Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 042.1--2011

替代 028--2008

中国银联金融集成电路IC卡辅助规范
第一部分 借记/贷记应用个人化模板

Unionpay Integrated Circuit Card Auxiliary Specifications

Part 1 Personalization Template Based on Debit/Credit Application

2011-11-20 发布　　2012-01-01 实施

中 国 银 联 股 份 有 限 公 司 发布

目　　录

前　言

本标准在编写过程中主要依据《中国金融集成电路（IC）卡规范》（JR/T0025－2005）借记贷记应用，在编写中也广泛征求了IC卡厂商、系统集成商和部分商业银行的意见。

本标准给出了符合《中国金融集成电路（IC）卡》借记贷记应用的银联IC卡个人化参数模板，供发卡银行个人化卡片时参考使用。

本标准由中国银联股份有限公司提出。

本标准由中国银联股份有限公司技术管理部组织制定。

本标准的主要起草单位：中国银联产品创新部。

本标准的主要起草人：徐晋耀、李春欢、回春野、柏建宁、顾伯华、张卫东、张栋。

中国银联金融集成电路 IC 卡辅助规范

第一部分 借记/贷记应用个人化模板

1 范围

本规范根据《中国金融集成电路（IC）卡规范》借记贷记应用，以EMV为基础，给出卡片个人化参数模板，以确保卡片个人化后能与终端之间协同工作。

本规范的目的是：

—— 帮助成员机构为卡片参数选择正确的值；

—— 提供一套能作为成员机构 IC 卡个人化指导的参考模板；

—— 确保成员机构的产品符合 EMV 和 PBOC 规范。

2 规范性引用文件

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

JR/T 0025.3-2005 中国金融集成电路（IC）卡规范第3部分：与借记/贷记应用无关的IC卡与终端接口需求规范

JR/T 0025.4-2005 中国金融集成电路（IC）卡规范第4部分：借记/贷记应用规范

JR/T 0025.5-2005 中国金融集成电路（IC）卡规范第5部分：借记/贷记卡片规范

JR/T 0025.6-2005 中国金融集成电路（IC）卡规范第6部分：借记/贷记终端规范

JR/T 0025.7-2005 中国金融集成电路（IC）卡规范第7部分：借记/贷记安全规范

JR/T 0025.10-2005 中国金融集成电路（IC）卡规范第10部分：借记/贷记应用个人化指南规范

EMV 2000 Integrated Circuit Card Specifications for Payment Systems, Books 1 to 4

3 符号和缩略语

3.1 符号

3.1.1 十六进制符号

以十六进制表示的数据都被附上了单引号， 例如十进制的数27509，转换成十六进制是 ‘6B75’。

3.1.2 二进制符号

以二进制形式表示的数值后面总是加上小写字母‘b’，例如十六进制的‘08’用二进制表示就是00001000b。

3.1.3 压缩数字符号

一个压缩数字所含有的数字个数如果是奇数，后面就要至少补上一个十六进制‘F’。例如，十进制数456表示成压缩数据类型是‘456F’，存放在两个字节空间里。

3.1.4 数据符号

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）
——var.（可变）
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

3.2 缩略语

以下缩略语和符号表示适用于本规范：

缩写	描述
AAC	应用认证密文(Application Authentication Cryptogram)
ADA	应用缺省行为(Application Default Action)
ADF	应用数据文件(Application Definition File)
AFL	应用文件定位器(Application File Locator)
AID	应用标识符(Application Identifier)
ARQC	授权请求密文(Authorization Request Cryptogram)
ATC	应用交易序号(Application Transaction Counter)
AUC	应用用途控制(Application Usage Control)
CAM	卡片认证方法(Card Authentication Method)
CVM	持卡人验证方法(Cardholder Verification Method)
CVN	密文版本号(Cryptogram Version Number)
CDOL	卡片风险管理数据对象列表(Card Risk Management Data Object List)
CPLC	卡片生产生命周期历史文件标识(Card Production Life Cycle History File Identifiers)
CTAL	累积交易限额(Cumulative Transaction Amount Limit)
DDA	动态数据认证(Dynamic Data Authentication)
DDOL	动态数据认证数据对象列表(Dynamic Data Authentication Data Object List)
EMV	(Europay, MasterCard, Visa)
hex	十六进制(Hexadecimal)
IAC	发卡行行为代码(Issuer Action Code)
ICC	集成电路卡(Integrated Circuit Card)
IPK	发卡行公钥(Issuer Public Key)
LCOL	连续脱机交易下限(Lower Consecutive Offline Limit)
MDK	主密钥(Master Derivation Key)
PAN	主账户(Primary Account Number)
PBOC	中国金融集成电路（IC）卡规范
PIN	个人密码(Personal Identification Number)
PIX	专用标识符扩展(Proprietary Identifier Extension)
PSE	支付系统环境(Payment System Environment)
RID	注册应用提供商标识(Registered Application Provider Identifier)
RFU	保留(Reserve for Future Use)
SDA	静态数据认证(Static Data Authentication)

缩写	描述
SAD	签名的静态应用数据(Signed Static Application Data)
TC	交易证书(Transaction Certificate)
UCOL	连续脱机交易上限(Upper Consecutive Offline Limit)
UDK	子密钥(Unique PBOC card level key generated by MDK)

4 PBOC 借记贷记应用个人化模板

为了帮助成员在卡片发行时候，能够方便地设置卡片参数，中国银联编写了用于说明技术设置的这些模板作为指南。

本文档中描述的模板为成员银行普遍使用，在《中国银联金融集成电路IC卡应用规范个人化指南》中，有关于个人化详细的描述。

本文档定义了为每个模板所必须的最小数据集，每个数据对象都需要一个数据值。这个数值是模板基于最优推荐提供或必须由发卡行指定的。

—— 模板 1 借记卡 SDA, 联机 PIN,发卡行认证, 和授权控制
—— 模板 2 借记卡 DDA, 联机 PIN,发卡行认证, 和授权控制
—— 模板 3 贷记卡 DDA, 联机 PIN,发卡行认证, 和授权控制
—— 模板 4 贷记卡 DDA, 签名，发卡行认证, 和授权控制
—— 模板 5 贷记卡 DDA, 联机 PIN,和授权控制
—— 模板 6 贷记卡 CDA, 脱机 PIN,和授权控制
—— 模板 7 准贷记卡 DDA, 联机 PIN,发卡行认证,和授权控制

—— 模板 11 纯电子现金卡 DDA, 无需 CVM
—— 模板 12 借记卡+电子现金+非接触式 IC 卡支付
—— 模板 13 贷记卡+电子现金+非接触式 IC 卡支付（1）
—— 模板 14 贷记卡+电子现金+非接触式 IC 卡支付（2）
—— 模板 15 准贷记卡+电子现金+非接触式 IC 卡支付

这里所描述的每一个模板都有一列数据标签、数据对象和标签值，它们提供了规定的功能。然而，有一些数据对象的使用受到了所使用的卡片类型或者发卡行特殊要求的限制。这些数据对象没有在模板中列出。

有关特殊卡片数据对象的一些例子如下：

—— AFL

应用文件定位器(AFL)，说明终端作交易处理要读出的卡片数据存放的文件位置和记录范围。

—— PSE vs. ADF

如果卡片和终端都支持具有可选性特征的目录选择方法，那么就要访问支付系统环境(PSE) 文件。这个文件列出了卡片所支持的所有支付应用。

应用定义文件(ADF) 包含了 交易处理过程中使用的数据对象，这是卡片和终端都具有的强制性特征。

有关具体的发卡行数据对象的例子如下：

卡片在生产周期中的文件标志符 (Tag 9F7F) – 为卡片在整个使用周期中提供核查功能。

应用首选名称 (Tag 9F12) – 和AID相关的便于记忆的名称。如果终端支持发卡行代码表索引中指定的字符集，那么就会显示出该名称。

发卡行代码表索引（Tag 9F11）－显示应用首选名称的代码表。

在模板中描述了下面这些数据对象，由于它们取决于发卡行的选择和要求，因而数值有所不同。

持卡人验证方法（Tag 8E）－按照优先顺序列出卡片应用支持的所有持卡人验证方法。

发卡行行为代码（Tags 9F0D, 9F0E, 9F0F） - 9F0D(缺省)： 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；9F0E(拒绝)：指定交易不进行联机直接拒绝的条件；9F0F(联机)：指定交易联机上送的条件。

应用用途控制（Tag 9F07）－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。

频度检查参数－ 这些变量的实际值应由银行确认设置。这些数据包括 ：

- 连续脱机交易限制数(Tag 9F53)
- 累计脱机交易金额限制数(Tag 9F54)
- 连续脱机交易下限(Tag 9F58)
- 连续脱机交易上限(Tag 9F59)
- 累计脱机交易金额上限(Tag 9F5C)
- 连续脱机交易限制数(Tag 9F72)
- 累计脱机交易金额限制数(Tag 9F75)

卡片附加处理（Tag 9F68）－标明发卡行所发行的支持非接触IC卡支付卡片对交易流程的选择和支持情况。

卡片交易属性（Tag 9F6C）－标明发卡行所发行的支持非接触IC卡支付卡片在脱机数据认证失败的情况下交易流程选择，以及卡片所支持的持卡人认证方法。

4.1 模板 1：借记卡—SDA，联机 PIN,发卡行认证，和授权控制

4.1.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征 (AIP)	b	'82'	2	**5C00** *详见 4.1.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	'87'	1	**01** *详见 4.1.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器 (ATC)	b	'9F36'	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	'9F08'	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移植途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.1.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
静态数据认证（SDA)失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				
发卡行认证指示位	b	‘9F56’	1	**00 或 80 推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（’80’)。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
日志格式	b	'9F4F'	Var.	**9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602** *详见 4.1.5*	列出日志记录中数据对象的标签和长度	✔			
连续脱机交易限制数（国际-货币）	b	'9F53'	1	**发卡行模板 推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	'9F72'	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器（国际-货币）	b	–	1	**初始设置为 0**	国际脱机交易计数器。 当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
累计脱机交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	'9F54'	6	**发卡行模板 推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限(LCOL)	b	‘9F58’	1	**发卡行模板 推荐值 0**	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。		✔		
连续脱机交易上限(UCOL)	b	‘9F59’	1	**发卡行模板 推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		
卡片风险管理数据对象列表 1 (CDOL1)	b	‘8C’	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见 4.1.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片风险管理数据对象列表 2 (CDOL2)	b	‘8D’	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见 4.1.7*	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），包括：发卡行响应码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔
密文信息数据	b	‘9F27’	1	初始设置为 0	表明卡片返回的密文类型	✔			
发卡行行为代码 (IAC)-拒绝	b	‘9F0E’	5	**00 10 00 00 00** *详见 4.1.8*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码 (IAC)-联机	b	‘9F0F’	5	**D0 68 9C F8 00** *详见 4.1.8*	指定交易联机上送的条件。	✔			✔
发卡行行为代码 (IAC)-缺省	b	‘9F0D’	5	**D0 60 9C A8 00** *详见 4.1.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07_ _ 01 03 00 00 00 01** *详见 4.1.9*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		
发卡行国家代码	n	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
首选语言	an	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’	2	**发卡行模板**	发卡行的国内货币。		✔		✔
应用标识符(AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.1.10*	注册应用提供商标识（RID）和专用标识符扩展：**A0 00 00 03 33 01 01 01** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样) ，01 01 01 表明 PBOC 借记应用。				
应用标签	ans	‘50’	1-16	**发卡行模板** *详见 4.1.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.1.11*	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。 用于提供更灵活的卡片服务控制（类似服务代码）。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔
磁条 2 等效数据	var.	‘57’	最大 19	磁条数据文件提供	等效磁条 2 数据（格式不一致） 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期（5F24）一致			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
持卡人验证方法(CVM)列表	b	‘8E’	12	**0000 0000 0000 0000 4203 0103 1F00** *详见 4.1.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
CA 公钥索引(PKI)	b	‘8F’	1	发卡行模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✔		✔
发卡行公钥(IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证		✔		✔
发卡行公钥余数(如果需要)	b	‘92’	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分		✔		✔
发卡行公钥指数	b	‘9F32’	1 to N_I/4	发卡行模板	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		✔		✔
签名的静态应用数据（SAD）	b	‘93’	var.	发卡行模板	用发卡行私钥签名的应用数据，在 SDA 过程中由终端验证			✔	✔
应用缺省行为(ADA)	b	‘9F52’	2	**C000** *详见 4.1.13*	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	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥 (UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥 (ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥 (MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥 (MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.1.2 应用交互特征(AIP)设置

‘5C00’ 十六进制

字节	位	值	含义
1	8	0	RFU

字节	位	值	含义
1	7	1	支持SDA
1	6	0	不支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.1.3 应用优先指示器

‘01’ 十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.1.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位	1 bit	0	-
发卡行认证失败指示位	1 bit	0	-
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit		-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits		-
连续脱机交易下限	1 字节	发卡行模板 =0	‘9F58’
连续脱机交易上限	1 字节	>=连续脱机交易下限，=0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’

卡片内部数据	保留	初始值	Tag
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板=0	‘9F54’
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数（国内），=0	‘9F5C’

注： 为了支持SDA,发卡行认证和授权控制处理,带阴影的指示位应当在个人化时设置。

4.1.5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’十六进制(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.1.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’十六进制*(数据对象的标签和长度)*

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6

数据对象名称	Tag(标签)	长度
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.1.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.1.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

’00 10 00 00 00’ 十六进制（发卡行行为代码-拒绝）

‘D0 68 9C F8 00’ 十六进制（发卡行行为代码-联机）

‘D0 60 9C A8 00’ 十六进制（发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	0	0
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**0**	1	1
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	**0**	1	1
要求输入PIN，密码键盘存在，但未输入PIN	**0**	1	1
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.1.9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07 (十六进制)	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	01 (十六进制)	密文版本号

字节	Bit	十六进制初始值	条件
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1		如果有发卡行自定义数据的话，自定义数据长度 (最长15)
10-24	8-1		1-15字节的发卡行自定义数据。

4.1.10 应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	专用标识符扩展(PIX)	卡种
A0 00 00 03 33	01 01 01	PBOC DEBIT

4.1.11 应用用途控制

'FF00' 十六进制

字节	b8	b7	b6	b5	b4	b3	B2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.1.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 0000 4203 0103 1F00’ 十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0100 0010 0000 0011	联机PIN	1	如果终端支持	应用后续的
0000 0001 0000 0011	脱机PIN	2	如果终端支持	CVM处理过程失败
0001 1111 0000 0000	不需要持卡人验证	3	总是	不会失败

4.1.13 应用缺省行为

‘C000’ 十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持卡片与发卡行认证和授权控制处理。

4.2 模板 2—借记卡—DDA, 联机 PIN,发卡行认证, 和授权控制

4.2.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征 (AIP)	b	'82'	2	**7C00** *详见4.2.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	'87'	1	**01** *详见 4.2.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器(ATC)	b	'9F36'	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	'9F08'	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.2.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				
静态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				
发卡行认证指示位	b	‘9F56’	1	**00 或 80 推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（‘80’）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
日志格式	b	‘9F4F’	Var.	**9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602** *详见 4.2.5*	列出日志记录中数据对象的标签和长度	✔			
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板 推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器（国际-货币）	b	–	1	**初始设置为 0**	国际脱机交易计数器。 当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
累计脱机交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		

