n3	2
商户名称	ans	20
交易类型	n2	1

应用交易计数器（ATC）	b	2
--------------	---	---

交易明细记录文件的短文件标识符取值范围必须在 11-20 之间，本规范推荐值为 11，数据元标签为 9F63，长度 1 个字节，具体描述在附录 A-1 表中。当卡片在发行时，发卡行将此数据和其它应用数据一起写入卡片中存放应用数据的记录文件中，并同时建立和此短文件标识一致并且唯一的交易明细记录文件。

在读应用数据阶段，终端根据卡片返回的 AFL，读取卡片中的应用数据，其中包括 9F63 数据元。终端由此可以定位卡片中的交易明细记录文件，通过发送 READ RECORD 命令，可以读取文件中的交易明细内容。

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。

19.2 交易记录数据元

交易明细记录的内容在表 19-1 中列出，下面描述卡片获取这些数据的方法。

交易记录数据元（标签为 9F65）是一个终端数据，长度为 40 字节，内容和表 19-1 中列出的内容和顺序一样，不包括最后 2 字节 ATC。

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。

只有当上一条 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. 卡片数据元素定义

A.1 卡片和发卡行数据元描述

表格 A-A-1中列出了本规范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）
- cn（压缩数字）
- b（二进制）
- an（字母数字）
- ans（特殊字母数字）

当为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（强制）：此数据必须存在并提供给终端，终端在读应用数据过程中，如果没有读到强制数据，终端中止交易。
- R（需要）：数据必须存在，在读应用数据过程中，终端不检查。
- C（有条件）：在一定条件下必须存在。
- O（可选）：可选数据元。

表格 A-A-1：卡片和终端的数据元描述

名字（格式；标签；长度）	需求	描述	值
--------------	----	----	---

应用密文（AC） F: b 64 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: n 3 T: 9F42 L: 2	C	如果CVM中要求金额检查，需要此数据。根据ISO4217编码	
应用货币代码 F: n 3 T: 9F51 L: 2	C 如果执行频度检查	PBOC专有数据。根据ISO4217编码	
应用货币指数 F: n 1 T: 9F44 L: 1	0	指出金额数据中小数点从最右边开始第几个位置	

应用缺省行为 (ADA) F: b 16 T: 9F52 L: 2	C	如果支持发卡行认证。 PBOC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: bit 8: 1 = 如果发卡行认证失败，下次联机交易 bit 7: 1 = 如果发卡行认证执行但失败，拒绝交易 bit 6: 1 = 如果发卡行认证必备但没有收到ARPC，拒绝交易 bit 5: 1 = 如果交易拒绝，生成通知 bit 4: 1 = 如果PIN在本次交易中已锁而且交易拒绝，生成通知 bit 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 bit 2: 1 = 如果是新卡，联机交易 bit 1: 1 = 如果是新卡，当交易无法联机时拒绝交易 字节 2: bit 8: 1 = 如果PIN在本次交易中锁定，应用锁定。 Bit 7: 1 = 如果PIN在前次交易中锁定，拒绝交易 bit 6: 1 = 如果PIN在前次交易中锁定，联机交易 bit 5: 1 = 如果PIN在前次交易中锁定，当交易无法联机时拒绝交易 bit 4: 1 = 如果发卡行脚本命令在前次交易中失败，联机交易 bit 3: 1 = 如果PIN在前次交易中锁定，拒绝交易并锁应用 bits 2-1: RFU (000)
应用自定义数据 F: b 8 - 256 T: 9F05 L: 1 - 32	0	和卡片应用有关的发卡行指定数据	

应用生效日期 F: n 6 YYMMDD T: 5F25 L: 3	0	卡片中应用启用日期	
应用失效日期 F: n 6 YYMMDD T: 5F24 L: 3	M	卡片中应用的失效日期	
应用文件定位器 (AFL) F: var. T: 94 L: var. up to 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)	<p>对于每一个要读的文件, AFL包括4个字节:</p> <p>字节1:</p> <p>Bits 8-4 = SFI 短文件标识符</p> <p>Bits 3-1 = 000</p> <p>字节 2: 文件中要读的第一个记录的记录号 (不能为0)</p> <p>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)</p> <p>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)</p>
应用标识符 (AID) F: b 40-128 T: 4F L: 5-16	R	根据7816-5规定标识应用。由注册的应用提供者标识 (RID) 和专用应用标识符扩展 (PIX) 组成。	

应用交互特征 (AIP) F: b 16 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: bit 8: 1 = RFU bit 7: 1 = 支持SDA bit 6: 1 = 支持DDA bit 5: 1 = 支持持卡人认证 bit 4: 1 = 执行终端风险管理 bit 3: 1 = 支持发卡行认证 bit 2: 1 = 支持CDA bit 1: RFU (0) 字节2: RFU (“00”)
应用标签 F: an 1 - 16 T: 50 L: 1 - 16	R (EMV规定将要 成为强制数据)	和AID相关的便于记忆的 数据。 用于应用选择。ADF的FCI 中和ADF目录入口的强制 数据	
应用首选名称 F: an 1 - 16 T: 9F12 L: 1 - 16	0	和AID相关的便于记忆的 数据。如果终端支持在发 卡行编码表索引数据中 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. up to cn 19 T: 5A L: var. up to 10	M	持卡人有效账号	
应用主账号序列号 F: n 2 T: 5F34 L: 1	0	用来表示卡片中使用同 一个账号的不同应用	

应用优先指示器 F: b 8 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	bit 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 bit7-5: RFU (000) bit4-1: 0000: 不指定优先级 xxxx: 应用现实和选择的顺序，从1-15。1的优先级最高
应用模板 F: b T: 61 L: var. up to 252	C 如果有PSE	根据ISO7816-5，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	0	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: bit 8: 1 = 国内现金交易有效 bit 7: 1 = 国际现金交易有效 bit 6: 1 = 国内商品有效 bit 5: 1 = 国际商品有效 bit 4: 1 = 国内服务有效 bit 3: 1 = 国际服务有效 bit 2: 1 = ATM有效 bit 1: 1 = 除ATM外的终端有效 字节2: bit 8: 1 = 允许国内返现 bit 7: 1 = 允许国际返现 bits 6-1: RFU (000000) PBOC限制: 字节1中, bit4, 6值相同; bit3, 5值相同
应用版本号 F: b 16 T: 9F08 L: 2	M	支付系统给应用分配的版本号	
授权响应码 F: an 2 T: 8A L: 2	来自发卡行或终端	标明了交易结果	按照ISO8583: 1987标准。发卡行生成。 下面的代码是终端生成: 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)