数据名称	**在卡片上的数据格式**	**Tag**	**数据长度 (bytes)**	**值** (十六进制)	**描述**	**模板缺省设置**	**发卡行通用数据**	**卡或持卡人特殊数据**	**数据存储在文件记录中**
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限 (LCOL)	b	‘9F58’	1	**发卡行模板 推荐值 0**	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。		✔		
连续脱机交易上限 (UCOL)	b	‘9F59’	1	**发卡行模板 推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		
卡片风险管理数据对象列表 1 (CDOL1)	b	‘8C’	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见 4.2.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片风险管理数据对象列表2 (CDOL2)	b	‘8D’	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见 4.2.7*	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），包括：发卡行响应码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔
密文信息数据	b	‘9F27’	1	初始设置为0	表明卡片返回的密文类型	✔			
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**00 10 00 00 00** *详见 4.2.8*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 9C F8 00** *详见 4.2.8*	指定交易联机上送的条件。	✔			✔
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 9C A8 00** *详见 4.2.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07_ _ 01 03 00 00 00 01** *详见 4.2.9*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		
发卡行国家代码	n	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
首选语言	an	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔
应用标识符(AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.2.10*	注册应用提供商标识（RID）和专用标识符扩展： **A0 00 00 03 33 01 01 01** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样) ，01 01 01 表明 PBOC 借记应用。				
应用标签	ans	‘50’	1-16	**发卡行模板** *详见 4.2.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.2.11*	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。 用于提供更灵活的卡片服务控制（类似服务代码）。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔
磁条 2 等效数据	var.	‘57’	最大 19	磁条数据文件提供	等效磁条 2 数据(格式不一致） 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期（5F24）一致			✔	✔
持卡人验证方法(CVM)列表	b	‘8E’	12	**0000 0000 0000 0000 4203 4103 1E03 1F00** *详见 4.2.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
CA 公钥索引(PKI)	b	‘8F’	1	发卡行模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✔		✔
发卡行公钥(IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证		✔		✔
发卡行公钥余数 (如果需要)	b	‘92’	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分		✔		✔
发卡行公钥指数	b	‘9F32’	1 to N_I/4	发卡行模板	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		✔		✔
签名的静态应用数据（SAD）	b	‘93’	var.	发卡行模板	用发卡行签名的应用数据，在 SDA 过程中由终端验证			✔	✔
IC 卡公钥证书	b	‘9F46’	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔
IC 卡公钥指数	b	‘9F47’	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔
IC 卡公钥余数	b	‘9F48’	N_{IC} –N_I+42	发卡行模板	没有放入 IC 卡公钥证书的 IC 卡公钥部分			✔	✔
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
动态数据认证数据对象列表(DDOL)	b	‘9F49’	最大252	发卡行模板 *详见4.2.13*	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。		✔		✔
应用缺省行为(ADA)	b	‘9F52’	2	**C000** *详见4.2.14*	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	✔			
子密钥(UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥(UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥(ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥(MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.2.2 应用交互特征(AIP)设置

'7C00' 十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.2.3 应用优先指示器

'01' 十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.2.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位	1 bit	0	-

卡片内部数据	保留	初始值	Tag
发卡行认证失败指示位	1 bit	0	-
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选　1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits		-
连续脱机交易下限	1 字节	发卡行模板 =0	‘9F58’
连续脱机交易上限	1 字节	>=连续脱机交易下限， =0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板=0	‘9F54’
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数（国内），=0	‘9F5C’

注： 为了支持DDA,SDA,发卡行认证和授权控制处理,带阴影的指示位应当在个人化时设置.

4.2.5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14　9C 01 9F36 02’十六进制(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6

数据对象名称	Tag(标签)	长度
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.2.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’十六进制(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.2.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’十六进制(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2

数据对象名称	Tag(标签)	长度
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.2.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

’00 10 00 00 00’ 十六进制 （发卡行行为代码-拒绝）

‘D8 68 9C F8 00’ 十六进制 （发卡行行为代码-联机）

‘D8 60 9C A8 00’ 十六进制 （发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**0**	1	1
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	**0**	1	1
要求输入PIN，密码键盘存在，但未输入PIN	**0**	1	1
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.2.9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1		如果有发卡行自定义数据的话，自定义数据长度(最长15)
10-24	8-1		1-15字节的发卡行自定义数据。

4.2.10 应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	专用标识符扩展(PIX)	卡种
A0 00 00 03 33	01 01 01	PBOC DEBIT

4.2.11 应用用途控制

'FF00' 十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.2.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 0000 4203 4103 1E03 1F00’十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0100 0010 0000 0011	联机PIN	1	如果终端支持	应用后续的
0100 0001 0000 0011	脱机PIN	2	如果终端支持	应用后续的
0001 1110 0000 0011	签名	3	如果终端支持	持卡人验证失败
0001 1111 0000 0000	不需要持卡人验证	4	总是	不会失败

4.2.13 动态数据对象列表 (DDOL)

‘9F37 04’十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度
不可预知数	9F37	4

4.2.14 应用缺省行为

‘C000’十六进制

字节	位	值	含义

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持卡片与发卡行认证和授权控制处理。

4.3 模板 3—贷记卡—DDA, 联机 PIN,发卡行认证, 和授权控制

4.3.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征(AIP)	b	'82'	2	**7C00** *详见4.3.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	'87'	1	**01** *详见 4.3.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器(ATC)	b	'9F36'	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	'9F08'	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.3.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				
静态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				
发卡行认证指示位	b	‘9F56’	1	**00 或 80 推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（’80’）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			
日志格式	b	‘9F4F’	Var.	**9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602** *详见 4.3.5*	列出日志记录中数据对象的标签和长度	✔			

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板 推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器（国际-货币）	b	–	1	**初始设置为 0**	国际脱机交易计数器。当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
累计脱机交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限 (LCOL)	b	‘9F58’	1	**发卡行模板 推荐值 0**	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。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易上限(UCOL)	b	'9F59'	1	**发卡行模板推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		
卡片风险管理数据对象列表 1(CDOL1)	b	'8C'	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见 4.3.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔
卡片风险管理数据对象列表 2(CDOL2)	b	'8D'	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见 4.3.7*	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），包括：发卡行返回码，授权金额,其他金额，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，终端不可预知数和交易时间。	✔			✔

数据名称	**在卡片上的数据格式**	**Tag**	**数据长度 (bytes)**	**值** (十六进制)	**描述**	**模板缺省设置**	**发卡行通用数据**	**卡或持卡人特殊数据**	**数据存储在文件记录中**
密文信息数据	b	‘9F27’	1	初始设置为 0	表明卡片返回的密文类型	✔			
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**00 10 00 00 00** *详见 4.3.8*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 9C F8 00** *详见 4.3.8*	指定交易联机上送的条件。	✔			✔
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 9C A8 00** *详见 4.3.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	7	**07_ _ 01 03 00 00 00 01** *详见 4.3.9*	在一个联机交易中，要传送到发卡行的专有应用数据。(一个分散密钥索引（DKI）)		✔		
发卡行国家代码	n	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔
首选语言	an	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔

数据名称	**在卡片上的数据格式**	**Tag**	**数据长度 (bytes)**	**值** (十六进制)	**描述**	**模板缺省设置**	**发卡行通用数据**	**卡或持卡人特殊数据**	**数据存储在文件记录中**
应用标识符 (AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.3.10*	注册应用提供商标识（RID）和专用标识符扩展： **A0 00 00 03 33 01 01 02** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样)，01 01 02 表明 PBOC 贷记应用。				
应用标签	ans	‘50’	1-16	发卡行模板 *详见 4.3.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.3.11*	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。 用于提供更灵活的卡片服务控制（类似服务代码）。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔
磁条1自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条1自定义数据相同			✔	✔
磁条2等效数据	var.	‘57’	最大19	磁条数据文件提供	等效磁条2数据（格式不一致） 磁条2等效数据中的有效期要求与IC卡内的应用失效日期（5F24）一致			✔	✔
持卡人验证方法(CVM)列表	b	‘8E’	12	**0000 0000 0000 0000 4203 1E03 1F00** *详见4.3.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
CA公钥索引(PKI)	b	‘8F’	1	发卡行模板	在SDA或DDA过程中，和RID一起使用，用来标识CA公钥		✔		✔
发卡行公钥(IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA认证过的发卡行公钥。用于脱机数据认证		✔		✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡行公钥余数 (如果需要)	b	'92'	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分		✔		✔
发卡行公钥指数	b	'9F32'	1 to N_I/4	发卡行模板	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		✔		✔
签名的静态应用数据（SAD）	b	'93'	var.	发卡行模板	用发卡行签名的应用数据，在 SDA 过程中由终端验证			✔	✔
IC 卡公钥证书	b	'9F46'	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔
IC 卡公钥指数	b	'9F47'	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔
IC 卡公钥余数	b	'9F48'	N_{IC} –N_I+42	发卡行模板	没有放入 IC 卡公钥证书的 IC 卡公钥部分			✔	✔
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	
动态数据认证数据对象列表 (DDOL)	b	'9F49'	最大 252	发卡行模板 *详见 4.3.13*	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。		✔		✔
应用缺省行为 (ADA)	b	'9F52'	2	**C000** *详见 4.3.14*	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	✔			

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥(UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥(ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.3.2 应用交互特征(AIP)设置

‘7C00’十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理

字节	位	值	含义
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.3.3 应用优先指示器

‘01’十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.3.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位	1 bit	0	-
发卡行认证失败指示位	1 bit	0	-
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits	00	-
连续脱机交易下限	1 字节	发卡行模板 = 0	‘9F58’
连续脱机交易上限	1 字节	发卡行模板 >= 连续脱机交易下限， =0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板	‘9F72’

卡片内部数据	保留	初始值	Tag
		=0	
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板 = 0	‘9F54’
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数（国内），=0	‘9F5C’

注： 为了支持DDA, SDA, 发卡行认证和授权控制处理, 带阴影的指示位应当在个人化时设置.

4.3.5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.3.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6

数据对象名称	Tag(标签)	长度
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.3.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.3.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

’00 10 00 00 00’ 十六进制 （发卡行行为代码-拒绝）

‘D8 68 9C F8 00’ 十六进制 （发卡行行为代码-联机）

‘D8 60 9C A8 00’ 十六进制 （发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话 脱机拒绝

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话 脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**0**	**1**	**1**
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	**0**	1	1
要求输入PIN，密码键盘存在，但未输入PIN	**0**	**1**	**1**
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.3.9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引

字节	Bit	十六进制初始值	条件
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1		如果有发卡行自定义数据的话，自定义数据长度 (最长15)
10-24	8-1		1-15字节的发卡行自定义数据。

4.3.10 应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	专用标识符扩展(PIX)	卡种
A0 00 00 03 33	01 01 02	PBOC CREDIT

4.3.11 应用用途控制

'FF00' 十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.3.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 0000 4203 1E03 1F00’十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0100 0010 0000 0011	联机PIN	1	如果终端支持	应用后续的
0001 1110 0000 0011	签名（纸上）	2	如果终端支持	持卡人验证失败
0001 1111 0000 0000	不需要持卡人验证	3	总是	不会失败

4.3.13 动态数据对象列表 (DDOL)

‘9F37 04’十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度
不可预知数	9F37	4

4.3.14 应用缺省行为

‘C000’十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持卡片与发卡行认证和授权控制处理。

4.4 模板 4—贷记卡—DDA, 签名,发卡行认证, 和授权控制

4.4.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征 (AIP)	b	'82'	2	**7C00** *详见 4.4.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	'87'	1	**01** *详见 4.4.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器(ATC)	b	'9F36'	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	'9F08'	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.4.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
静态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				
发卡行认证指示位	b	‘9F56’	1	**00 或 80** **推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（’80’）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
日志格式	b	‘9F4F’	Var.	**9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602** *详见 4.4.5*	列出日志记录中数据对象的标签和长度	✔			
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板 推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器（国际-货币）	b	–	1	**初始设置为 0**	国际脱机交易计数器。当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
累计脱机交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限 (LCOL)	b	‘9F58’	1	**发卡行模板推荐值 0**	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。		✔		
连续脱机交易上限 (UCOL)	b	‘9F59’	1	**发卡行模板推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		
卡片风险管理数据对象列表 1 (CDOL1)	b	‘8C’	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见 4.4.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片风险管理数据对象列表2 (CDOL2)	b	‘8D’	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见 4.4.7*	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），包括：发卡行返回码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔
密文信息数据	b	‘9F27’	1	初始设置为0	表明卡片返回的密文类型	✔			
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**0010 0000 00** *详见 4.4.8*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 04 F8 00** *详见 4.4.8*	指定交易联机上送的条件。	✔			✔
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 04 A8 00** *详见 4.4.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07_ _ 01 03 00 00 00 01** *详见 4.4.9*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		
发卡行国家代码	n	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
首选语言	an	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔
应用标识符 (AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.4.10*	注册应用提供商标识（RID）和专用标识符扩展：**A0 00 00 03 33 01 01 02** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样) ，01 01 02 表明 PBOC 贷记应用。				
应用标签	ans	‘50’	1-16	发卡行模板 *详见 4.4.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.4.11*	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。 用于提供更灵活的卡片服务控制（类似服务代码）。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔
磁条 2 等效数据	var.	‘57’	最大 19	磁条数据文件提供	等效磁条 2 数据（格式不一致） 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期（5F24）一致			✔	✔
持卡人验证方法(CVM)列表	b	‘8E’	14	**0000 0000 0000 0000 1E03 0203 1F00** *详见 4.4.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
CA 公钥索引 (PKI)	b	‘8F’	1	发卡行模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✔		✔
发卡行公钥 (IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证		✔		✔
发卡行公钥余数 (如果需要)	b	‘92’	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分		✔		✔
发卡行公钥指数	b	‘9F32’	1 to N_I/4	发卡行模板	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		✔		✔
签名的静态应用数据（SAD）	b	‘93’	var.	发卡行模板	用发卡行签名的应用数据，在 SDA 过程中由终端验证			✔	✔
IC 卡公钥证书	b	‘9F46’	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔
IC 卡公钥指数	b	‘9F47’	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔
IC 卡公钥余数	b	‘9F48’	N_{IC} –N_I+42	发卡行模板	没有放入IC卡公钥证书的IC卡公钥部分			✔	✔
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
动态数据认证数据对象列表(DDOL)	b	‘9F49’	最大252	发卡行模板 *详见 4.4.13*	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。		✔		✔
应用缺省行为(ADA)	b	‘9F52’	2	**C000** *详见 4.4.14*	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	✔			
子密钥(UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥(ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥(MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.4.2 应用交互特征(AIP)设置

'7C00'十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.4.3 应用优先指示器

'01'十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU

字节	位	值	含义
1	4-1	0001	最高优先级

4.4.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位 发卡行认证失败指示位	1 bit 1 bit	0 0	- -
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits	00	-
连续脱机交易下限	1 字节	发卡行模板 = 0	‘9F58’
连续脱机交易上限	1 字节	发卡行模板 > =连续脱机交易下限，=0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板 = 0	‘9F54’
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数（国内），=0	‘9F5C’

注： 为了支持DDA, SDA, 发卡行认证和授权控制处理, 带阴影的指示位应当在个人化时设置.