卡片风险管理数据 对象列表1 (CDOL1) F: b T: 8C L: var. up to 252	M	列出第一个生成应用密 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. up to 252	M	列出第二个生成应用密 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: b 32 T: - L: 4.	M	PBOC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: bits 8-7: 00 = 第二个GENERATE AC返回AAC 01 = 第二个GENERATE AC返回TC 10 = 不请求第二个GENERATE AC 11 = RFU bits 6-5: 00 = 第一个GENERATE AC返回AAC 01 = 第一个GENERATE AC返回TC 10 = 第一个GENERATE AC返回ARQC 11 = 不能返回11 bit 4: 1 = 发卡行认证执行但失败 bit 3: 1 = 脱机PIN执行 bit 2: 1 = 脱机PIN认证失败 bit 1: 1 = 不能联机

卡片验证结果 (CVR) (继续)			字节 3: bit 8: 1 = 上次联机交易没有完成 bit 7: 1 = PIN锁定 bit 6: 1 = 超过频率检查 bit 5: 1 = 新卡 bit 4: 1 = 上次联机交易发卡行认证失败 bit 3: 1 = 联机授权后, 发卡行认证没有执行 bit 2: 1 = 由于PIN锁卡片锁定应用 bit 1: 1 = 上次交易SDA失败交易拒绝 字节4: bits 8-5: 上次交易第二个GENERATE AC命令后收到的带有安全报文的发卡行脚本命令 bit 4: 1 = 上次交易发卡行脚本处理失败指针 bit 3: 1 = 上次交易DDA失败交易拒绝 bit 2: 1 = DDA执行 bit 1: RFU (0) 在应用初始化时, 字节2-4置零
持卡人姓名 F: ans 2 - 26 T: 5F20 L: 2 - 26	R	持卡人姓名, 符合ISO7813	
持卡人姓名扩展 F: ans 27 - 45 T: 9F0B L: 1-19	0	如果持卡人姓名大于26字节, 多出部分放在此数据元中。符合ISO7813	

持卡人证件号 F: an 40 T: 9F61 L: 1-40	0	持卡人证件号。	
持卡人证件类型 F: cn 1 T: 9F62 L: 1	0	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

<p>持卡人验证方法 (CVM) 列表</p> <p>F: b</p> <p>T: 8E</p> <p>L: var. up to 252</p>	R	<p>按照优先顺序列出卡片应用支持的所有持卡人验证方法</p> <p>注意: 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。</p>	<p>字节1 - 4: 金额X (二进制)</p> <p>字节5 - 8: 金额Y (二进制)</p> <p>字节9 (CVM Code):</p> <p>bit 8: 0 = 只有符合此规范的取值 (如果不为1, 说明有自定义的值)</p> <p>bit 7:</p> <p>1 = 如果此CVM失败, 应用后续的</p> <p>0 = 如果此CVM失败, 则持卡人验证失败</p> <p>bits 6 - 1 (CVM Type):</p> <p>000000 = CVM失败处理</p> <p>000001 = 卡片执行明文PIN核对</p> <p>000010 = 联机加密PIN验证</p> <p>000011 = 卡片执行明文PIN核对+签名 (纸上)</p> <p>000100 = EMV保留</p> <p>000101 = EMV保留</p> <p>011110 = 签名 (纸上)</p> <p>011111 = 不需CVM</p> <p>000110 - 011101 = 保留给加入的支付系统</p> <p>100000 - 101111 = 保留给各自独立的支付系统</p> <p>110000 - 111110 = 保留给发卡行</p> <p>111111 = RFU</p>
---	---	---	--

<p>持卡人验证方法 (CVM) 列表</p> <p>(继续)</p>			<p>PBOC定义:</p> <p>100000 = 持卡人证件出示</p> <p>字节10 (CVM Condition Code):</p> <p>00 = 总是</p> <p>01 = 如果是现金或返现 (包括准现金)</p> <p>02 = 如果不是现金或返现 (包括准现金)</p> <p>03 = 如果终端支持这个CVM</p> <p>04 = RFU</p> <p>05 = RFU</p> <p>06 = 如果交易货币等于应用货币码而且小于X值</p> <p>07 = 如果交易货币等于应用货币码而且大于X值</p> <p>08 = 如果交易货币等于应用货币码而且小于Y值</p> <p>09 = 如果交易货币等于应用货币码而且大于Y值</p> <p>0A - 7F: RFU</p> <p>80 - FF: RFU 保留给各个支付系统</p> <p>下一个CVM用另外两个CVM码和CVM条件字节表示</p>
<p>CA公钥索引 (PKI)</p> <p>F: b 8</p> <p>T: 8F</p> <p>L: 1</p>	<p>C</p> <p>如果支持SDA或DDA。</p>	<p>在SDA或DDA过程中, 和RID一起使用, 用来标识CA公钥</p>	

连续脱机交易计数器（国际-货币） F: b 8 T: - L: 1	C 如果执行国际-货币频度检查	PBOC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: b 8 T: 9F53 L: 1	C 如果执行国际-货币频度检查	PBOC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） F: b 8 T: - L: 1	C 如果执行国际-国家频度检查	PBOC专有数据元。记录自从上次联机后，不在发卡行所在国家内进行的脱机交易次数	初始值为0，每接受一次国际-国家交易脱机后加1
连续脱机交易限制数（国际-国家） F: b 8 T: 9F72 L: 1	C 如果执行国际-国家频度检查	PBOC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: b 8 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。	bits 8-7: 00 = AAC 01 = TC 10 = ARQC 11 = AAR (本版本不支持) bit 6-5: RFU (00) bit 4: 1 = 需要通知 bits 3-1 (相应/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: b 8 T: - L: 1	R	PBOC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	PBOC指定密文版本号11 (‘0B’)
累计脱机交易金额 F: n 12 T: - L: 6	C 如果执行累计金额频度检查	PBOC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: n 12 T: 9F54 L: 6	C 如果执行累计金额频度检查	PBOC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: n 12 T: - L: 6	C 如果执行累计金 额（双货币）频 度检查	PBOC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二 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 二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: n 12 T: 9F75 L: 6	C 如果执行累计金 额（双货币）频 度检查	PBOC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	PBOC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	用来将第二应用货币转 换成指定应用货币的10 进制数。	字节1 bit8-5: 小数点位置。从右边开始移动的位数 bit4-1: 转换因子的第一个数字 字节2-4: 剩下的6个数字
数据认证码 F: b 16 T: 9F45 L: 2	0	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 64 T: - L: 16	C 如果执行修改PIN	PBOC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	根据ISO7816-4规定的，DF的名字	
分散密钥索引（DKI） F: b 8 T: - L: 1	0	PBOC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（ 定义 ） ？ ？ ？ 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. up to 252	0	根据ISO7816-5，目录中发卡行自定义部分	

动态数据认证数据对象列表 (DDOL) F: b T: 9F49 L: var. up to 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	PBOC专有数据。标明当上次交易拒绝时DDA是否失败。	bit 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. up to 222	0	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	根据ISO7816-4，标识FCI模板中，专用于EMV4.0的数据对象。	
文件控制信息 (FCI) 模板 F: var. T: 6F L: var. up to 252	R	根据ISO7816-4，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。	
ICC私钥 F: b T: - L: NIC	C 如果支持DDA	IC卡公钥对中的私钥部分。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 T: 9F47 L: 1 or 3	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。	
IC卡公钥证书 F: b T: 9F46 L: NI	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: NIC - NI + 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: b 40 T: 9F0D L: 5	R 将变成强制	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: b 40 T: 9F0E L: 5	R 将变成强制	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: b 40 T: 9F0F L: 5	R 将变成强制	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。

<p>发卡行应用数据</p> <p>F: b</p> <p>T: 9F10</p> <p>L: var. up to 32</p>	R	<p>在一个联机交易中,要传送到发卡行的专有应用数据。</p> <p>第1字节是PBOC自定义数据长度。</p> <p>格式内容:</p> <p>长度(07)(1字节)</p> <p>分散密钥索引(1字节)</p> <p>密文版本号(1字节)</p> <p>卡片验证结果(CVR)(4字节)</p> <p>算法标识(1字节)</p> <p>如果由发卡行自定义数据。在上述数据后跟一个发卡行自定义数据长度字节和1-15字节的发卡行自定义数据。</p>	
<p>发卡行认证数据</p> <p>F: b 64 - 128</p> <p>T: 91</p> <p>L: 8 - 16</p>	0	<p>用于发卡行认证的数据,从发卡行传来由终端送入卡片。</p> <p>本版本中,发卡行认证数据包括两部分:</p> <p>ARPC(8字节)</p> <p>授权响应码(2字节)</p>	

<p>发卡行认证失败指示位</p> <p>F: b 1</p> <p>T: -</p> <p>L: -</p>	<p>C</p> <p>如果支持发卡行认证</p>	<p>PBOC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：</p> <p>发卡行认证执行但失败</p> <p>发卡行认证没有执行但是强制</p>	<p>bit 1: 1 = 上次联机交易发卡行验证失败</p>
<p>发卡行认证指示位</p> <p>F: b 8</p> <p>T: 9F56</p> <p>L: - 1</p>	<p>C</p> <p>如果支持发卡行认证</p>	<p>PBOC专有数据。标明当支持发卡行认证时，是强制还是可选。</p>	<p>bit 8:</p> <p>1 = 发卡行认证强制</p> <p>0 = 发卡行认证可选</p> <p>bits 7-1: RFU (0000000)</p>
<p>发卡行代码表索引</p> <p>F: n 2</p> <p>T: 9F11</p> <p>L: 1</p>	<p>C</p> <p>如果有应用首选名称</p>	<p>根据ISO8859，显示应用首选名称的代码表。</p>	<p>01 = ISO 8859, Part 1</p> <p>02 = ISO 8859, Part 2</p> <p>03 = ISO 8859, Part 3</p> <p>04 = ISO 8859, Part 4</p> <p>05 = ISO 8859, Part 5</p> <p>06 = ISO 8859, Part 6</p> <p>07 = ISO 8859, Part 7</p> <p>08 = ISO 8859, Part 8</p> <p>09 = ISO 8859, Part 9</p> <p>10 = ISO 8859, Part 10</p>

发卡行国家代码 F: n 3 T: 5F28 L: 2	C 如果有应用用途控制	根据ISO3166指出发卡行的国家。	
发卡行国家代码 F: n 3 T: 9F57 L: 2	C 如果支持卡片频度检查 如果支持地域检查	PBOC专有数据。根据ISO3166指出发卡行的国家。	
发卡行公钥证书 F: b T: 90 L: NCA	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 F: b T: 9F32 L: 1 or 3	C 如果支持SDA, DDA	发卡行公钥指数, 用来验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: NI-NCA+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 up to 261	0	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: b 4 T: - L: -	C 如果支持发卡行脚本	PBOC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。	bits 4-1: 第二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: b 1 T: - L: -	C 如果支持发卡行脚本	PBOC专有数据。当上次交易发卡行脚本处理失败时设置。	bit 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，发送到卡片的包括发卡行自定义数据。	
发卡行URL F: ans T: 5F50 L: var.	0	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.	0	PBOC定义的。存放发卡行服务器在互联网上的位置	
首选语言 F: an 2 T: 5F2D L: 2 - 8	0	顺序存放的1-4种语言。根据ISO639编码	
上次联机应用交易计数器 (ATC) 寄存器 F: b 16 T: 9F13 L: 2	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

连续脱机交易下限 F: b 8 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: b 8 T: 9F58 L: 1	C 如果执行卡片频 度检查	PBOC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。	
安全报文认证(MAC) 密钥 F: b 64 T: - L: 16	C 如果支持发卡行 脚本使用安全报 文	PBOC专有数据。双长度安 全报文认证(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: b 1 T: - L: -	C 如果卡片风险管 理检查允许得出 拒绝结论	PBOC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: b 1 T: - L: -	C 如果卡片支持发 卡行授权或发卡 行脚本处理	PBOC专有数据。如果卡片 请求ARQC但是终端不能 完成时设置。	bit 1: 1 = 本次获上次交易中, 需要联机授 权但是没有实现