4.4.5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.4.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.4.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.4.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

’00 10 00 00 00’ 十六进制（发卡行行为代码-拒绝）

‘D8 68 04 F8 00’ 十六进制（发卡行行为代码-联机）

‘D8 60 04 A8 00’ 十六进制（发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	0	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	0	0	0
要求输入PIN，密码键盘存在，但未输入PIN	0	0	0
输入联机PIN	0	**1**	**1**

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4. 4. 9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1		如果有发卡行自定义数据的话，自定义数据长度 (最长15)
10-24	8-1		1-15字节的发卡行自定义数据。

4. 4. 10 应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	专用标识符扩展(PIX)	卡种
A0 00 00 03 33	01 01 02	PBOC CREDIT

4. 4. 11 应用用途控制

‘FF00’十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.4.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 0000 1E03 0203 1F00’十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0001 1110 0000 0011	签名	1	如果终端支持	CVM处理过程失败
0000 0010 0000 0011	联机PIN	2	如果终端支持	CVM处理过程失败
0001 1111 0000 0000	不需要持卡人验证	3	总是	不会失败

4.4.13 动态数据对象列表 (DDOL)

‘9F37 04’十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度
不可预知数	9F37	4

4.4.14 应用缺省行为

‘C000’十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。

字节	位	值	含义
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持卡片与发卡行认证和授权控制处理。

4.5 模板 5—贷记卡—DDA,联机 PIN,和授权控制

4.5.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征 (AIP)	b	'82'	2	**7C00** *详见4.5.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	'87'	1	**01** *详见 4.5.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器 (ATC)	b	'9F36'	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	'9F08'	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.5.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				
静态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				
发卡行认证指示位	b	‘9F56’	1	**00 或 80 推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（’80’）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
日志格式	b	‘9F4F’	Var.	**9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602** *详见 4.5.5*	列出日志记录中数据对象的标签和长度	✔			
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板 推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器（国际-货币）	b	–	1	**初始设置为 0**	国际脱机交易计数器。 当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
PIN 尝试限制数	b	–	1	**发卡行模板**	持卡人可以尝试输入不正确的 PIN 的次数。		✔		
PIN 尝试次数计数器	b	‘9F17’	1	**初始化为 0，在个人化的过程中，设置成 PIN 尝试限制数**	等于 PIN 尝试限制数。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
累计脱机交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限 (LCOL)	b	‘9F58’	1	**发卡行模板 推荐值 0**	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。		✔		
连续脱机交易上限 (UCOL)	b	‘9F59’	1	**发卡行模板 推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片风险管理数据对象列表 1 (CDOL1)	b	‘8C’	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见 4.5.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔
卡片风险管理数据对象列表 2 (CDOL2)	b	‘8D’	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见 4.5.7*	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），包括：发卡行返回码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔
密文信息数据	b	‘9F27’	1	初始设置为 0	表明卡片返回的密文类型	✔			
发卡行行为代码 (IAC)-拒绝	b	‘9F0E’	5	**00 10 80 00 00** *详见 4.5.8*	指定交易不进行联机直接拒绝的条件。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 3C F8 00** *详见 4.5.8*	指定交易联机上送的条件。	✔			✔
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 3C A8 00** *详见 4.5.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07_ _ 01 03 00 00 00 01** *详见 4.5.9*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		
发卡行国家代码	n	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔
首选语言	an	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔
应用标识符(AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.5.10*	注册应用提供商标识（RID）和专用标识符扩展：**A0 00 00 03 33 01 01 02** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样) ，01 01 02 表明 PBOC 贷记应用。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用标签	ans	‘50’	1-16	发卡行模板 *详见 4.5.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.5.11*	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。 用于提供更灵活的卡片服务控制（类似服务代码）。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔
磁条 2 等效数据	var.	‘57’	最大 19	磁条数据文件提供	等效磁条 2 数据（格式不一致） 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期（5F24）一致			✔	✔
持卡人验证方法(CVM)列表	b	‘8E’	12	**0000 0000 0000 0000 4203 4103 1E03 1F00** *详见 4.5.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
CA 公钥索引(PKI)	b	‘8F’	1	发卡行模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✔		✔
发卡行公钥(IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证。		✔		✔
发卡行公钥余数(如果需要)	b	‘92’	N_1 -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分。		✔		✔
发卡行公钥指数	b	‘9F32’	1 to N_I/4	发卡行模板	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。		✔		✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
签名的静态应用数据（SAD）	b	‘93’	var.	发卡行模板	用发卡行签名的应用数据，在 SDA 过程中由终端验证。			✔	✔
IC 卡公钥证书	b	‘9F46’	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔
IC 卡公钥指数	b	‘9F47’	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔
IC 卡公钥余数	b	‘9F48’	N_{IC} –N_I+42	发卡行模板	没有放入 IC 卡公钥证书的 IC 卡公钥部分			✔	✔
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	
动态数据认证数据对象列表 (DDOL)	b	‘9F49’	最大 252	发卡行模板 *详见 4.5.13*	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。		✔		✔
应用缺省行为 (ADA)	b	‘9F52’	2	**C040** *详见 4.5.14*	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	✔			
脱机 PIN	cn	–	2-6	发卡行提供	在卡片个人化时，由发卡行写入卡片				

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥 (UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥 (ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥 (MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥 (MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.5.2 应用交互特征(AIP)设置

‘7C00’十六进制

字节	位	值	含义
1	8	0	RFU

字节	位	值	含义
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.5.3 应用优先指示器

‘01’十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.5.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位	1 bit	0	-
发卡行认证失败指示位	1 bit	0	-
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits	00	-
连续脱机交易下限	1 字节	发卡行模板 = 0	‘9F58’
连续脱机交易上限	1 字节	发卡行模板>=连续脱机交易下限，=0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’

卡片内部数据	保留	初始值	Tag
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板 = 0	‘9F54’
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数（国内），=0	‘9F5C’

注： 为了支持DDA,SDA,脱机PIN,发卡行认证和授权控制处理,带阴影的指示位应当在个人化时设置.

4.5.5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.5.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6

数据对象名称	Tag(标签)	长度
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.5.7 卡片风险管理数据对象列表(CDOL) 2

'8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03' 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.5.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

'00 10 80 00 00' 十六进制 (发卡行行为代码-拒绝)

'D8 68 3C F8 00' 十六进制 (发卡行行为代码-联机)

'D8 60 3C A8 00' 十六进制 (发卡行行为代码-缺省)

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**1**	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	**1**	**1**
要求输入PIN但密码键盘不存在或不工作	0	**1**	**1**
要求输入PIN，密码键盘存在，但未输入PIN	0	**1**	**1**
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.5.9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	01	密文版本号

字节	Bit	十六进制初始值	条件
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1		如果有发卡行自定义数据的话，自定义数据长度 (最长15)
10-24	8-1		1-15字节的发卡行自定义数据。

4.5.10 应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	专用标识符扩展(PIX)	卡种
A0 00 00 03 33	01 01 02	PBOC CREDIT

4.5.11 应用用途控制

'FF00' 十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.5.12 持卡人验证方法(CVM)列表

'0000 0000 0000 0000 4203 4103 1E03 1F00' 十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0100 0010 0000 0011	联机加密PIN验证	1	如果终端支持	应用后续的
0100 0001 0000 0011	脱机PIN	2	如果终端支持	应用后续的
0001 1110 0000 0011	签名（纸上）	3	如果终端支持	持卡人验证失败
0001 1111 0000 0000	不需要持卡人验证	4	总是	不会失败

4.5.13 动态数据对象列表 (DDOL)

‘9F37 04’ 十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度
不可预知数	9F37	4

4.5.14 应用缺省行为

‘C040’ 十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	**1**	如果PIN在前次交易中锁定，拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持PIN、卡片与发卡行认证和授权控制处理。

4.6 模板 6—贷记卡—CDA,脱机 PIN,和授权控制

4.6.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征 (AIP)	b	'82'	2	**7D00** *详见 4.6.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	'87'	1	**01** *详见 4.6.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器(ATC)	b	'9F36'	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	'9F08'	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.6.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				
静态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				
发卡行认证指示位	b	‘9F56’	1	**00 或 80** **推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（’80’）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			
日志格式	b	‘9F4F’	Var.	**9A03** **9F2103** **9F0206** **9F0306** **9F1A02** **5F2A02** **9F4E14** **9C01** **9F3602** *详见 4.6.5*	列出日志记录中数据对象的标签和长度	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板 推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器(国际-货币)	b	–	1	**初始设置为 0**	国际脱机交易计数器。当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
PIN 尝试限制数	b	–	1	**发卡行模板**	持卡人可以尝试输入不正确的 PIN 的次数。		✔		
PIN 尝试次数计数器	b	‘9F17’	1	**初始化为 0，在个人化的过程中，设置成 PIN 尝试限制数**	等于 PIN 尝试限制数				
累计脱机交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	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。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易下限 (LCOL)	b	'9F58'	1	**发卡行模板 推荐值 0**	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。		✔		
连续脱机交易上限 (UCOL)	b	'9F59'	1	**发卡行模板 推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		
卡片风险管理数据对象列表 1 (CDOL1)	b	'8C'	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见 4.6.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔
卡片风险管理数据对象列表 2 (CDOL2)	b	'8D'	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见 4.6.7*	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），包括：发卡行返回码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
密文信息数据	b	‘9F27’	1	初始设置为 0	表明卡片返回的密文类型	✔			
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**04 10 80 00 00** *详见 4.6.8*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 3C F8 00** *详见 4.6.8*	指定交易联机上送的条件。	✔			✔
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 3C A8 00** *详见 4.6.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07_ _ 01 03 00 00 00 01** *详见 4.6.9*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		
发卡行国家代码	n	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔
首选语言	an	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔
应用标识符(AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.6.10*	注册应用提供商标识（RID）和专用标识符扩展： **A0 00 00 03 33 01 01 02** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样) ， 01 01 02 表明 PBOC 贷记应用。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用标签	ans	‘50’	1-16	发卡行模板 *详见 4.6.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.6.11*	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。 用于提供更灵活的卡片服务控制（类似服务代码）。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔
磁条 2 等效数据	var.	‘57’	最大 19	磁条数据文件提供	等效磁条 2 数据（格式不一致） 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期（5F24）一致			✔	✔
持卡人验证方法(CVM)列表	b	‘8E’	12	**0000 0000 0000 0000 4103 4203 1E03 1F00** *详见 4.6.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
CA 公钥索引(PKI)	b	‘8F’	1	发卡行模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✔		✔
发卡行公钥(IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证。		✔		✔
发卡行公钥余数 (如果需要)	b	‘92’	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分。		✔		✔
发卡行公钥指数	b	‘9F32’	1 to N_I/4	发卡行模板	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。		✔		✔
签名的静态应用数据（SAD）	b	‘93’	var.	发卡行模板	用发卡行签名的应用数据，在 SDA 过程中由终端验证。			✔	✔
IC 卡公钥证书	b	‘9F46’	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
IC 卡公钥指数	b	'9F47'	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔
IC 卡公钥余数	b	'9F48'	N_{IC} –N_I+42	发卡行模板	没有放入 IC 卡公钥证书的 IC 卡公钥部分			✔	✔
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	
动态数据认证数据对象列表 (DDOL)	b	'9F49'	最大 252	发卡行模板 *详见 4.6.13*	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。		✔		✔
应用缺省行为 (ADA)	b	'9F52'	2	**C040** *详见 4.6.14*	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	✔			
脱机 PIN	cn	_	2-6	发卡行提供	在卡片个人化时，由发卡行写入卡片				
子密钥 (UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥(ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.6.2 应用交互特征(AIP)设置

‘7D00’十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	1	支持CDA
2	8-1	0000 0000	RFU

4.6.3 应用优先指示器

‘01’十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.6.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位	1 bit	0	-
发卡行认证失败指示位	1 bit	0	-
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits	00	-
连续脱机交易下限	1 字节	发卡行模板 = 0	‘9F58’
连续脱机交易上限	1 字节	发卡行模板 > =连续脱机交易下限， =0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板 = 0	‘9F54’
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数（国内），=0	‘9F5C’

注： 为了支持DDA,SDA,脱机PIN,发卡行认证和授权控制处理,带阴影的指示位应当在个人化时设置.

4.6.5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.6.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.6.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.6.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

’04 10 80 00 00’十六进制（发卡行行为代码-拒绝）

‘D8 68 3C F8 00’十六进制（发卡行行为代码-联机）

‘D8 60 3C A8 00’十六进制（发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	**1**	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
RFU	000	000	000
持卡人验证失败	**1**	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	**1**	**1**
要求输入PIN但密码键盘不存在或不工作	0	**1**	**1**
要求输入PIN，密码键盘存在，但未输入PIN	0	**1**	**1**
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4. 6. 9　发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1		如果有发卡行自定义数据的话，自定义数据长度 (最长15)
10-24	8-1		1-15字节的发卡行自定义数据。

4. 6. 10　应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	专用标识符扩展(PIX)	卡种
A0 00 00 03 33	01 01 02	PBOC CREDIT

4.6.11 应用用途控制

‘FF00’十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.6.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 0000 4103 4203 1E03 1F00’十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0100 0001 0000 0011	脱机PIN	1	如果终端支持	应用后续的
0100 0010 0000 0011	联机加密PIN验证	2	如果终端支持	应用后续的
0001 1110 0000 0011	签名（纸上）	3	如果终端支持	持卡人验证失败
0001 1111 0000 0000	不需要持卡人验证	4	总是	不会失败

4.6.13 动态数据对象列表 (DDOL)

‘9F37 04’十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度
不可预知数	9F37	4

4.6.14 应用缺省行为

‘C040’十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	**1**	如果PIN在前次交易中锁定，拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持PIN、卡片与发卡行认证和授权控制处理。

4.7 模板 7—准贷记卡—DDA,联机 PIN,发卡行认证,和授权控制

4.7.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征 (AIP)	b	'82'	2	**7C00** *详见 4.7.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	'87'	1	**01** *详见 4.7.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器(ATC)	b	'9F36'	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	'9F08'	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.7.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				
静态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				
发卡行认证指示位	b	‘9F56’	1	**00 或 80 推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（’80’）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			
日志格式	b	‘9F4F’	Var.	**9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602** *详见 4.7.5*	列出日志记录中数据对象的标签和长度	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器(国际-货币)	b	–	1	**初始设置为 0**	国际脱机交易计数器。当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
累计脱机交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限 (LCOL)	b	‘9F58’	1	**发卡行模板推荐值 0**	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。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易上限 (UCOL)	b	‘9F59’	1	**发卡行模板推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		
卡片风险管理数据对象列表 1 (CDOL1)	b	‘8C’	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见 4.7.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔
卡片风险管理数据对象列表 2 (CDOL2)	b	‘8D’	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见 4.7.7*	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），包括：发卡行返回码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
密文信息数据	b	‘9F27’	1	初始设置为 0	表明卡片返回的密文类型	✔			
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**00 10 98 00 00** *详见 4.8.7*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 04 F8 00** *详见 4.7.8*	指定交易联机上送的条件。	✔			✔
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 04 A8 00** *详见 4.7.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	7	**07_ _ 01 03 00 00 00 01** *详见 4.7.9*	在一个联机交易中，要传送到发卡行的专有应用数据。（一个分散密钥索引（DKI））		✔		
发卡行国家代码	n	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔
首选语言	an	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用标识符 (AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.7.10*	注册应用提供商标识（RID）和专用标识符扩展，例如： **A0 00 00 03 33 01 01 03** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样) ， 01 01 03 表明 PBOC 准贷记应用。				
应用标签	ans	‘50’	1-16	发卡行模板 *详见 4.7.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.7.11*	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。 用于提供更灵活的卡片服务控制(类似服务码)。‘2’ = hex **FF00** 是模板缺省值，卡片仅支持国内功能时设为‘6’ = hex **AB00。**	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔
磁条 2 等效数据	var.	‘57’	最大 19	磁条数据文件提供	等效磁条 2 数据(格式不一致) 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期（5F24）一致			✔	✔
持卡人验证方法(CVM)列表	b	‘8E’	14	**0000 0000 0000 0000 0203 1E03 1F00** *详见 4.7.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
CA 公钥索引 (PKI)	b	‘8F’	1	发卡行模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✔		✔
发卡行公钥 (IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证		✔		✔
发卡行公钥余数 (如果需要)	b	‘92’	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分		✔		✔
发卡行公钥指数	b	‘9F32’	1 to N_I/4	发卡行模板	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		✔		✔
签名的静态应用数据（SAD）	b	‘93’	var.	发卡行模板	用发卡行签名的应用数据，在 SDA 过程中由终端验证。			✔	✔
IC 卡公钥证书	b	‘9F46’	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔
IC 卡公钥指数	b	‘9F47’	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔
IC 卡公钥余数	b	‘9F48’	N_{IC} –N_I+42	发卡行模板	没有放入 IC 卡公钥证书的 IC 卡公钥部分			✔	✔
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	
动态数据认证数据对象列表 (DDOL)	b	‘9F49’	最大 252	发卡行模板 *详见 4.7.13*	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。		✔		✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用缺省行为(ADA)	b	'9F52'	2	**C000** *详见 4.7.14*	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	✔			
子密钥(UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥(ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.7.2 应用交互特征(AIP)设置

'7C00' 十六进制

字节	位	值	含义

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.7.3 应用优先指示器

‘01’十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.7.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位	1 bit	0	-
发卡行认证失败指示位	1 bit	0	-
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits	00	-
连续脱机交易下限	1 字节	发卡行模板 = 0	‘9F58’
连续脱机交易上限	1 字节	发卡行模板	‘9F59’

卡片内部数据	保留	初始值	Tag
		>= 连续脱机交易下限，=0	
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板 = 0	‘9F54’
累计脱机交易上限	6 字节	发卡行模板 > CTAL	‘9F5C’

注： 为了支持DDA, SDA, 发卡行认证和授权控制处理, 带阴影的指示位应当在个人化时设置.

4.7.5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.7.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.7.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.7.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

’00 10 98 00 00’ 十六进制 （发卡行行为代码-拒绝）

‘D8 68 04 F8 00’ 十六进制 （发卡行行为代码-联机）

‘D8 60 04 A8 00’ 十六进制（发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**1**	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	**1**	0	0
要求输入PIN，密码键盘存在，但未输入PIN	**1**	0	0
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.7.9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度

字节	Bit	十六进制初始值	条件
2	8-1	发卡行模板	分散密钥索引
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1		如果有发卡行自定义数据的话，自定义数据长度 (最长15)
10-24	8-1		1-15字节的发卡行自定义数据。

4. 7. 10　应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	专用标识符扩展(PIX)	卡种
A0 00 00 03 33	01 01 03	PBOC QUASICREDIT

4. 7. 11　应用用途控制

'FF00' 十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设

置为6，则只有国内功能被允许。

4.7.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 0000 0203 1E03 1F00’十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0000 0010 0000 0011	联机PIN	1	如果终端支持	CVM处理过程失败
0001 1110 0000 0011	签名	2	如果终端支持	CVM处理过程失败
0001 1111 0000 0000	不需要持卡人验证	3	总是	不会失败

4.7.13 动态数据对象列表 (DDOL)

‘9F37 04’十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度
不可预知数	9F37	4

4.7.14 应用缺省行为

‘C000’十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持卡片与发卡行认证和授权控制处理。

4.8 模板 11—纯电子现金卡—DDA，无需 CVM

4.8.1 标准 PBOC

4.8.1.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征(AIP)	b	‘82’	2	**7C00** *详见 4.8.1.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	‘87’	1	**01** *详见 4.8.1.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器(ATC)	b	‘9F36’	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	‘9F08’	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.8.1.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				
动态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				
发卡行认证指示位	b	‘9F56’	1	**00 或 80 推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（‘80’）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			
日志格式	b	‘9F4F’	Var.	**9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602** *详见 4.8.1.5*	列出日志记录中数据对象的标签和长度	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板 推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器（国际-货币）	b	–	1	**初始设置为 0**	国际脱机交易计数器。当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
累计交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限 (LCOL)	b	‘9F58’	1	**发卡行模板 推荐值 0**	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。		✔		
连续脱机交易上限 (UCOL)	b	‘9F59’	1	**发卡行模板 推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片风险管理数据对象列表 1 (CDOL1)	b	‘8C’	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见 4.8.1.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔
卡片风险管理数据对象列表 2 (CDOL2)	b	‘8D’	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见 4.8.1.7*	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），包括：发卡行响应码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔
密文信息数据	b	‘9F27’	1	初始设置为 0	表明卡片返回的密文类型	✔			
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**00 10 98 00 00** *详见 4.8.1.8*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 04 F8 00** *详见 4.8.1.8*	指定交易联机上送的条件。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 04 A8 00** *详见 4.8.1.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07_ _ 01 03 00 00 00 01 0A 01** *详见 4.8.1.9*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		
发卡行国家代码	b	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔
首选语言	ans	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔
应用标识符(AID)	b	‘4F’	5-16	**初始化好的** *详见 4.8.1.10*	注册应用提供商标识（RID）和专用标识符扩展： **A0 00 00 03 33 01 01 06** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样) ， 01 01 01 表明 PBOC 借记应用。				
应用标签	ans	‘50’	1-16	**发卡行模板** *详见 4.8.1.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		

数据名称	**在卡片上的数据格式**	**Tag**	**数据长度 (bytes)**	**值** (十六进制)	**描述**	**模板缺省设置**	**发卡行通用数据**	**卡或持卡人特殊数据**	**数据存储在文件记录中**
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.8.1.11*	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。 用于提供更灵活的卡片服务控制（类似服务代码）。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
磁条 2 等效数据	var.	‘57’	最大 19	磁条数据文件提供	等效磁条 2 数据(格式不一致） 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期（5F24）一致			✔	✔
持卡人验证方法(CVM)列表	b	‘8E’	12	**0000 0000 0000 0000 0203 1F00** *详见 4.8.1.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
CA 公钥索引(PKI)	b	‘8F’	1	发卡行模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✔		✔
发卡行公钥(IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证		✔		✔
发卡行公钥余数 (如果需要)	b	‘92’	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分		✔		✔
发卡行公钥指数	b	‘9F32’	1 to N_I/4	发卡行模板	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		✔		✔
签名的静态应用数据（SAD）	b	‘93’	var.	发卡行模板	用发卡行签名的应用数据，在 SDA 过程中由终端验证			✔	✔
IC 卡公钥证书	b	‘9F46’	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔
IC 卡公钥指数	b	‘9F47’	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔
IC 卡公钥余数	b	‘9F48’	N_{IC} –N_I+42	发卡行模板	没有放入 IC 卡公钥证书的 IC 卡公钥部分			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	
动态数据认证数据对象列表(DDOL)	b	'9F49'	最大252	发卡行模板 *详见 4.8.1.13*	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。		✔		✔
应用缺省行为(ADA)	b	'9F52'	2	**C000** *详见 4.8.1.14*	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	✔			
子密钥(UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥(ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥(MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.8.1.2 应用交互特征(AIP)设置

'7C00'十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.8.1.3 应用优先指示器

'01'十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.8.1.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-

卡片内部数据	保留	初始值	Tag
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位 发卡行认证失败指示位	1 bit 1 bit	0 0	- -
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选　1=强制)	1 字节	00或80 推荐00	'9F56'
发卡行脚本命令计数器	4 bits		-
连续脱机交易下限	1 字节	发卡行模板 =0	'9F58'
连续脱机交易上限	1 字节	>=连续脱机交易下限， =0	'9F59'
上次联机应用交易计数器（ATC）寄存器	2 字节	0	'9F13'
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	'9F53'
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	'9F72'
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	'9F17'
累计脱机交易金额数（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板=0	'9F54'
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数（国内），=0	'9F5C'

注： 为了支持DDA, SDA, 发卡行认证和授权控制处理, 带阴影的指示位应当在个人化时设置.

4.8.1.5　日志格式

'9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14　9C 01 9F36 02' 十六进制(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
交易日期	9A	3

数据对象名称	Tag(标签)	长度
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.8.1.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’十六进制(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.8.1.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’十六进制(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6

数据对象名称	Tag(标签)	长度
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.8.1.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

’00 10 98 00 00’ 十六进制（发卡行行为代码-拒绝）

‘D8 68 04 F8 00’ 十六进制（发卡行行为代码-联机）

‘D8 60 04 A8 00’ 十六进制（发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**1**	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	**1**	0	0
要求输入PIN，密码键盘存在，但未输入PIN	**1**	0	0
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话 脱机拒绝
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.8.1.9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1	0A	发卡行自定义数据(IDD)-自定义数据长度 (最长15)
10	8-1	01	IDD ID
11-15	8-1	初始设置为0	金额域
16-19	8-1	初始设置为0	MAC
20-24	8-1		其它的发卡行自定义数据

4.8.1.10 应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	专用标识符扩展(PIX)	卡种
A0 00 00 03 33	01 01 06	纯电子现金应用

4.8.1.11 应用用途控制

'FF00' 十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.8.1.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 0000 0203 1F00’十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0000 0010 0000 0011	联机PIN	1	如果终端支持	CVM处理过程失败
0001 1111 0000 0000	不需要持卡人验证	2	总是	不会失败

4.8.1.13 动态数据对象列表 (DDOL)

‘9F37 04’十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度
不可预知数	9F37	4

4.8.1.14 应用缺省行为

‘C000’十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	00	RFU

注： 带阴影的指示位表示支持卡片与发卡行认证和授权控制处理。

4.8.2 电子现金—无需 CVM

4.8.2.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
电子现金余额	n	‘9F79’	6	**初始设置为 0**	保存了可供脱机消费的剩余总额。				
电子现金余额上限	n	‘9F77’	6	**发卡行模板**	表示在电子现金应用中，持卡人可脱机消费的最大累积额度，也即卡片充值所能达到的上限。			✔	
电子现金发卡行授权码	an	‘9F74’	6	**ECC001**	卡片上用于标识批准电子现金交易的代码。	✔			✔
电子现金单笔交易限额	n	‘9F78’	6	**发卡行模板**	卡片上单笔电子现金交易额的上限，用于控制单笔电子现金交易风险。			✔	
电子现金重置阈值	n	‘9F6D’	6	**发卡行模板**	触发卡片进行自动充值的可用余额下限。			✔	
处理选项数据对象列表(PDOL)	b	‘9F38’	9	**9F7A 01 9F02 06 5F2A 02** *详见 4.8.2.2*	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）。	✔			✔
持卡人验证方法(CVM)列表	b	‘8E’	10	**0000 0000 0000 0000 1F03** *详见 4.8.2.3*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**00 10 80 00 00** *详见 4.8.2.4*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 3C F8 00** *详见 4.8.2.4*	指定交易联机上送的条件。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡行行为代码(IAC)-缺省	b	'9F0D'	5	**D8 60 3C A8 00** *详见 4.8.2.4*	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。	✔			✔

4.8.2.2 处理选项数据对象列表(PDOL)

'9F7A 01 9F02 06 5F2A 02' 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
电子现金终端支持指示器	9F7A	1
授权金额	9F02	6
交易货币代码	5F2A	2

4.8.2.3 持卡人验证方法(CVM)列表

'0000 0000 0000 0000 1F03' 十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0001 1111 0000 0011	不需要持卡人验证	1	如果终端支持	CVM处理过程失败

4.8.2.4 发卡行行为代码 (IAC)(拒绝、联机和缺省)

'00 10 80 00 00' 十六进制 (发卡行行为代码-拒绝)

'D8 68 3C F8 00' 十六进制 (发卡行行为代码-联机)

'D8 60 3C A8 00' 十六进制 (发卡行行为代码-缺省)

条件	结果		
	IAC拒绝- 脱机拒绝	IAC 联机 – 要求联机	IAC 缺省 – 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**1**	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	**1**	**1**
要求输入PIN但密码键盘不存在或不工作	0	**1**	**1**
要求输入PIN，密码键盘存在，但未输入PIN	0	**1**	**1**
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.8.3 非接触式 IC 卡支付—fDDA，应用密文版本 17，小额检查

4.8.3.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片附加处理	b	‘9F68’	4	**81 00 00 00** *详见 4.8.3.4*	指出卡片处理需求和参数选择。				
卡片内部指示器	b	_	2	**初始设置为 0**	用于控制 qPBOC 卡片内部过程。				
卡片交易属性	b	‘9F6C’	2	**初始设置为 00 00** *详见 4.8.3.5*	主要用于向终端指明卡片要求的 CVM。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
脱机消费可用余额	n	‘9F5D’	6	**初始设置为 1**	一个计算域，可用于终端显示卡片的脱机可用额度、或用于发卡行风险管控。				
应用交互特征(AIP)	b	‘82’	2	**7C00** *详见 4.8.3.2*	说明此应用中卡片支持的功能。	✔			
处理选项数据对象列表(PDOL)	b	‘9F38’	12	**9F66 04 9F02 06 9F37 04 5F2A 02** *详见 4.8.3.3*	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）。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07 _ 17 03 00 00 00 01 0A 01 _ _** *详见 4.8.3.6*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		

4.8.3.2 应用交互特征(AIP)设置

‘7C00’ 十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持fDDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	00000000	RFU

4.8.3.3 处理选项数据对象列表(PDOL)

‘9F66 04 9F02 06 9F37 04 5F2A 02’ 十六进制

（数据对象的标签和长度）

数据对象名称	Tag(标签)	长度
终端交易属性	9F66	4
授权金额	9F02	6
不可预知数	9F37	4
交易货币代码	5F2A	2

4.8.3.4 卡片附加处理

‘81 40 00 00’十六进制

字节	位	值	含义
1	8	1	支持小额检查
1	7	0	不支持小额和CTTA检查
1	6	0	不支持小额或CTTA检查
1	5	0	不支持新卡检查
1	4	0	不支持PIN重试次数超过检查
1	3	0	不允许货币不匹配的脱机交易
1	2	0	卡片不优先选择接触式PBOC联机
1	1	1	返回脱机消费可用额度
2	8	0	不支持预付
2	7	1	不允许不匹配货币的交易
2	6	0	如果是新卡且读卡器仅支持脱机，不拒绝交易
2	5-1	00000	RFU
3	8	0	匹配货币的交易不支持联机PIN
3	7	0	不匹配货币的交易不支持联机PIN
3	6	0	对于不匹配货币交易，卡不要求CVM
3	5	0	不支持签名
3	4-1	0000	RFU
4	8-1	00000000	RFU

4.8.3.5 卡片交易属性

‘00 00’十六进制

字节	位	值	含义

字节	位	值	含义
1	8	0	不需要联机PIN
1	7	0	不需要签名
1	6	0	如果脱机数据认证失败且终端可联机，不要求联机
1	5	0	如果脱机数据认证失败且终端支持接触式PBOC，不终止
1	4-1	0000	RFU
2	8-1	00000000	RFU

4.8.3.6 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	17(十六进制)	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1	0A	发卡行自定义数据(IDD)-自定义数据长度 (最长15)
10	8-1	01	IDD ID
11-15	8-1	初始设置为0	金额域
16-19	8-1	初始设置为0	MAC
20-24	8-1		其它的发卡行自定义数据

4.9 模板 12—借记卡+电子现金+非接触式 IC 卡支付

4.9.1 标准 PBOC—借记卡—DDA，联机 PIN,发卡行认证，和授权控制

4.9.1.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征(AIP)	b	‘82’	2	**7C00** *详见 4.9.1.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	‘87’	1	**01** *详见 4.9.1.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器(ATC)	b	‘9F36’	2	**初始设置为 0**	记录个人化以后交易处理的次数。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用版本号	b	'9F08'	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.9.1.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				
动态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				
发卡行认证指示位	b	'9F56'	1	**00 或 80 推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（'00'）或强制（'80'）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			
日志格式	b	‘9F4F’	Var.	**9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602** *详见 4.9.1.5*	列出日志记录中数据对象的标签和长度	✔			
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器（国际-货币）	b	–	1	**初始设置为 0**	国际脱机交易计数器。当计数器超过累计脱机交易限制数时，卡片请求交易联机。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
累计交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限 (LCOL)	b	‘9F58’	1	**发卡行模板推荐值 0**	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。		✔		
连续脱机交易上限 (UCOL)	b	‘9F59’	1	**发卡行模板推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片风险管理数据对象列表 1 (CDOL1)	b	‘8C’	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见 4.9.1.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔
卡片风险管理数据对象列表 2 (CDOL2)	b	‘8D’	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见 4.9.1.7*	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），包括：发卡行响应码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔
密文信息数据	b	‘9F27’	1	初始设置为 0	表明卡片返回的密文类型	✔			
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**00 10 00 00 00** *详见 4.9.1.8*	指定交易不进行联机直接拒绝的条件。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 9C F8 00** *详见 4.9.1.8*	指定交易联机上送的条件。	✔			✔
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 9C A8 00** *详见 4.9.1.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07_ _ 01 03 00 00 00 01 0A 01** *详见 4.9.1.9*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		
发卡行国家代码	b	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔
首选语言	ans	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔
应用标识符(AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.9.1.10*	注册应用提供商标识（RID）和专用标识符扩展： **A0 00 00 03 33 01 01 01** A0 00 00 03 33 确定 PBOC 注册应用提供商(所有的卡片都一样) ，01 01 01 表明 PBOC 借记应用。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用标签	ans	‘50’	1-16	**发卡行模板** *详见 4.9.1.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.9.1.11*	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。 用于提供更灵活的卡片服务控制（类似服务代码）。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于26字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔
磁条 2 等效数据	var.	‘57’	最大 19	磁条数据文件提供	等效磁条 2 数据（格式不一致） 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期（5F24）一致			✔	✔
持卡人验证方法(CVM)列表	b	‘8E’	14	**0000 0000 0000 4203 4103 1E03 1F00** *详见 4.9.1.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
CA 公钥索引(PKI)	b	‘8F’	1	发卡行模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✔		✔
发卡行公钥(IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证		✔		✔
发卡行公钥余数 (如果需要)	b	‘92’	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分		✔		✔
发卡行公钥指数	b	‘9F32’	1 to N_I/4	发卡行模板	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		✔		✔
签名的静态应用数据（SAD）	b	‘93’	var.	发卡行模板	用发卡行签名的应用数据，在 SDA 过程中由终端验证			✔	✔
IC 卡公钥证书	b	‘9F46’	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔
IC 卡公钥指数	b	‘9F47’	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
IC 卡公钥余数	b	‘9F48’	N_{IC} –N_I+42	发卡行模板	没有放入 IC 卡公钥证书的 IC 卡公钥部分			✔	✔
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	
动态数据认证数据对象列表 (DDOL)	b	‘9F49’	最大 252	发卡行模板 *详见 4.9.1.13*	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。		✔		✔
应用缺省行为 (ADA)	b	‘9F52’	2	**C000** *详见 4.9.1.14*	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	✔			
子密钥 (UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥 (ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥 (MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥 (MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.9.1.2 应用交互特征(AIP)设置