卡片请求联机指示位 F: b 1 T: - L: -	R	PBOC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尝试次数计数器 F: b 8 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）
PIN尝试限制数 F: b 8 T: - L: 1	C 如果支持脱机PIN	PBOC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）	
专用应用标识符扩展（PIX） F: b T: - L: 0 - 11	R	根据ISO7815-5规定的，AID的组成部分之一。	PBOC PIX值有：

脱机PIN F: b T: - L: 8	C 如果支持脱机PIN	PBOC专有数据。在卡片个人化时由发卡行写入卡片。	
注册的应用提供者标识符（RID） F: b T: - L: 5	R	根据ISO7816-5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）	
第二应用货币 F: n 3 T: 9F76 L: 2	C 如果支持双货币频度检查。	第二种货币，要转换成应用指定货币。根据ISO4217编码	
服务码 F: n 3 T: 5F30 L: 2	0	根据ISO/IEC7813标准，和在磁条1和2中定义的数据一致。	

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: EMV专用 11 - 20: 支付系统专用 21 - 30: 发卡行专用
签名的动态应用数据 F: b T: 9F4B L: NIC	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: NI	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: b 1 T: - L: -	C 如果支持SDA	PBOC专有数据。标明当上次交易拒绝时SDA是否失败	bit 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	根据ISO/IEC7813, 磁条1 中的自定义数据	
磁条2等效数据 F: B T: 57 L: var. up to 19 n, var. up to 19 1 n4 n3 0 or n 5 n, var. hex.	M	根据ISO/IEC7813, 磁条2 的数据。不包括起始位、 结束位和LRC (校验码), 包括: 应用主账号 (PAN) 分隔符 (“D”) 期满日期 (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 列表 (TDOL) F: b T: 97 L: var. up to 252	C 如果需要预先哈希。	终端使用列出的数据对象 (标签和长度)生成TC 哈希值。	

交易明细记录文件 短文件标识符 F: b T: 9F63 L: 1	0	发卡行在发卡时写入卡片，由终端读出可以定位交易明细记录文件。	bit 8-6: 000 bit 5-1: 01011-10100 取值范围：11-20（16进制0b-14）
应用密文（AC）密钥 F: b 64 T: - L: 16	M	PBOC专有数据。双长度应用密文密钥的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: b 8 T: 9F23 L: 1	C 如果支持终端频率检查	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	PBOC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	
PBOC自定义数据 F: b 56 T: - L: var 7 to 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。	

A. 2 卡片和发卡行数据元需求

表格 A-2中是卡片和发卡行数据元的需求。

A. 2. 1 标签 (Tag)

标签列是数据元的标签 (Tag)。

A. 2. 2 需求

强制/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

表格 A-2: 数据需求

名称	标签	强制/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				
应用货币码	9F42	C	29		N	读记录				和9F51匹配
应用货币码	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			
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	将来是强制
应用首选名称	9F12	0			N	读记录 选择			ADF	
应用PAN	5A	M			N	读记录				
应用PAN序列号	5F34	0			N	读记录				
应用优先指示位	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	0			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	0			N	读记录				
持卡人证件号	9F61	0			N	读记录				

持卡人证件类型	9F62	0			N	读记录				
持卡人验证方式（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		设置数据	取数据（特殊设备）				
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	0	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	0				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		0			N	N				9F10的一部分
目录定义文件（DDF）名称	5D	C	11		N	读记录			DDF	
目录自定义模板	73	0			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	0			N	选择				
FCI专有模板	A5	R			N	选择				
FCI模板	6F	R			N	选择				
地域指示器	9F55	C	12		N	取数据（特殊设 备）	静态			
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 ● 公钥证书 ● 公钥模数 ● 公钥余数										
		C	31		N	N		秘密		
	9F47	C	31		N	读记录				
	9F46	C	31		N	读记录				
	9F48	C	15		N	读记录				
发卡行行为代码-缺省	9F0D	R*			N	读记录				将来强制
发卡行行为代码-拒绝	9F0E	R*			N	读记录				将来强制
发卡行行为代码-联机	9F0F	R*			N	读记录				将来强制
发卡行应用数据	9F10	R			N	生成应用密文				
发卡行认证数据	91	0	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, 12		N	取数据（特殊设备）	静态			和5F28匹配

发卡行公钥数据										
● 发卡行公钥证书	90	C	30或31		N	读记录				
● 发卡行公钥模数	9F32	C	30或31		N	读记录				
● 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	0				选择				
发卡行URL2	9F5A	0				选择				
首选语言	5F2D	0				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获24				
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		
处理选项数据对象列表 (PDOL)	9F38	C	22, 12			选择				
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				
第二应用货币代码	9F76	C	3		N	取数据（特殊设备）	静态			
服务码	5F30	0			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				必须是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, 24	备份	修改记录	读记录				
连续脱机交易上限	9F59	C	8	备份	设置数据	取数据（特殊设备）				
交易明细记录文件短文件标识符	9F63	C	34		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下表

表格 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
12	如果应用初始化时支持地域限制检查
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
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

B. 命令规范—描述卡片支持的命令

此附录中描述了各个章节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）
- 取处理选项（GET PROCESSING OPTIONS）
- 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）
- 校验（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节 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。报文验证码（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（APPLICATION BLOCK）命令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 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 GENERATE AC 命令，一个无效的应用应该返回 AAC 代替 AC 作为应答。

B.2.2 命令报文

APPLICATION BLOCK 命令报文根据下表编码：

表格 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安全规范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（APPLICATION UNBLOCK）命令APDU

B. 3. 1 定义和范围

APPLICATION UNBLOCK 命令是一个发行行脚本命令，用来恢复当前被选择的应用。
当 APPLICATION UNBLOCK 命令成功之行后，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 命令报文通过下表编码。

表格 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（CARD BLOCK）命令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 命令报文根据下表编码。

表格 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（EXTERNAL AUTHENTICATE）命令APDU

B. 5. 1 定义和范围

EXTERNAL AUTHENTICATE 命令要求 IC 卡中的应用认证一个密码。

IC 卡的应答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

EXTERNAL AUTHENTICATE 命令报文根据下表编码：

表格 B-4：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 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 EMV 规范的规定，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。