'7C00' 十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.9.1.3 应用优先指示器

'01' 十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.9.1.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位 发卡行认证失败指示位	1 bit 1 bit	0 0	- -
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选　1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits		-
连续脱机交易下限	1 字节	发卡行模板 =0	‘9F58’
连续脱机交易上限	1 字节	>=连续脱机交易下限，=0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额数（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板=0	‘9F54’
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数（国内），=0	‘9F5C’

注： 为了支持DDA,SDA,发卡行认证和授权控制处理,带阴影的指示位应当在个人化时设置.

4.9.1.5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’十六进制(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
交易日期	9A	3

数据对象名称	Tag(标签)	长度
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.9.1.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’十六进制(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.9.1.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’十六进制(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6

数据对象名称	Tag(标签)	长度
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.9.1.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

'00 10 00 00 00' 十六进制 (发卡行行为代码-拒绝)

'D8 68 9C F8 00' 十六进制 (发卡行行为代码-联机)

'D8 60 9C A8 00' 十六进制 (发卡行行为代码-缺省)

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**0**	1	1
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	**0**	1	1
要求输入PIN，密码键盘存在，但未输入PIN	**0**	1	1
输入联机PIN	0	**1**	**1**
RFU	00	00	00

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.9.1.9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1	0A	发卡行自定义数据(IDD)-自定义数据长度 (最长15)
10	8-1	01	IDD ID
11-15	8-1	初始设置为0	金额域
16-19	8-1	初始设置为0	MAC
20-24	8-1		其它的发卡行自定义数据

4.9.1.10 应用标识符和应用标签

应用标识符 (AID)		**应用标签**
注册应用提供商标识(RID)	**专用标识符扩展(PIX)**	**卡种**
A0 00 00 03 33	01 01 01	PBOC DEBIT

4.9.1.11 应用用途控制

‘FF00’ 十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.9.1.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 4203 4103 1E03 1F00’十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0100 0010 0000 0011	联机PIN	1	如果终端支持	应用后续的
0100 0001 0000 0011	脱机PIN	2	如果终端支持	应用后续的
0001 1110 0000 0011	签名	3	如果终端支持	持卡人验证失败
0001 1111 0000 0000	不需要持卡人验证	4	总是	不会失败

4.9.1.13 动态数据对象列表 (DDOL)

‘9F37 04’十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度
不可预知数	9F37	4

4.9.1.14 应用缺省行为

‘C000’ 十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持卡片与发卡行认证和授权控制处理。

4.9.2 电子现金—签名

4.9.2.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
电子现金余额	n	‘9F 79’	6	**初始设置为 0**	保存了可供脱机消费的剩余总额。				
电子现金余额上限	n	‘9F 77’	6	**发卡行模板**	表示在电子现金应用中，持卡人可脱机消费的最大累积额度，也即卡片充值所能达到的上限。			✔	
电子现金发卡行授权码	an	‘9F 74’	6	**ECC001**	卡片上用于标识批准电子现金交易的代码。	✔			✔
电子现金单笔交易限额	n	‘9F 78’	6	**发卡行模板**	卡片上单笔电子现金交易额的上限，用于控制单笔电子现金交易风险。			✔	
电子现金重置阈值	n	‘9F 6D’	6	**发卡行模板**	触发卡片进行自动充值的可用余额下限。			✔	
处理选项数据对象列表(PDOL)	b	‘9F 38’	9	**9F7A 01 9F02 06 5F2A 02** *详见 4.9.2.2*	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）。	✔			✔
持卡人验证方法(CVM)列表	b	‘8E’	12	**0000 0000 0000 0000 1E03 1F00** *详见 4.9.2.3*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
脱机 PIN	cn	_	2-6	发卡行提供	在卡片个人化时，由发卡行写入卡片				
PIN 尝试限制数	b	–	1	**发卡行模板**	持卡人可以尝试输入不正确的 PIN 的次数。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
PIN 尝试次数计数器	b	'9F 17'	1	**初始化为0，在个人化的过程中，设置成 PIN 尝试限制数**	等于 PIN 尝试限制数。				
发卡行行为代码(IAC)-拒绝	b	'9F 0E'	5	**00 10 80 00 00** *详见 4.9.2.4*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	'9F 0F'	5	**D8 68 3C F8 00** *详见 4.9.2.4*	指定交易联机上送的条件。	✔			✔
发卡行行为代码(IAC)-缺省	b	'9F 0D'	5	**D8 60 3C A8 00** *详见 4.9.2.4*	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。	✔			✔

4.9.2.2 处理选项数据对象列表(PDOL)

'9F7A 01 9F02 06 5F2A 02' 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
电子现金终端支持指示器	9F7A	1
授权金额	9F02	6
交易货币代码	5F2A	2

4.9.2.3 持卡人验证方法(CVM)列表

'0000 0000 0000 0000 1E03 1F00' 十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0001 1110 0000 0011	签名	1	如果终端支持	CVM处理过程失败
0001 1111 0000 0000	不需要持卡人验证	2	总是	不会失败

4.9.2.4 发卡行行为代码 (IAC)(拒绝、联机和缺省)

'00 10 80 00 00' 十六进制（发卡行行为代码-拒绝）

‘D8 68 3C F8 00’ 十六进制（发卡行行为代码-联机）

‘D8 60 3C A8 00’ 十六进制（发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话 脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**1**	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	**1**	**1**
要求输入PIN但密码键盘不存在或不工作	0	**1**	**1**
要求输入PIN，密码键盘存在，但未输入PIN	0	**1**	**1**
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.9.3 非接触式 IC 卡支付—fDDA，应用密文版本 01，小额检查

4.9.3.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片附加处理	b	‘9F 68’	4	**99 00 F0 00** *详见 4.9.3.4*	指出卡片处理需求和参数选择。				
卡片持卡人验证方法限额	n	‘9F 6B’	6	**发卡行模板**	如果出现，表示当卡片和终端货币类型匹配且一个非接触交易超过这个值，则需要由卡片提供 CVM。 目前 qPBOC 支持两种 CVM：联机 PIN 和签名。			✔	
卡片内部指示器	b	_	2	**初始设置为 0**	用于控制 qPBOC 卡片内部过程。				
卡片交易属性	b	‘9F 6C’	2	**初始设置为 00 00** *详见 4.9.3.5*	主要用于向终端指明卡片要求的 CVM。				
脱机消费可用余额	n	‘9F 5D’	6	**初始设置为 1**	一个计算域，可用于终端显示卡片的脱机可用额度、或用于发卡行风险管控。				
应用交互特征 (AIP)	b	‘82’	2	**7C00** *详见 4.9.3.2*	说明此应用中卡片支持的功能。	✔			
处理选项数据对象列表 (PDOL)	b	‘9F 38’	24	**9F66 04 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04** *详见 4.9.3.3*	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）。	✔			✔

4.9.3.2 应用交互特征(AIP)设置

‘7C00’ 十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA

字节	位	值	含义
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	00000000	RFU

4.9.3.3 处理选项数据对象列表(PDOL)

‘9F66 04 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
终端交易属性	9F66	4
授权金额	9F02	6
其它金额	9F03	6
终端国家代码	9F1A	2
终端验证结果（TVR）	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4

4.9.3.4 卡片附加处理

‘99 00 F0 00’十六进制

字节	位	值	含义
1	8	1	支持小额检查
1	7	0	不支持小额和CTTA检查
1	6	0	不支持小额或CTTA检查
1	5	1	支持新卡检查
1	4	1	支持PIN重试次数超过检查
1	3	0	不允许货币不匹配的脱机交易
1	2	0	卡片不优先选择接触式PBOC联机

字节	位	值	含义
1	1	1	返回脱机消费可用额度
2	8	0	不支持预付
2	7	0	允许不匹配货币的交易
2	6	0	如果是新卡且读卡器仅支持脱机，不拒绝交易
2	5-1	00000	RFU
3	8	1	匹配货币的交易支持联机PIN
3	7	1	不匹配货币的交易支持联机PIN
3	6	1	对于不匹配货币交易，卡要求CVM
3	5	1	支持签名
3	4-1	0000	RFU
4	8-1	00000000	RFU

4.9.3.5 卡片交易属性

‘00 00’十六进制

字节	位	值	含义
1	8	0	不需要联机PIN
1	7	0	不需要签名
1	6	0	如果脱机数据认证失败且终端可联机，不要求联机
1	5	0	如果脱机数据认证失败且终端支持接触式PBOC，不终止
1	4-1	0000	RFU
2	8-1	00000000	RFU

4.10 模板 13—贷记卡+电子现金+非接触式 IC 卡支付（1）

4.10.1 标准 PBOC—贷记卡—DDA，联机 PIN,发卡行认证，和授权控制

4.10.1.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征(AIP)	b	‘82’	2	**7C00** *详见 4.10.1.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	‘87’	1	**01** *详见 4.10.1.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器(ATC)	b	‘9F36’	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	‘9F08’	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.10.1.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				
动态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				
发卡行认证指示位	b	‘9F56’	1	**00 或 80 推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（’80’）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			
日志格式	b	‘9F4F’	Var.	**9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602** *详见 4.10.1.5*	列出日志记录中数据对象的标签和长度	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板 推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器（国际-货币）	b	–	1	**初始设置为 0**	国际脱机交易计数器。当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
累计交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限 (LCOL)	b	‘9F58’	1	**发卡行模板 推荐值 0**	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。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易上限 (UCOL)	b	'9F59'	1	**发卡行模板推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		
卡片风险管理数据对象列表 1 (CDOL1)	b	'8C'	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见 4.10.1.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔
卡片风险管理数据对象列表 2 (CDOL2)	b	'8D'	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见 4.10.1.7*	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），包括：发卡行返回码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔
密文信息数据	b	'9F27'	1	初始设置为 0	表明卡片返回的密文类型	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**00 10 00 00 00** *详见 4.10.1.8*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 9C F8 00** *详见 4.10.1.8*	指定交易联机上送的条件。	✔			✔
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 9C A8 00** *详见 4.10.1.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	7	**07_ _ 01 03 00 00 00 01 0A 01** *详见 4.10.1.9*	在一个联机交易中，要传送到发卡行的专有应用数据。(一个分散密钥索引（DKI))		✔		
发卡行国家代码	b	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔
首选语言	ans	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔
应用标识符(AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.10.1.10*	注册应用提供商标识（RID）和专用标识符扩展： **A0 00 00 03 33 01 01 02** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样) ， 01 01 02 表明 PBOC 贷记应用。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用标签	ans	‘50’	1-16	发卡行模板 *详见 4.10.1.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.10.111*	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。 用于提供更灵活的卡片服务控制（类似服务代码）。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
磁条 2 等效数据	var.	‘57’	最大 19	磁条数据文件提供	等效磁条 2 数据（格式不一致） 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期（5F24）一致			✔	✔
持卡人验证方法(CVM)列表	b	‘8E’	14	**0000 0000 0000 0000 4203 1E03 1F00** *详见 4.10.1.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
CA 公钥索引(PKI)	b	‘8F’	1	发卡行模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✔		✔
发卡行公钥(IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证		✔		✔
发卡行公钥余数 (如果需要)	b	‘92’	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分		✔		✔
发卡行公钥指数	b	‘9F32’	1 to N_I/4	发卡行模板	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		✔		✔
签名的静态应用数据（SAD）	b	‘93’	var.	发卡行模板	用发卡行签名的应用数据，在 SDA 过程中由终端验证			✔	✔
IC 卡公钥证书	b	‘9F46’	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔
IC 卡公钥指数	b	‘9F47’	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
IC 卡公钥余数	b	‘9F48’	N_{IC} –N_I+42	发卡行模板	没有放入 IC 卡公钥证书的 IC 卡公钥部分			✔	✔
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	
动态数据认证数据对象列表(DDOL)	b	‘9F49’	最大 252	发卡行模板 *详见 4.10.1.13*	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。		✔		✔
应用缺省行为(ADA)	b	‘9F52’	2	**C000** *详见 4.10.1.14*	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	✔			
子密钥(UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥(ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥(MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.10.1.2 应用交互特征(AIP)设置

'7C00'十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.10.1.3 应用优先指示器

'01'十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.10.1.4 卡片内部数据

卡片内部数据	保留	初始值	Tag

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位 发卡行认证失败指示位	1 bit 1 bit	0 0	- -
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits	00	-
连续脱机交易下限	1 字节	发卡行模板 = 0	‘9F58’
连续脱机交易上限	1 字节	发卡行模板 > =连续脱机交易下限，=0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额数（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板 = 0	‘9F54’
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数（国内），=0	‘9F5C’

注： 为了支持DDA,SDA,发卡行认证和授权控制处理,带阴影的指示位应当在个人化时设置.

4.10.1.5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.10.1.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.10.1.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.10.1.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

’00 10 00 00 00’ 十六进制 （发卡行行为代码-拒绝）

‘D8 68 9C F8 00’ 十六进制 （发卡行行为代码-联机）

‘D8 60 9C A8 00’ 十六进制 （发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话 脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**0**	**1**	**1**
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	**0**	1	1
要求输入PIN，密码键盘存在，但未输入PIN	**0**	**1**	**1**

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话 脱机拒绝
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.10.1.9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1	0A	发卡行自定义数据(IDD)-自定义数据长度 (最长15)
10	8-1	01	IDD ID
11-15	8-1	初始设置为0	金额域
16-19	8-1	初始设置为0	MAC
20-24	8-1		其它的发卡行自定义数据

4.10.1.10 应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	**专用标识符扩展(PIX)**	**卡种**
A0 00 00 03 33	01 01 02	PBOC CREDIT

4.10.1.11 应用用途控制

'FF00' 十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.10.1.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 0000 4203 1E03 1F00’十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0100 0010 0000 0011	联机PIN	1	如果终端支持	应用后续的
0001 1110 0000 0011	签名（纸上）	2	如果终端支持	持卡人验证失败
0001 1111 0000 0000	不需要持卡人验证	3	总是	不会失败

4.10.1.13 动态数据对象列表 (DDOL)

‘9F37 04’十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度
不可预知数	9F37	4

4.10.1.14 应用缺省行为

‘C000’十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持卡片与发卡行认证和授权控制处理。

4.10.2 电子现金—签名

4.10.2.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
电子现金余额	n	‘9F 79’	6	**初始设置为 0**	保存了可供脱机消费的剩余总额。				
电子现金余额上限	n	‘9F 77’	6	**发卡行模板**	表示在电子现金应用中，持卡人可脱机消费的最大累积额度，也即卡片充值所能达到的上限。			✔	
电子现金发卡行授权码	an	‘9F 74’	6	**ECC001**	卡片上用于标识批准电子现金交易的代码。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
电子现金单笔交易限额	n	‘9F 78’	6	**发卡行模板**	卡片上单笔电子现金交易额的上限，用于控制单笔电子现金交易风险。			✔	
电子现金重置阈值	n	‘9F 6D’	6	**发卡行模板**	触发卡片进行自动充值的可用余额下限。			✔	
处理选项数据对象列表(PDOL)	b	‘9F 38’	9	**9F7A 01 9F02 06 5F2A 02** *详见 4.10.2.2*	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）。	✔			✔
持卡人验证方法(CVM)列表	b	‘8E’	12	**0000 0000 0000 0000 1E03 1F00** *详见 4.10.2.3*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
脱机 PIN	cn	_	2-6	发卡行提供	在卡片个人化时，由发卡行写入卡片				
PIN 尝试限制数	b	–	1	**发卡行模板**	持卡人可以尝试输入不正确的 PIN 的次数。		✔		
PIN 尝试次数计数器	b	‘9F 17’	1	**初始化为 0，在个人化的过程中，设置成 PIN 尝试限制数**	等于 PIN 尝试限制数。				
发卡行行为代码(IAC)-拒绝	b	‘9F 0E’	5	**00 10 80 00 00** *详见 4.10.2.4*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	‘9F 0F’	5	**D8 68 3C F8 00** *详见 4.10.2.4*	指定交易联机上送的条件。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡行行为代码(IAC)-缺省	b	'9F 0D'	5	**D8 60 3C A8 00** *详见 4.10.2.4*	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。	✔			✔

4.10.2.2 处理选项数据对象列表(PDOL)

'9F7A 01 9F02 06 5F2A 02' 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
电子现金终端支持指示器	9F7A	1
授权金额	9F02	6
交易货币代码	5F2A	2

4.10.2.3 持卡人验证方法(CVM)列表

'0000 0000 0000 0000 1E03 1F00' 十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0001 1110 0000 0011	签名	1	如果终端支持	CVM处理过程失败
0001 1111 0000 0000	不需要持卡人验证	2	总是	不会失败

4.10.2.4 发卡行行为代码 (IAC)(拒绝、联机和缺省)

'00 10 80 00 00' 十六进制 (发卡行行为代码-拒绝)

'D8 68 3C F8 00' 十六进制 (发卡行行为代码-联机)

'D8 60 3C A8 00' 十六进制 (发卡行行为代码-缺省)

条件	结果		
	IAC拒绝- 脱机拒绝	IAC 联机 – 要求联机	IAC 缺省 – 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**1**	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	**1**	**1**
要求输入PIN但密码键盘不存在或不工作	0	**1**	**1**
要求输入PIN，密码键盘存在，但未输入PIN	0	**1**	**1**
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.10.3 非接触式 IC 卡支付—fDDA，应用密文版本 01，小额检查

4.10.3.1 卡片数据对象

数据名称	**在卡片上的数据格式**	**Tag**	**数据长度 (bytes)**	**值** (十六进制)	**描述**	**模板缺省设置**	**发卡行通用数据**	**卡或持卡人特殊数据**	**数据存储在文件记录中**
卡片附加处理	b	‘9F68’	4	**99 00 F0 00** *详见 4.10.3.4*	指出卡片处理需求和参数选择。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片持卡人验证方法限额	n	‘9F6B’	6	**发卡行模板**	如果出现，表示当卡片和终端货币类型匹配且一个非接触交易超过这个值，则需要由卡片提供 CVM。 目前 qPBOC 支持两种 CVM：联机 PIN 和签名。			✔	
卡片内部指示器	b	_	2	**初始设置为 0**	用于控制 qPBOC 卡片内部过程。				
卡片交易属性	b	‘9F6C’	2	**初始设置为 00 00** *详见 4.10.3.5*	主要用于向终端指明卡片要求的 CVM。				
脱机消费可用余额	n	‘9F5D’	6	**初始设置为 1**	一个计算域，可用于终端显示卡片的脱机可用额度、或用于发卡行风险管控。				
应用交互特征(AIP)	b	‘82’	2	**7C00** *详见 4.10.3.2*	说明此应用中卡片支持的功能。	✔			
处理选项数据对象列表(PDOL)	b	‘9F38’	24	**9F66 04 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04** *详见 4.10.3.3*	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）。	✔			✔

4.10.3.2 应用交互特征(AIP)设置

‘7C00’ 十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持fDDA

字节	位	值	含义
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	00000000	RFU

4.10.3.3 处理选项数据对象列表(PDOL)

‘9F66 04 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
终端交易属性	9F66	4
授权金额	9F02	6
其它金额	9F03	6
终端国家代码	9F1A	2
终端验证结果（TVR）	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4

4.10.3.4 卡片附加处理

‘99 00 F0 00’十六进制

字节	位	值	含义
1	8	1	支持小额检查
1	7	0	不支持小额和CTTA检查
1	6	0	不支持小额或CTTA检查
1	5	1	支持新卡检查
1	4	1	支持PIN重试次数超过检查
1	3	0	不允许货币不匹配的脱机交易
1	2	0	卡片不优先选择接触式PBOC联机

字节	位	值	含义
1	1	1	返回脱机消费可用额度
2	8	0	不支持预付
2	7	0	允许不匹配货币的交易
2	6	0	如果是新卡且读卡器仅支持脱机，不拒绝交易
2	5-1	00000	RFU
3	8	1	匹配货币的交易支持联机PIN
3	7	1	不匹配货币的交易支持联机PIN
3	6	1	对于不匹配货币交易，卡要求CVM
3	5	1	支持签名
3	4-1	0000	RFU
4	8-1	00000000	RFU

4.10.3.5 卡片交易属性

‘00 00’十六进制

字节	位	值	含义
1	8	0	不需要联机PIN
1	7	0	不需要签名
1	6	0	如果脱机数据认证失败且终端可联机，不要求联机
1	5	0	如果脱机数据认证失败且终端支持接触式PBOC，不终止交易
1	4-1	0000	RFU
2	8-1	00000000	RFU

4.11 模板 14—贷记卡+电子现金+非接触式 IC 卡支付（2）

4.11.1 标准 PBOC—贷记卡—DDA, 签名,发卡行认证, 和授权控制

4.11.1.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征(AIP)	b	‘82’	2	**7C00** *详见 4.11.1.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	‘87’	1	**01** *详见 4.11.1.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			
应用交易计数器(ATC)	b	‘9F36’	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	‘9F08’	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.11.1.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				
动态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				
发卡行认证指示位	b	‘9F56’	1	**00 或 80 推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（’80’）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			
日志格式	b	‘9F4F’	Var.	**9A03 9F2103 9F0206 9F0306 9F1A02 5F2A02 9F4E14 9C01 9F3602** *详见 4.11.1.5*	列出日志记录中数据对象的标签和长度	✔			

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板 推荐值 0**	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		✔		
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器（国际-货币）	b	–	1	**初始设置为 0**	国际脱机交易计数器。当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
累计交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板 推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限(LCOL)	b	‘9F58’	1	**发卡行模板 推荐值 0**	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。		✔		
连续脱机交易上限(UCOL)	b	‘9F59’	1	**发卡行模板 推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片风险管理数据对象列表1(CDOL1)	b	‘8C’	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见4.11.1.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔
卡片风险管理数据对象列表2(CDOL2)	b	‘8D’	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见4.11.1.7*	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），包括：发卡行返回码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔
密文信息数据	b	‘9F27’	1	初始设置为0	表明卡片返回的密文类型	✔			
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**0010 0000 00** *详见4.11.1.8*	指定交易不进行联机直接拒绝的条件。	✔			✔
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 04 F8 00** *详见4.11.1.8*	指定交易联机上送的条件。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 04 A8 00** *详见 4.11.1.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07_ _ 01 03 00 00 00 01 0A 01** *详见 4.11.1.9*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		
发卡行国家代码	b	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔
首选语言	ans	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔
应用标识符(AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.11.1.10*	注册应用提供商标识（RID）和专用标识符扩展： **A0 00 00 03 33 01 01 02** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样) ， 01 01 02 表明 PBOC 贷记应用。				
应用标签	ans	‘50’	1-16	发卡行模板 *详见 4.11.1.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.11.1.11*	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。 用于提供更灵活的卡片服务控制（类似服务代码）。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
磁条 2 等效数据	var.	'57'	最大 19	磁条数据文件提供	等效磁条 2 数据(格式不一致) 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期(5F24)一致			✔	✔
持卡人验证方法(CVM)列表	b	'8E'	14	**0000 0000 0000 0000 1E03 0203 1F00** *详见 4.11.1.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意: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。	✔			✔
CA 公钥索引(PKI)	b	'8F'	1	发卡行模板	在 SDA 或 DDA 过程中,和 RID 一起使用,用来标识 CA 公钥		✔		✔
发卡行公钥(IPK)证书	b	'90'	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证		✔		✔
发卡行公钥余数(如果需要)	b	'92'	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分		✔		✔
发卡行公钥指数	b	'9F32'	1 to N_I/4	发卡行模板	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		✔		✔
签名的静态应用数据(SAD)	b	'93'	var.	发卡行模板	用发卡行签名的应用数据,在 SDA 过程中由终端验证			✔	✔
IC 卡公钥证书	b	'9F46'	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔
IC 卡公钥指数	b	'9F47'	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔
IC 卡公钥余数	b	'9F48'	N_{IC} –N_I+42	发卡行模板	没有放入 IC 卡公钥证书的 IC 卡公钥部分			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	
动态数据认证数据对象列表(DDOL)	b	‘9F49’	最大252	发卡行模板 *详见 4.11.1.13*	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。		✔		✔
应用缺省行为(ADA)	b	‘9F52’	2	**C000** *详见 4.11.1.14*	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	✔			
子密钥(UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥(ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥(MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.11.1.2 应用交互特征(AIP)设置

'7C00'十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.11.1.3 应用优先指示器

'01'十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.11.1.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位 发卡行认证失败指示位	1 bit 1 bit	0 0	- -
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits	00	-
连续脱机交易下限	1 字节	发卡行模板 = 0	‘9F58’
连续脱机交易上限	1 字节	发卡行模板 >= 连续脱机交易下限，=0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额数（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板 = 0	‘9F54’
累计脱机交易上限	6 字节	>=累计脱机交易金额限制数（国内），=0	‘9F5C’

注： 为了支持DDA, SDA, 发卡行认证和授权控制处理, 带阴影的指示位应当在个人化时设置.

4. 11. 1. 5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.11.1.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.11.1.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.11.1.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

’00 10 00 00 00’ 十六进制 （发卡行行为代码-拒绝）

‘D8 68 04 F8 00’ 十六进制 （发卡行行为代码-联机）

‘D8 60 04 A8 00’ 十六进制 （发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话 脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	0	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	0	0	0
要求输入PIN，密码键盘存在，但未输入PIN	0	0	0

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
输入联机PIN	0	**1**	**1**
RFU	00	00	00
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4. 11. 1. 9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1	0A	发卡行自定义数据(IDD)-自定义数据长度 (最长15)
10	8-1	01	IDD ID
11-15	8-1	初始设置为0	金额域
16-19	8-1	初始设置为0	MAC
10-24	8-1		其它的发卡行自定义数据

4. 11. 1. 10 应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	**专用标识符扩展(PIX)**	**卡种**
A0 00 00 03 33	01 01 02	PBOC CREDIT

4. 11. 1. 11 应用用途控制

'FF00' 十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.11.1.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 0000 1E03 0203 1F00’ 十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0001 1110 0000 0011	签名	1	如果终端支持	CVM处理过程失败
0000 0010 0000 0011	联机PIN	2	如果终端支持	CVM处理过程失败
0001 1111 0000 0000	不需要持卡人验证	3	总是	不会失败

4.11.1.13 动态数据对象列表 (DDOL)

‘9F37 04’ 十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度
不可预知数	9F37	4

4.11.1.14 应用缺省行为

‘C000’十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持卡片与发卡行认证和授权控制处理。

4.11.2 电子现金—签名

4.11.2.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
电子现金余额	n	‘9F79’	6	**初始设置为0**	保存了可供脱机消费的剩余总额。				
电子现金余额上限	n	‘9F77’	6	**发卡行模板**	表示在电子现金应用中，持卡人可脱机消费的最大累积额度，也即卡片充值所能达到的上限。			✔	
电子现金发卡行授权码	an	‘9F74’	6	**ECC001**	卡片上用于标识批准电子现金交易的代码。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
电子现金单笔交易限额	n	‘9F78’	6	**发卡行模板**	卡片上单笔电子现金交易额的上限，用于控制单笔电子现金交易风险。			✔	
电子现金重置阈值	n	‘9F6D’	6	**发卡行模板**	触发卡片进行自动充值的可用余额下限。			✔	
处理选项数据对象列表(PDOL)	b	‘9F38’	9	**9F7A 01 9F02 06 5F2A 02** *详见 4.11.2.2*	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）。	✔			✔
持卡人验证方法（CVM）列表	b	‘8E’	12	**0000 0000 0000 0000 1E03 1F00** ***详见 4.11.2.3***	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔

4.11.2.2 处理选项数据对象列表(PDOL)

‘9F7A 01 9F02 06 5F2A 02’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
电子现金终端支持指示器	9F7A	1
授权金额	9F02	6
交易货币代码	5F2A	2

4.11.2.3 持卡人验证方法列表(CVM)

‘0000 0000 0000 0000 1E03 1F00’十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0001 1110 0000 0011	签名（纸上）	1	如果终端支持	持卡人验证失败
0001 1111 0000 0000	不需要持卡人验证	2	总是	不会失败

4.11.3 非接触式 IC 卡支付—fDDA，应用密文版本 17，小额检查

4.11.3.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片附加处理	b	‘9F68’	4	**91 00 B0 00** *详见 4.11.3.4*	指出卡片处理需求和参数选择。				
卡片持卡人验证方法限额	n	‘9F6B’	6	**发卡行模板**	如果出现，表示当卡片和终端货币类型匹配且一个非接触交易超过这个值，则需要由卡片提供 CVM。 目前 qPBOC 支持两种 CVM：联机 PIN 和签名。			✔	
卡片内部指示器	b	_	2	**初始设置为 0**	用于控制 qPBOC 卡片内部过程。				
卡片交易属性	b	‘9F6C’	2	**初始设置为 00 00** *详见 4.11.3.5*	主要用于向终端指明卡片要求的 CVM。				
脱机消费可用余额	n	‘9F5D’	6	**初始设置为 1**	一个计算域，可用于终端显示卡片的脱机可用额度、或用于发卡行风险管控。				
应用交互特征 (AIP)	b	‘82’	2	**7C00** *详见 4.11.3.2*	说明此应用中卡片支持的功能。	✔			

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
处理选项数据对象列表(PDOL)	b	‘9F38’	12	**9F6604 9F0206 9F3704 5F2A02** *详见4.11.3.3*	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）。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07 _ 17 03 00 00 00 01 0A 01** _ _ *详见4.11.3.6*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		

4.11.3.2 应用交互特征(AIP)设置

‘7C00’十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持fDDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	00000000	RFU

4.11.3.3 处理选项数据对象列表(PDOL)

‘9F66 04 9F02 06 9F37 04 5F2A 02’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
终端交易属性	9F66	4
授权金额	9F02	6
不可预知数	9F37	4
交易货币代码	5F2A	2