在本版本中，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（GENERATE AC）命令APDU

B. 6. 1 定义和范围

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。这个密文是一个由本规范定义的应用密码(AC)，下表列出了密文类型。

表格 B-5：生成应用的密文类型

类型	意义
应用鉴定密文（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

GENERATE AC 命令报文根据下表编码：

表格 B-6：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’

GENERATE AC 命令中的引用控制参数根据下表编码

表格 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 密码生成
		1						请求复合动 态数据认证/ 应用密码生 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。数据域由如下表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)。

表格 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
应用交易序号（ATC）	必备
应用密码（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，但是必须包括密码信息数据、应用交易序号和由 IC 卡计算出的密码(可以是应用密码或专有密码)。对于响应报文中可能包含的专有数据对象的应用和解释,不在本规范的范围之内。

如果响应报文是如本规范第 10 章，第 15 章及第 17 章定义的签名数据，对 CDA 的应答，则采用格式 2。该应答数据单元格式参见安全规范第 6.3.6.。

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，在生成应用密码命令的响应报文中包括的密码数据按照下表的方式编码:

表格 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							AAR
		x	x					支付系统密码
				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（GET DATA）命令APDU

B. 7. 1 定义和范围

B.7.1.1 用GET DATA命令得到的数据

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

- 特殊设备

- 下表列出的静态数据可以在发卡行控制的特殊设备上通过 GET DATA 命令访问。普通终端不能用取数据命令获得。

表格 B-10：使用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
第二应用货币代码

- 金融交易

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。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')或密码重试计数器(标签为'9F17')。

B. 7. 2 命令报文

GET DATA 命令报文根据下表编码：

表格 B-11：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 取处理选项（GET PROCESSING OPTIONS）命令APDU

B. 8. 1 定义和范围

GET PROCESSING OPTIONS 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

GET PROCESSING OPTIONS 命令报文根据下表编码：

表格 B-12：GET PROCESSING OPTIONS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 卡提供的处理选择数据对象列表(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。数据域由如下表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)。

表格 B-13：GET PROCESSING OPTIONS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（INTERNAL AUTHENTICATE）命令APDU

B. 9. 1 定义和范围

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

INTERNAL AUTHENTICATE 命令根据下表编码：

表格 B-14：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 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。它是根据本规范第二册中定义的动态数据认证数据对象列表(DDOL)规则来编码的。

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安全规范中的规则定义。

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（PIN CHANGE/UNBLOCK）命令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 尝试计数器的值将复位到 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 命令报文根据下表编码。

表格 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：

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。
2. 生成过程密钥 Ks
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) 生成第二个 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

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

5. 将数据块 D3 和 D4 执行异或得到 D。

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：

- 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。
- 2. 生成过程密钥 Ks
- 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) 生成第二个 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

- 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（PUT DATA）命令APDU

B. 11. 1 定义和范围

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PUT DATA命令修改的数据

下表列出的数据可以使用此命令修改。

表格 B-16：使用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

PUT DATA 命令报文根据下表编码。

表格 B-17：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。
下表列出了命令可能返回的警告信息：

表格 B-18：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

下表列出了命令可能返回的错误信息

表格 B-19：PUT DATA命令的错误响应码

SW1	B. 11. 6SW2	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（READ RECORD）命令APDU

B. 12. 1 定义和范围

READ RECORD 命令从一个线性文件中读一条文件记录。
从 IC 卡返回的应答中将包含这条被读出的记录。

B. 12. 2 命令报文

READ RECORD 命令报文根据下表编码：

表格 B-19：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-20
Lc	不存在
数据域	不存在
Le	‘00’

下表定义了命令报文的引用控制参数。

表格 B-20：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 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。它按照下表编码。

表格 B-21：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，不在本规范的范围描述范围内。

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（SELECT）命令APDU

B. 13. 1 定义和范围

SELECT 命令通过文件名或 AID 来选择 IC 卡中的 PSE、DDF 或 ADF。应用选择在本规范的第7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 卡返回的应答报文包含回送 FCI。

B. 13. 2 命令报文

SELECT 命令报文编码见下表：

表格 B-22：SELECT命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数(见表B-23)
P2	选择选项(见表B-24)
Lc	‘05’ - ‘10’
Data	文件名
Le	‘00’

下表定义了 SELECT 命令报文的引用控制参数：

表格 B-23：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	

下表定义了 SELECT 命令报文的选项 P2：

表格 B-24：SELECT命令的可选参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
						0	0	第一个有或仅有一个
						1	0	下一个

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 应答报文数据域

应答报文中数据域应包括所选择的 PSE、DDF 或 ADF 的 FCI。表格 B-25、表格 B-26和表格 B-27 定义了本规范所应用的标识。对于本规范所不规定的 FCI 中回送的附加标签应该被忽略。

下表定义了成功选择 PSE 后回送的 FCI:

表格 B-25: 选择PSE的应答报文 (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’	语言选择	O
	‘9F11’	发卡行代码表索引	O
	‘BF0C’	发卡行自定义数据(FCI)	O
	‘XXXX’ (第3册规定的 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

下表定义了成功选择 DDF 后回送的 FCI:

表格 B-26: 选择DDF的应答报文 (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’ (第3册规定的标 识符)	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

下表定义了成功选择 ADF 后回送的 FCI:

表格 B-27：选择ADF的应答报文（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		O
	‘87’	应用优先指示符		O
	‘9F38’	PDOL		O
	‘5F2D’	首选语言		O
	‘9F11’	发卡行代码表索引		O
	‘9F12’	应用优先名称		O
	‘BF0C’	发卡行自定义数据(FCI)		O
		‘XXXX’ (第3册规定的标识符)	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

注意：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 应答报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡是否支持使用部分 DF 名进行 DF 文件选择不作强制规定。但是，如果 IC 卡支持部分名称选择，那么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（UPDATE RECORD）命令APDU

B. 14. 1 定义和范围

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

UPDATE RECORD 命令报文编码见下表：

表格 B-28：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-29
Lc	记录数据加MAC的长度
Data	记录数据和MAC
Le	不存在

下表定义了命令报文的引用控制参数。

表格 B-29：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。

下表列出了命令可能返回的警告信息：

表格 B-30：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

下表列出了命令可能返回的错误信息

表格 B-31: 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 校验（VERIFY）命令APDU

B. 15.1 定义和范围

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。如本规范第12章所述，当从 CVM 列表中选择持卡人验证方式（CVM）是脱机 PIN 时，使用 VERIFY 命令。

B. 15.2 命令报文

VERIFY 命令报文根据下表编码：

表格 B-32: 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

下表定义了参考数据(P2)的意义.