4.11.3.4 卡片附加处理

‘91 00 B0 00’十六进制

字节	位	值	含义
1	8	1	支持小额检查
1	7	0	不支持小额和CTTA检查
1	6	0	不支持小额或CTTA检查
1	5	1	支持新卡检查
1	4	0	不支持PIN重试次数超过检查
1	3	0	不允许货币不匹配的脱机交易
1	2	0	卡片不优先选择接触式PBOC联机
1	1	1	返回脱机消费可用额度
2	8	0	不支持预付
2	7	0	允许不匹配货币的交易
2	6	0	如果是新卡且读卡器仅支持脱机，不拒绝交易
2	5-1	00000	RFU
3	8	1	匹配货币的交易支持联机PIN
3	7	0	不匹配货币的交易不支持联机PIN
3	6	1	对于不匹配货币交易，卡要求CVM
3	5	1	支持签名
3	4-1	0000	RFU
4	8-1	00000000	RFU

4.11.3.5 卡片交易属性

‘00 00’十六进制

字节	位	值	含义
1	8	0	不需要联机PIN
1	7	0	不需要签名
1	6	0	如果脱机数据认证失败且终端可联机，不要求联机
1	5	0	如果脱机数据认证失败且终端支持接触式PBOC，不终止
1	4-1	0000	RFU
2	8-1	00000000	RFU

4.11.3.6 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	17(十六进制)	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1	0A	发卡行自定义数据(IDD)-自定义数据长度 (最长15)
10	8-1	01	IDD ID
11-15	8-1	初始设置为0	金额域
16-19	8-1	初始设置为0	MAC
20-24	8-1		其它的发卡行自定义数据

4.12 模板 15—准贷记卡+电子现金+非接触式 IC 卡支付

4.12.1 标准 PBOC—准贷记卡—DDA,联机 PIN,发卡行认证,和授权控制

4.12.1.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交互特征(AIP)	b	‘82’	2	**7C00** *详见 4.7.2*	说明此应用中卡片支持的功能。	✔			
应用优先指示器	b	‘87’	1	**01** *详见 4.7.3*	如果卡片中有多个应用，指出同一目录中的应用的优先级。	✔			

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用交易计数器(ATC)	b	‘9F36’	2	**初始设置为 0**	记录个人化以后交易处理的次数。				
应用版本号	b	‘9F08’	2	**初始化好的。** 00 20	支付系统给应用分配的版本号，为以后增加新功能提供一种移值的途径。终端会比较自己与卡片的版本号。	✔			✔
卡片内部数据 *(下面一个表概述了这些内部指示器的用法.)*	var.	–		*详见 4.7.4*	用于发卡行提供交易处理信息和影响交易结果的卡片内部计数器和指示器。				
上次联机交易未完成指示位	b	–	1 bit	**初始设置为 0**	表明上次联机交易没有完成。				
卡片请求联机指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易联机时设置。				
卡片请求脱机拒绝指示位	b	–	1 bit	**初始设置为 0**	在交易处理过程中，当卡片决定交易拒绝时设置。				
发卡行认证失败指示位	b	–	1 bit	**初始设置为 0**	表明上次交易出现的发卡行认证错误的情况。				
静态数据认证（SDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 SDA 是否失败。				
动态数据认证（DDA）失败指示位	b	–	1 bit	**初始设置为 0**	标明当上次交易拒绝时 DDA 是否失败。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡行认证指示位	b	‘9F56’	1	**00 或 80** **推荐 00**	交易联机后控制交易如何处理的指示器。发卡行认证可以是可选（’00’）或强制（’80’）。如果是强制但没有授权响应密文返回，则发卡行可以选择不管联机返回报文结果如何，拒绝本次交易。		✔		
上次联机应用交易计数器（ATC）寄存器	b	‘9F13’	2	**初始设置为 0**	上次联机上送交易时的 ATC 值				
日志入口	b	‘9F4D’	2	**0B 0A**	提供日志文件的 SFI 和日志文件记录个数，PBOC 规范提供推荐值：0B 0A 字节 1: 循环交易日志文件的 SFI，为 11（十进制） 字节 2: 交易日志文件中的记录个数，为 10（十进制）	✔			
日志格式	b	‘9F4F’	Var.	**9A03** **9F2103** **9F0206** **9F0306** **9F1A02** **5F2A02** **9F4E14** **9C01** **9F3602** *详见 4.7.5*	列出日志记录中数据对象的标签和长度	✔			
连续脱机交易限制数（国际-货币）	b	‘9F53’	1	**发卡行模板推荐值 0**	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		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
连续脱机交易限制数（国际-国家）	b	‘9F72’	1	**发卡行模板，推荐值 0**	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		✔		
累计交易计数器(国际-货币）	b	–	1	**初始设置为 0**	国际脱机交易计数器。当计数器超过累计脱机交易限制数时，卡片请求交易联机。				
累计脱机交易金额(国内)	n	–	6	**初始设置为 0**	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				
累计脱机交易金额限制数	n	‘9F54’	6	**发卡行模板推荐值 00 00 00 00 00 00**	累计脱机交易金额的最大限制数。超过交易请求联机		✔		
累计脱机交易金额上限	n	‘9F5C’	6	**发卡行模板推荐值 00 00 00 00 00 00**	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。		✔		
连续脱机交易下限 (LCOL)	b	‘9F58’	1	**发卡行模板推荐值 0**	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。		✔		
连续脱机交易上限 (UCOL)	b	‘9F59’	1	**发卡行模板推荐值 0**	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，超过此值如果交易要求联机但联机不成功，则拒绝交易。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片风险管理数据对象列表1 (CDOL1)	b	‘8C’	27	**9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03 9F4E 14** *详见4.7.6*	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。用于支持密文版本01和授权控制处理过程。内容是终端数据对象（标签和长度），数据包括：授权金额，其他金额，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，终端不可预知数，交易时间和商户名称。	✔			✔
卡片风险管理数据对象列表2 (CDOL2)	b	‘8D’	26	**8A02 9F02 069F 0306 9F1A 0295 055F 2A02 9A03 9C01 9F37 04 9F21 03** *详见4.7.7*	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），包括：发卡行返回码，授权金额，其他金额，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，终端不可预知数和交易时间。	✔			✔
密文信息数据	b	‘9F27’	1	初始设置为0	表明卡片返回的密文类型	✔			
发卡行行为代码(IAC)-拒绝	b	‘9F0E’	5	**00 10 98 00 00** *详见4.8.7*	指定交易不进行联机直接拒绝的条件。	✔			✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
发卡行行为代码(IAC)-联机	b	‘9F0F’	5	**D8 68 04 F8 00** *详见 4.7.8*	指定交易联机上送的条件。	✔			✔
发卡行行为代码(IAC)-缺省	b	‘9F0D’	5	**D8 60 04 A8 00** *详见 4.7.8*	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。	✔			✔
发卡行应用数据	b	‘9F10’	7	**07_ _ 01 03 00 00 00 01** *详见 4.7.9*	在一个联机交易中，要传送到发卡行的专有应用数据。（一个分散密钥索引（DKI））		✔		
发卡行国家代码	n	‘5F28’	2	**发卡行模板**	指明卡片发行者的国家。		✔		✔
首选语言	an	‘5F2D’	2	**发卡行模板**	当终端支持多种语言时，终端根据发卡行首选语言显示终端信息。		✔		
应用货币码	n	‘9F51’		**发卡行模板**	发卡行的国内货币。		✔		✔
应用标识符(AID)	b	‘4F’	5-16	**初始化好的。** *详见 4.7.10*	注册应用提供商标识（RID）和专用标识符扩展，例如： **A0 00 00 03 33 01 01 03** A0 00 00 03 33 确定 PBOC 注册应用提供商 (所有的卡片都一样) ， 01 01 03 表明 PBOC 准贷记应用。				
应用标签	ans	‘50’	1-16	发卡行模板 *详见 4.7.10*	终端显示给消费者一个可选应用列表的时候应用的名称。		✔		

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
应用用途控制	b	‘9F07’	2	**FF 00** *详见 4.7.11*	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。 用于提供更灵活的卡片服务控制（类似服务码）。‘2’ = hex **FF00** 是模板缺省值，卡片仅支持国内功能时设为‘6’ = hex **AB00**。	✔			✔
应用主帐户序列号	n	‘5F34’	1	发卡行在磁条数据文件中提供	用来表示卡片中使用同一个账号的不同应用			✔	✔
持卡人姓名	ans	‘5F20’	2-26	从磁条数据文件提供	等同磁条中持卡人姓名。			✔	✔
持卡人姓名扩展	ans	‘9F0B’	1－19	从磁条数据文件提供	如果持卡人姓名大于 26 字节，多出部分放在此数据元中。			✔	✔
持卡人证件号	an	‘9F61’	1-40	从磁条数据文件提供	持卡人证件号			✔	✔
持卡人证件类型	cn	‘9F62’	1	从磁条数据文件提供	表明持卡人证件类型			✔	✔
应用失效日期	n	‘5F24’	3	磁条数据文件提供	卡片应用失效日期			✔	✔
应用生效日期	n	‘5F25’	3	发卡行模板	卡片中应用启用日期。		✔		✔
应用主帐户(PAN)	cn	‘5A’	最大 10	磁条数据文件提供	等同磁条上的应用主帐户。			✔	✔
服务码	n	‘5F30’	2	磁条数据文件提供	和磁条中定义的服务码相同。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
磁条 1 自定义数据	ans	‘9F1F’	var.	磁条数据文件提供	与磁条上的磁条 1 自定义数据相同			✔	✔
磁条 2 等效数据	var.	‘57’	最大 19	磁条数据文件提供	等效磁条 2 数据（格式不一致） 磁条 2 等效数据中的有效期要求与 IC 卡内的应用失效日期（5F24）一致			✔	✔
持卡人验证方法(CVM)列表	b	‘8E’	14	**0000 0000 0000 0000 0203 1E03 1F00** *详见 4.7.12*	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔
CA 公钥索引(PKI)	b	‘8F’	1	发卡行模板	在 SDA 或 DDA 过程中，和 RID 一起使用，用来标识 CA 公钥		✔		✔
发卡行公钥(IPK)证书	b	‘90’	N_{CA}	发卡行模板	CA 认证过的发卡行公钥。用于脱机数据认证		✔		✔
发卡行公钥余数 (如果需要)	b	‘92’	N_I -N_{CA}+36	发卡行模板	没有放入发卡行公钥证书中的发卡行公钥部分		✔		✔
发卡行公钥指数	b	‘9F32’	1 to N_I/4	发卡行模板	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		✔		✔
签名的静态应用数据（SAD）	b	‘93’	var.	发卡行模板	用发卡行签名的应用数据，在 SDA 过程中由终端验证。			✔	✔
IC 卡公钥证书	b	‘9F46’	N_I	发卡行模板	发卡行认证过的 IC 卡公钥。			✔	✔

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
IC 卡公钥指数	b	‘9F47’	1 or 3	发卡行模板	IC 卡公钥指数用于验证签名的动态应用数据。			✔	✔
IC 卡公钥余数	b	‘9F48’	N_{IC} –N_I+42	发卡行模板	没有放入 IC 卡公钥证书的 IC 卡公钥部分			✔	✔
IC 卡私钥	b	–	N_{IC}	发卡行模板	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。			✔	
动态数据认证数据对象列表(DDOL)	b	‘9F49’	最大 252	发卡行模板 *详见 4.7.13*	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。		✔		✔
应用缺省行为(ADA)	b	‘9F52’	2	**C000** *详见 4.7.14*	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	✔			
子密钥(UDK) A	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (UDK) B	b	_	8	发卡行模板	由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。			✔	
子密钥 (ENC Key)A	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
子密钥(ENC Key)B	b	_	8	发卡行模板	用于发卡行脚本的加密密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)A	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				
子密钥(MAC Key)B	b	_	8	发卡行模板	用于发卡行脚本的安全报文密钥，由每个发卡行唯一的主密钥分散生成每张卡片唯一的子密钥。				

4.12.1.2 应用交互特征(AIP)设置

'7C00'十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持DDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	0000 0000	RFU

4.12.1.3 应用优先指示器

'01'十六进制

字节	位	值	含义
1	8	0	没有持卡人确认应用可以选择。

字节	位	值	含义
1	7-5	000	RFU
1	4-1	0001	最高优先级

4.12.1.4 卡片内部数据

卡片内部数据	保留	初始值	Tag
联机授权指示位	1 bit	0	-
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位	1 bit	0	-
发卡行认证失败指示位	1 bit	0	-
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits	00	-
连续脱机交易下限	1 字节	发卡行模板 = 0	‘9F58’
连续脱机交易上限	1 字节	发卡行模板 >= 连续脱机交易下限，=0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板 = 0	‘9F54’
累计脱机交易上限	6 字节	发卡行模板 > CTAL	‘9F5C’
卡片内部数据	**保留**	**初始值**	**Tag**
联机授权指示位	1 bit	0	-

卡片内部数据	保留	初始值	Tag
卡片请求ARQC指示位	1 bit	0	-
卡片请求AAC指示位 发卡行认证失败指示位	1 bit 1 bit	0 0	- -
静态数据(SDA)认证失败指示位	1 bit	0	-
动态数据认证(DDA)失败指示位	1 bit	0	-
发卡行脚本失败指示位	1 bit		-
发卡行认证指示位 (bit8 0=可选 1=强制)	1 字节	00或80 推荐00	‘9F56’
发卡行脚本命令计数器	4 bits	00	-
连续脱机交易下限	1 字节	发卡行模板 = 0	‘9F58’
连续脱机交易上限	1 字节	发卡行模板 >= 连续脱机交易下限，=0	‘9F59’
上次联机应用交易计数器（ATC）寄存器	2 字节	0	‘9F13’
连续脱机交易限制数（国际-货币）	1 字节	发卡行模板 =0	‘9F53’
连续脱机交易限制数（国际-国家）	1 字节	发卡行模板 =0	‘9F72’
累计脱机交易计数器（国际）	1 字节	0	-
PIN尝试限制数	1 字节	发卡行模板	-
PIN尝试次数计数器	1 字节	= PIN尝试限制数	‘9F17’
累计脱机交易金额（国内）	6 字节	0	-
累计脱机交易金额限制数（国内）	6 字节	发卡行模板 = 0	‘9F54’
累计脱机交易上限	6 字节	发卡行模板 > CTAL	‘9F5C’

注： 为了支持DDA,SDA,发卡行认证和授权控制处理,带阴影的指示位应当在个人化时设置.