表格 B-33: 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	IOS/IEC 7816-4定义 ¹
1	0	0	0	0	0	0	0	明文PIN, 格式如下
1	0	0	0	0	x	x	x	本规范保留
1	0	0	0	1	0	0	0	EMV保留
1	0	0	0	1	0	x	x	本规范保留
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 VERIFY 命令的处理在本规范第 8 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0010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。

¹ 本规范未采用P2= ‘00’。

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’。

C. 安全报文

本部分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认证通过 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

在本规范中的描述的安全报文个是符合 ISO7816-4 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 报文完整性和认证 (MACing)

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

PBOC 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生成过程密钥”。MAC 过程密钥由卡片中的安全报文认证 (MAC) 密钥 (MAC UDK) 生成。

C.2.4 MAC计算

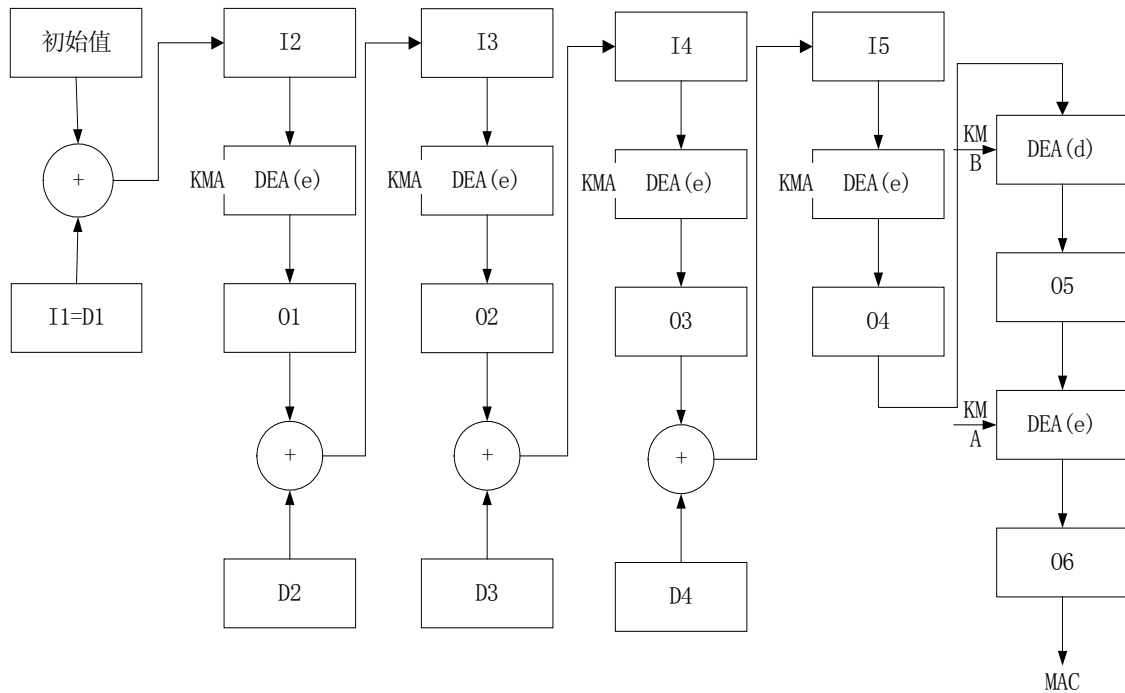
命令中需要加密的数据加密以后再计算 MAC。MAC 使用对称密钥算法计算的,步骤如下:

1. 初始值为 8 字节全零。(此步骤可省略)

2. 下列数据按顺序排列得到一个数据块 D:
 - CLA, INS, P1, P2, 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)
 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。
 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。
 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 过程密钥生成”。
- 图表 C-1 是使用 MAC 过程密钥 A 和 B 生成 MAC 的流程图。
6. MAC 的计算结果为 8 字节, 从最左边的字节开始取 4 字节。

图表 C-1：使用双长度DEA密钥计算MAC的算法



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

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生成过程密钥”。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 L_d （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。

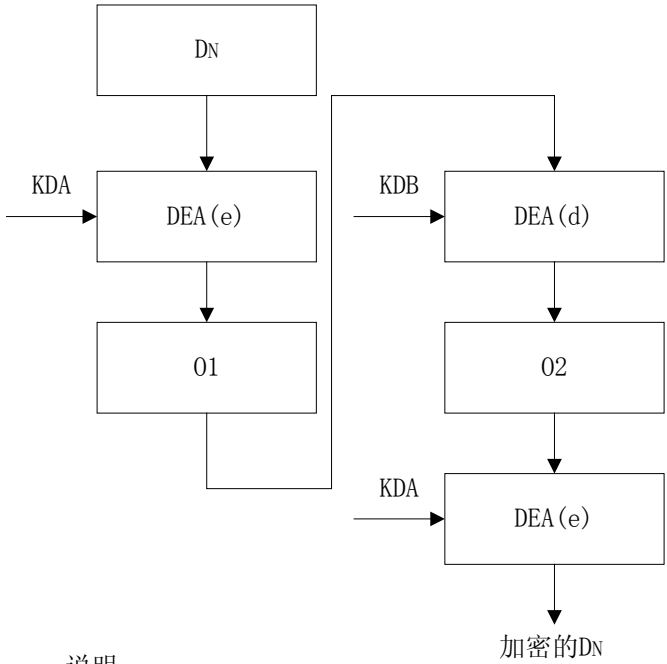
C. 3. 3数据加密计算

数据加密在 MAC 计算之前进行。步骤如下：

- 1. 设 Ld 为明文数据的长度。
- 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。
- 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。
- 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 “C.4生成过程密钥”。

下图是使用数据加密过程密钥 A 和 B 对数据块加密的流程。

图表 C-2：用双长度DEA密钥进行数据加密



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

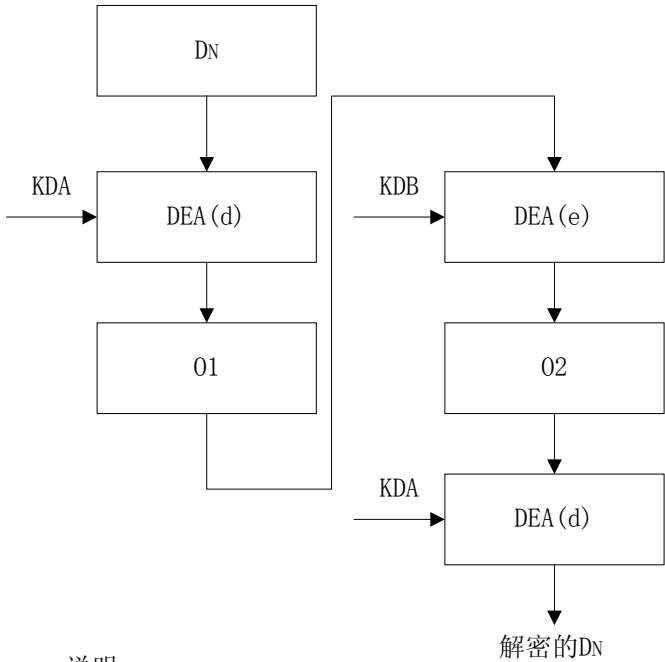
- 5. 结束后，所有的加密后的数据块顺序连接（加密的 D1，加密的 D2，加密的 D3...）就是命令数据域中的最终数据。

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：

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。
 下图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。

图表 C-3：使用双长度DEA密钥进行数据解密



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

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。
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：

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）。
2. 将两字节的 ATC 右对齐，前面补 6 个字节 00...（详细内容参考安全规范）
3. 将两字节的 ATC 取反后右对齐，前面补 6 个字节 00...（详细内容参考安全规范）

C.5 命令中的安全报文

D. 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 数据源

发卡行要决定生成应用密钥的数据源。

下表列出了生成应用密文的数据顺序。

表格 D-1: TC/AAC/ARQC数据元顺序

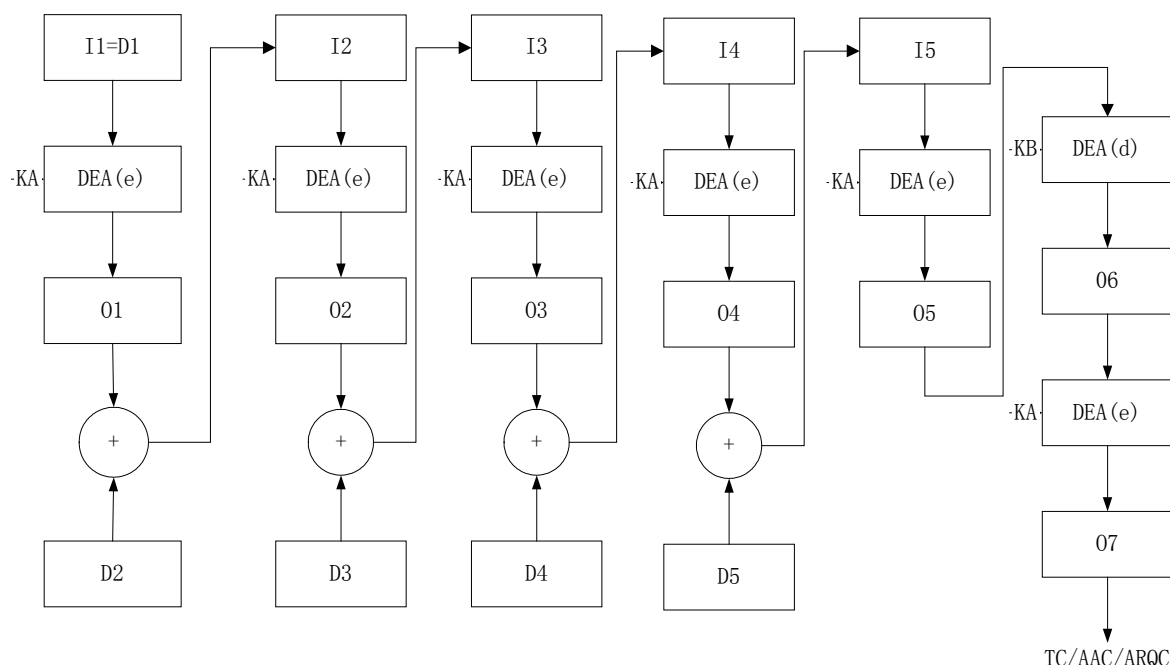
数据元	来自终端的数据	在交易证书（TC） 哈希中的顺序	卡片内数据
授权金额	✓	✓	
其它金额	✓	✓	
终端国家代码	✓	✓	
终端验证结果	✓	✓	
交易货币代码	✓	✓	
交易日期	✓	✓	
交易类型	✓	✓	
不可预知数	✓	✓	
应用交互特征（AIP）			✓
应用交易计数器（ATC）			✓
卡片验证结果（CVR）			✓

D.2 生成TC，AAC和ARQC

密文生成的步骤如下：

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。
2. 根据卡片风向管理的结果，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
3. 将上述数据块分成 8 字节一组：D1，D2，D3...
 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。
 5. 使用过程密钥用对称密钥算法生成应用密文。
 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。下图是使用过程密钥 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

图表 D-1：TC/AAC/ARQC的生成算法。

D. 3 生成授权响应密文ARPC

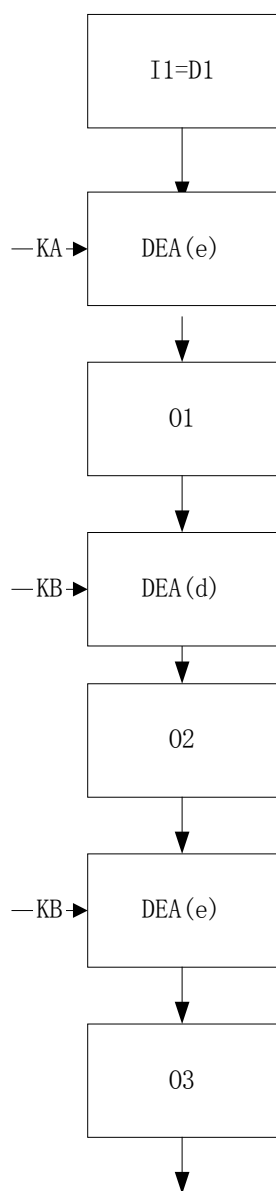
卡片在收到外部认证命令时，生成一个 ARPC 和命令中传送进来的 ARPC 进行比较。生成 ARPC 的步骤如下：