4.12.1.5 日志格式

‘9A 03 9F21 03 9F02 06 9F03 06 9F1A 02 5F2A 02 9F4E 14 9C 01 9F36 02’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
交易日期	9A	3
交易时间	9F21	3

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
交易货币代码	5F2A	2
商户名称	9F4E	20
交易类型	9C	1
应用交易计数器（ATC）	9F36	2

4.12.1.6 卡片风险管理数据对象列表(CDOL)1

‘9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03 9F4E 14’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权金额	9F02	6
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3
商户名称	9F4E	20

4.12.1.7 卡片风险管理数据对象列表(CDOL) 2

‘8A 02 9F02 06 9F03 06 9F1A 02 95 05 5F2A 02 9A 03 9C 01 9F37 04 9F21 03’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
授权响应码	8A	2
授权金额	9F02	6

数据对象名称	Tag(标签)	长度
其他金额	9F03	6
终端国家代码	9F1A	2
终端验证结果	95	5
交易货币代码	5F2A	2
交易日期	9A	3
交易类型	9C	1
不可预知数	9F37	4
交易时间	9F21	3

4.12.1.8 发卡行行为代码 (IAC)(拒绝、联机和缺省)

’00 10 98 00 00’ 十六进制（发卡行行为代码-拒绝）

‘D8 68 04 F8 00’ 十六进制（发卡行行为代码-联机）

‘D8 60 04 A8 00’ 十六进制（发卡行行为代码-缺省）

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
未进行脱机数据认证	0	**1**	**1**
脱机静态数据认证（SDA）失败	0	**1**	**1**
IC卡数据缺失	0	0	0
卡片出现在终端异常文件中	0	**1**	**1**
脱机动态数据认证（DDA）失败	0	**1**	**1**
复合动态数据认证/应用密码生成（CDA）失败	0	0	0
RFU	00	00	00
IC卡和终端应用版本不一致	0	0	0
应用已过期	0	**1**	**1**
应用尚未生效	0	**1**	**1**
卡片不允许所请求的服务	**1**	0	0
新卡	0	**1**	0
RFU	000	000	000
持卡人验证失败	**1**	0	0
未知的CVM	0	0	0
PIN重试次数超限	0	0	0
要求输入PIN但密码键盘不存在或不工作	**1**	0	0
要求输入PIN，密码键盘存在，但未输入PIN	**1**	0	0
输入联机PIN	0	**1**	**1**
RFU	00	00	00

条件	结果		
	IAC拒绝- 脱机拒绝	**IAC 联机 –** 要求联机	**IAC 缺省 –** 如果不能联机的话脱机拒绝
交易超过最低限额	0	**1**	**1**
超过连续脱机交易下限	0	**1**	0
超过连续脱机交易上限	0	**1**	**1**
交易被随机选择联机处理	0	**1**	0
商户要求联机处理	0	**1**	**1**
RFU	000	000	000
使用缺省的TDOL	0	0	0
发卡行认证失败	0	0	0
最后一次GENERATE AC 命令之前脚本处理失败	0	0	0
最后一次GENERATE AC 命令之后脚本处理失败	0	0	0
RFU	0000	0000	0000

4.12.1.9 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	01	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1		如果有发卡行自定义数据的话，自定义数据长度 (最长15)
10-24	8-1		1-15字节的发卡行自定义数据。

4.12.1.10 应用标识符和应用标签

应用标识符 (AID)		应用标签
注册应用提供商标识(RID)	专用标识符扩展(PIX)	卡种
A0 00 00 03 33	01 01 03	PBOC QUASICREDIT

4.12.1.11 应用用途控制

'FF00' 十六进制

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法

字节	b8	b7	b6	b5	b4	b3	b2	B1	用法
1	1	0	0	0	0	0	0	0	国内现金交易有效
1	0	1	0	0	0	0	0	0	国际现金交易有效
1	0	0	1	0	0	0	0	0	国内商品有效
1	0	0	0	1	0	0	0	0	国际商品有效
1	0	0	0	0	1	0	0	0	国内服务有效
1	0	0	0	0	0	1	0	0	国际服务有效
1	0	0	0	0	0	0	1	0	ATM有效
1	0	0	0	0	0	0	0	1	除ATM外的终端有效
2	0	0	0	0	0	0	0	0	允许国内返现
2	0	0	0	0	0	0	0	0	允许国际返现
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU
2	0	0	0	0	0	0	0	0	RFU

注： 表中相应位设置为1，表示该服务是被允许的。此处设置的值是磁条上的服务代码设置为2时的例子，如果设置为6，则只有国内功能被允许。

4.12.1.12 持卡人验证方法(CVM)列表

‘0000 0000 0000 0000 0203 1E03 1F00’ 十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0000 0010 0000 0011	联机PIN	1	如果终端支持	CVM处理过程失败
0001 1110 0000 0011	签名	2	如果终端支持	CVM处理过程失败
0001 1111 0000 0000	不需要持卡人验证	3	总是	不会失败

4.12.1.13 动态数据对象列表 (DDOL)

‘9F37 04’ 十六进制

(数据对象的标签和长度)

值	标签(Tag)	长度

值	标签(Tag)	长度
不可预知数	9F37	4

4.12.1.14 应用缺省行为

‘C000’十六进制

字节	位	值	含义
1	8	**1**	如果发卡行认证失败，下次联机交易。
1	7	**1**	如果发卡行认证执行但失败，拒绝交易。
1	6	0	如果发卡行认证必需但没有收到ARPC，不拒绝交易。
1	5	0	如果交易拒绝，不生成通知 。
1	4	0	如果PIN在本次交易中已锁而且交易拒绝，不生成通知。
1	3	0	如果因为发卡行认证失败或没有执行导致交易拒绝，不生成通知。
1	2	0	如果是新卡，不联机交易。
1	1	0	如果是新卡，当交易无法联机时不拒绝交易。
2	8	0	如果PIN在本次交易中锁定，应用不锁定。
2	7	0	如果PIN在前次交易中锁定，不拒绝交易。
2	6	0	如果PIN在前次交易中锁定，不联机交易。
2	5	0	如果PIN在前次交易中锁定，当交易无法联机时不拒绝交易
2	4	0	如果发卡行脚本命令在前次交易中失败，不联机交易。
2	3	0	如果PIN在前次交易中锁定，不拒绝交易并不锁应用
2	2-1	0000	RFU

注： 带阴影的指示位表示支持卡片与发卡行认证和授权控制处理。

4.12.2 电子现金—签名

4.12.2.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
电子现金余额	n	‘9F79’	6	**初始设置为0**	保存了可供脱机消费的剩余总额。				

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
电子现金余额上限	n	‘9F77’	6	**发卡行模板**	表示在电子现金应用中，持卡人可脱机消费的最大累积额度，也即卡片充值所能达到的上限。			✔	
电子现金发卡行授权码	an	‘9F74’	6	**ECC001**	卡片上用于标识批准电子现金交易的代码。	✔			✔
电子现金单笔交易限额	n	‘9F78’	6	**发卡行模板**	卡片上单笔电子现金交易额的上限，用于控制单笔电子现金交易风险。			✔	
电子现金重置阈值	n	‘9F6D’	6	**发卡行模板**	触发卡片进行自动充值的可用余额下限。			✔	
处理选项数据对象列表(PDOL)	b	‘9F38’	9	**9F7A 01 9F02 06 5F2A 02** *详见 4.11.2.2*	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）。	✔			✔
持卡人验证方法（CVM）列表	b	‘8E’	12	**0000 0000 0000 0000 1E03 1F00** ***详见 4.11.2.3***	按照优先顺序列出卡片应用支持的所有持卡人验证方法 注意：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。	✔			✔

4.12.2.2 处理选项数据对象列表(PDOL)

‘9F7A 01 9F02 06 5F2A 02’ 十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
电子现金终端支持指示器	9F7A	1
授权金额	9F02	6
交易货币代码	5F2A	2

4.12.2.3 持卡人验证方法列表(CVM)

‘0000 0000 0000 0000 1E03 1F00’ 十六进制

CVM编码 –前八个字节为0	持卡人验证方法	处理顺序	条件	如果此CVM失败
0001 1110 0000 0011	签名（纸上）	1	如果终端支持	持卡人验证失败
0001 1111 0000 0000	不需要持卡人验证	2	总是	不会失败

4.12.3 非接触式 IC 卡支付—fDDA，应用密文版本 17，小额检查

4.12.3.1 卡片数据对象

数据名称	在卡片上的数据格式	Tag	数据长度 (bytes)	值 (十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
卡片附加处理	b	‘9F68’	4	**91 00 B0 00** *详见 4.11.3.4*	指出卡片处理需求和参数选择。				
卡片持卡人验证方法限额	n	‘9F6B’	6	**发卡行模板**	如果出现，表示当卡片和终端货币类型匹配且一个非接触交易超过这个值，则需要由卡片提供 CVM。 目前 qPBOC 支持两种 CVM：联机 PIN 和签名。			✔	
卡片内部指示器	b	_	2	**初始设置为 0**	用于控制 qPBOC 卡片内部过程。				
卡片交易属性	b	‘9F6C’	2	**初始设置为 00 00** *详见 4.11.3.5*	主要用于向终端指明卡片要求的 CVM。				
脱机消费可用余额	n	‘9F5D’	6	**初始设置为 1**	一个计算域，可用于终端显示卡片的脱机可用额度、或用于发卡行风险管控。				
应用交互特征 (AIP)	b	‘82’	2	**7C00** *详见 4.11.3.2*	说明此应用中卡片支持的功能。	✔			

数据名称	在卡片上的数据格式	Tag	数据长度(bytes)	值(十六进制)	描述	模板缺省设置	发卡行通用数据	卡或持卡人特殊数据	数据存储在文件记录中
处理选项数据对象列表(PDOL)	b	‘9F38’	12	**9F6604 9F0206 9F3704 5F2A02** *详见4.11.3.3*	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）。	✔			✔
发卡行应用数据	b	‘9F10’	8	**07 _ 17 03 00 00 00 01 0A 01** _ _ *详见4.11.3.6*	在一个联机交易中，要传送到发卡行的专有应用数据。		✔		

4.12.3.2 应用交互特征(AIP)设置

‘7C00’十六进制

字节	位	值	含义
1	8	0	RFU
1	7	1	支持SDA
1	6	1	支持fDDA
1	5	1	支持持卡人认证
1	4	1	支持终端风险管理
1	3	1	支持发卡行认证
1	2	0	RFU
1	1	0	不支持CDA
2	8-1	00000000	RFU

4.12.3.3 处理选项数据对象列表(PDOL)

‘9F66 04 9F02 06 9F37 04 5F2A 02’十六进制

(数据对象的标签和长度)

数据对象名称	Tag(标签)	长度
终端交易属性	9F66	4
授权金额	9F02	6
不可预知数	9F37	4
交易货币代码	5F2A	2

4.12.3.4 卡片附加处理

‘91 00 B0 00’十六进制

字节	位	值	含义
1	8	1	支持小额检查
1	7	0	不支持小额和CTTA检查
1	6	0	不支持小额或CTTA检查
1	5	1	支持新卡检查
1	4	0	不支持PIN重试次数超过检查
1	3	0	不允许货币不匹配的脱机交易
1	2	0	卡片不优先选择接触式PBOC联机
1	1	1	返回脱机消费可用额度
2	8	0	不支持预付
2	7	0	允许不匹配货币的交易
2	6	0	如果是新卡且读卡器仅支持脱机，不拒绝交易
2	5-1	00000	RFU
3	8	1	匹配货币的交易支持联机PIN
3	7	0	不匹配货币的交易不支持联机PIN
3	6	1	对于不匹配货币交易，卡要求CVM
3	5	1	支持签名
3	4-1	0000	RFU
4	8-1	00000000	RFU

4.12.3.5 卡片交易属性

‘00 00’十六进制

字节	位	值	含义
1	8	0	不需要联机PIN
1	7	0	不需要签名
1	6	0	如果脱机数据认证失败且终端可联机，不要求联机
1	5	0	如果脱机数据认证失败且终端支持接触式PBOC，不终止
1	4-1	0000	RFU
2	8-1	00000000	RFU

4.12.3.6 发卡行应用数据

字节	Bit	十六进制初始值	条件
1	8-1	07	长度
2	8-1	发卡行模板	分散密钥索引
3	8-1	17(十六进制)	密文版本号
4-7	8-1	03 00 00 00	卡片验证结果(CVR)
8	8-1	01	算法标识
9	8-1	0A	发卡行自定义数据(IDD)-自定义数据长度 (最长15)
10	8-1	01	IDD ID
11-15	8-1	初始设置为0	金额域
16-19	8-1	初始设置为0	MAC
20-24	8-1		其它的发卡行自定义数据

附 录 A

A.1 PBOC数据定义补充说明

A.1.1 CVM列表

在借贷记应用的个人化模板中,推荐的CVM列表的值已覆盖大部分借记卡和贷记卡的基本业务规则以及持卡人的使用习惯。但由于各发卡行的风险策略和卡片的面向群体不尽相同，因此发卡行在发卡时，可根据实际情况对CVM列表进行调整，以满足特定的需要。

A.1.2 静态签名数据

如卡片支持非接触快速支付应用（qPBOC)，则在qPBOC的签名的静态应用数据中不应该包括应用主账号序列号（5F34)。

原因是：如果5F34被包括在签名的静态应用数据中，则该数据可能会在交易中被终端重复读取，导致交易异常。

A.1.3 qPBOC的AFL

如卡片支持非接触快速支付应用（qPBOC)，则推荐将电子现金授权码（9F74）作为qPBOC 应用AFL列表中的最后一条记录，且最后一条记录仅包含该数据元。

原因是：在某些情况下，卡片在送出所有记录后，终端仍有可能由于未完整接收最后一条记录而使脱机数据认证失败。将一条短记录作为AFL列表的最后一条记录，可降低终端在读取最后一条记录时因数据过长而未完整读取的概率。

A.1.4 卡片有效期

卡背面磁条信息中的失效日期、芯片内首要借贷记应用的应用失效日期和二磁道等效数据中的失效日期应保持一致。

同时，如果卡片正面印制了有效期，则卡片正面的有效期也应与芯片内首要借贷记应用的应用失效日期保持一致。

发卡机构应保证认证中心公钥的有效期长于印制在卡片表面的有效期。

A.2 个人化模板使用场景说明

A.2.1 一般性说明

本规范所列12个模板，包括了单一模板和复合模板。单一模板主要是针对接触式IC卡的单一金融应用，包括了借记卡模板（模板1和模板2)、贷记卡模板（模板3到模板6)、准贷记卡模板（模板7)。复合模板主要是针对双界面IC卡应用，它整合了借贷记应用、电子现金应用和非接触IC卡支付应用，根据应用的不同的组合方式，包括了纯电子现金应用模板（模板11)、借记复合模板（模板12)、贷记复合模板（模板13和模板14)、准贷记复合模板（模板15)。

对于持卡人认证方法而言，不论是单一模板还是复合模板，借记应用应至少支持联机PIN，贷记、准贷记卡应至少支持签名。借记、贷记应用均推荐支持脱机PIN。

A.2.2 借记卡模板

模板1为借记卡SDA模板。国内发行的金融IC卡均应为DDA卡。因此国内发行的卡不推荐采用该模板。

模板2为借记卡DDA模板。此模板的持卡人认证方法为联机PIN，当终端不支持联机PIN时采用脱机PIN验证，如联机PIN和脱机PIN均不支持，则采用签名的认证方式。如发行的借记IC卡支持联机PIN、脱机PIN，且支持发卡行认证，则可采用此模板。如果发行的借记IC卡不支持脱机PIN，则可先对持卡人认证方法列表（8E）做相应的更新，然后采用此模板。

A.2.3 贷记卡模板

模板3、模板4、模板5均为贷记卡DDA模板。如发行卡片支持联机PIN则推荐采用模板3；如发行卡片仅支持签名，则推荐适用模板4；如发行卡片既支持联机PIN，又支持脱机PIN，则推荐采用模板5。

模板6为贷记卡CDA模板，如发行卡片支持CDA，则推荐采用模板6。

A.2.4 准贷记卡模板

模板7为准贷记卡DDA模板。如发行卡片为准贷记卡，则推荐采用模板7。

A.2.5 复合模板

复合模板包括模板11到模板15。复合模板是在上述单一模板的基础上，借助双界面IC卡非接触接口的特性，扩充了小额支付应用。根据借贷记、电子现金、非接触IC卡支付的不同组合方式，分为5个模板。

纯电子现金模板只有一个模板，即模板11。该模板仅仅借助借贷记的流程实现了小额支付的功能，不支持借贷记应用。如发行的卡片为不记名卡，且没有对应的借贷记应用主账户，仅支持电子现金应用，则推荐采用此模板。

借记+电子现金+非接触IC卡支付模板只有一个模板，即模板12。如发行的双界面借记IC卡需要同时支持电子现金和非接触IC卡支付，则推荐采用模板12。

贷记+电子现金+非接触IC卡支付模板，包括模板13和模板14。如发行的双界面贷记IC卡需要同时支持电子现金和非接触IC卡支付，则推荐采用模板13或模板14。 如非接触IC卡支付中qPBOC应用支持密文版本1，则采用模板13；如支持密文版本17，则采用模板14。

准贷记+电子现金+非接触IC卡支付模板只有一个模板，即模板15。如发行的双界面准贷记IC卡需要同时支持电子现金和非接触IC卡支付，则推荐采用模板15。