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。

2. 异或的结果是一个 8 字节的数据块 D1。
3. 使用过程密要用对称密钥算法计算 ARPC。下图是 ARPC 的生成方法。



说明：

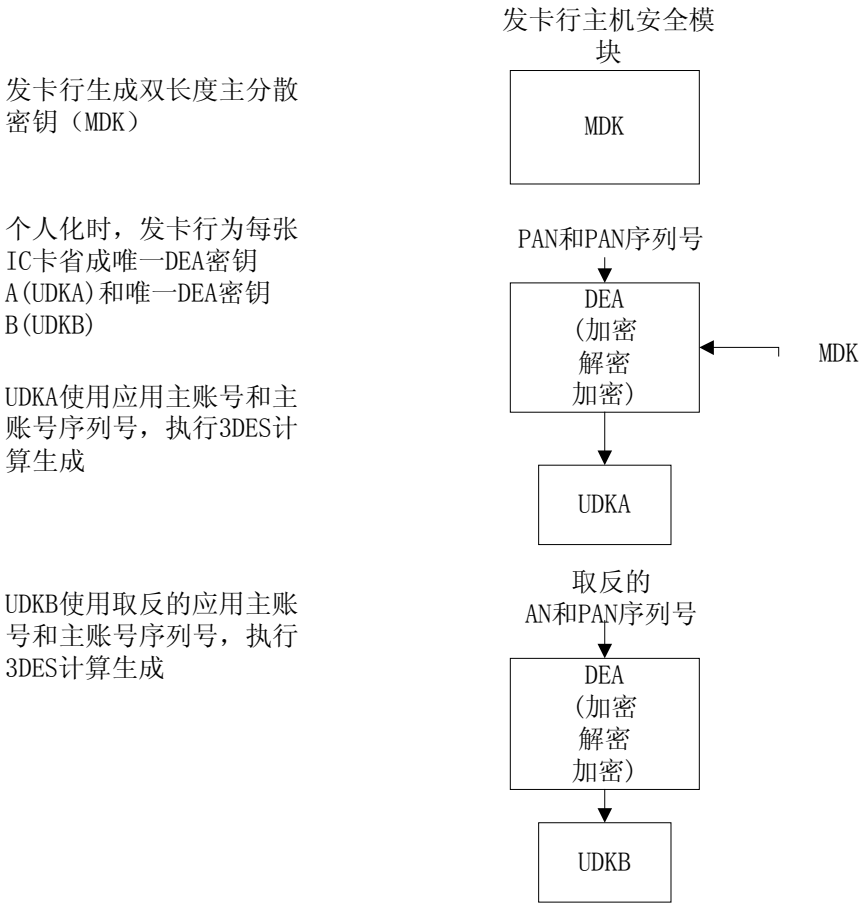
I = 输入	D = 数据块
DEA(e) = 数据加密算法（加密模式）	KA = 密钥A
DEA(d) = 数据加密算法（解密模式）	KB = 密钥B
0 = 输出	

图表 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。

下图是唯一 DEA 密钥 A 和 B 的生成流程。



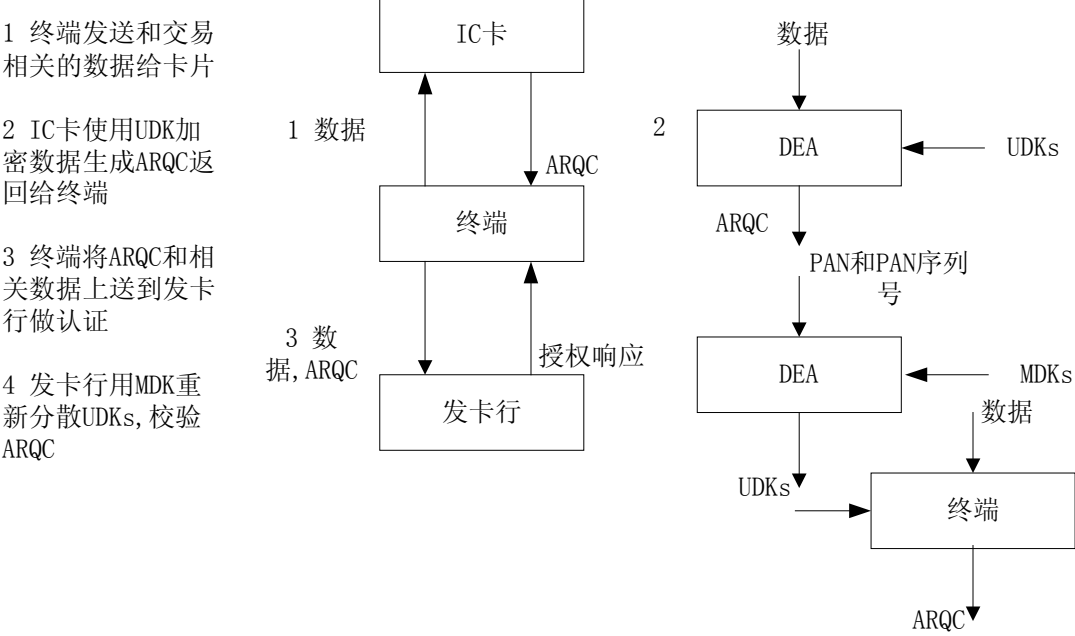
图表 D-3：密钥分散

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 D2 取反，用来生成分散的唯一 DEA 密钥 B。

下图是卡片使用唯一 DEA 密钥 A 和 B (UDKA 和 UDKB) 进行卡片认证的过程。



图表 D-4：使用UDK执行卡片认证

如图所示，主机安全模块要得到分散的 UDK 验证 ARQC

E. 支持的密文版本

PBOC 定义的密文版本为 01（0x01）。
下表列出的是生成 TC/AAC 和 ARQC 的数据元和顺序。

表格 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。

F. 算法标识

发卡行自定义数据元中由一个 PBOC 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。取值情况为：

表格 F-1：算法标识

算法	值（16进制）
3DES	01
SSF33	02