Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 042.3—2011
代替Q/CUP 030-2008

中国金融集成电路（IC）卡借记/贷记应用 收单行实施指南

China financial integrated circuit card debit/credit application-
Member Implementation Guide for Acquirers

中国银联股份有限公司 发布

目　　次

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）卡规范》借记贷记应用的收单行实施指南，供收单银行实施PBOC迁移时参考使用。

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、张卫东、李春欢、柏建宁。

中国集成电路（IC）卡借记/贷记应用收单行实施指南

1 范围

本指南的编写目的是为收单行实施 PBOC 迁移计划提供一个整体引导。它引述其它规范性文档的专业信息，或提供这些文档的索引信息。本指南帮助收单行改造其主系统和后台架构，以支持 PBOC 迁移；也包含协助收单行选择终端、支持商户等信息。

为了便于使用，每章都包含一个“执行活动”节，集中描述收单行应该完成的策略、业务、风险管理和技术方面的活动。另外，文档还提供建议、活动逐步描述等形式，协助收单行的实施。

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 0025.4-2005 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 0025.7-2005 中国金融集成电路（IC）卡规范第8部分：与应用无关的非接触式规范

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

金融IC 卡借记/贷记应用根CA 公钥认证规范

中国银联基于借记/贷记应用的小额支付规范

中国银联非接触式IC卡支付规范

3 术语和定义

本标准采用下列术语和定义：

3.1 中国金融集成电路（IC）卡规范 （2005 版）

系中华人民共和国金融行业标准之一，由中国人民银行起草并于 2005 年 3 月 10 日发布/实施，用来规范金融行业集成电路（IC）卡应用的规范。包含 10 个部分，涵盖电子钱包/电子存折应用和借记/贷记应用，本文只涉及借记/贷记应用，以下简称为“PBOC”。

该规范缺省支持接触式支付界面，在与非接触式支付规范（如：qPBOC）对照描述时，会称作“标准 PBOC”。

3.2 qPBOC(Quick PBOC)

最小化的PBOC，以保证通过非接触界面进行快速交易。

3.3 金融 IC 卡借记/贷记应用根 CA(Financial IC Card Debit/Credit Applications Root CA)

由中国人民银行授权建立的、由中国银联统一管理的服务于金融行业 IC 卡安全应用的根认证中心，以下简称“根 CA”。实现该根认证中心功能的应用系统是“金融 IC 卡借记/贷记应用根 CA 系统”，以下简称“根 CA 系统”。

3.4 应用 Application

卡片和终端之间的应用协议和相关的数据集。

3.5 命令 Command

终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.6 密文 Cryptogram

加密运算的结果。

3.7 金融交易 Financial Transaction

持卡人、商户和收单行之间基于收、付款方式的商品或服务交换行为。

3.8 功能 Function

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

3.9 集成电路 Integrated Circuit(IC)

完成处理和/或存储功能的电子器件。

3.10 集成电路卡(IC 卡) Integrated Circuit(s) Card

内部封装一个或多个集成电路用于执行处理和存储功能的卡片。

3.11 接口设备 Interface Device

终端上插入 IC 卡的部分，包括其中的机械和电气部分。

3.12 发卡行行为代码（Issuer Action Code）

发卡行根据 TVR 的内容选择的动作。

3.13 磁条 Magstripe

包括磁编码信息的条状物。

3.14 路径 Path

没有分隔的文件标识符的连接。

3.15 支付系统环境 Payment System Environment

当符合本规范的支付系统应用被选择，或者用于支付系统应用目的的目录定义文件（DDF）被选择后，IC 卡中所确立的逻辑条件。

3.16 响应 Response

IC 卡处理完收到的命令报文后，返回给终端的报文。

3.17 脚本（Script）

发卡行向终端发送的命令或命令序列，目的是向 IC 卡连续输入命令。

3.18 终端 Terminal

为完成金融交易而在交易点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其它部件和接口，例如与主机通讯的接口。

3.19 终端行为代码（Terminal Action Code）

终端行为代码（缺省、拒绝、联机）反映了收单行根据 TVR 的内容选择的动作。

4 符号和缩略语

以下缩略语和符号表示适用于本规范：

AAC	应用认证密文(Application Authentication Cryptogram)
AAR	应用授权参考(Application Authorization Referral)
AC	应用密文(Application Cryptogram)
ADA	应用缺省行为(Application Default Action)
ADF	应用数据文件(Application Definition File)
AEF	应用基本文件(Application Elementary File)
AFL	应用文件定位器(Application File Locator)
AID	应用标识符(Application Identifier)
AIP	应用交互特征(Application Interchange Profile)
APDU	应用协议数据单元(Application Protocol Data Unit)

ARPC	授权响应密文(Authorization Response Cryptogram)
ARQC	授权请求密文(Authorization Request Cryptogram)
ATC	应用交易序号(Application Transaction Counter)
ATM	自动柜员机(Automated Teller Machine)
ATS	选择应答(Answer To Select)
AUC	应用用途控制(Application Usage Control)
BER	基本编码规则(Basic Encoding Rules)
CA	认证中心(Certificate Authority)
CAM	联机卡片认证(Card Authentication Method)
CDA	复合动态数据认证/应用密文生成(Combined DDA/AC Generation)
CDOL	卡片风险管理数据对象列表（Card Rish Management Data Object List）
CID	密文信息数据(Cryptogram Information Data)
CLA	命令报文的类别字节(Class Byte of the Command Message)
cn	压缩数字格式(compress numeric)
C-TPDU	命令 TPDU(Command TPDU)
CTTA	累计脱机交易金额(Cumulative Total Transaction Amount)
CTTAL	累计脱机交易金额限制数(Cumulative Total Transaction Amount Limit)
CTTAUL	累计脱机交易金额上限(Cumulative Total Transaction Amount Upper Limit)
CUPS	中国银联信息处理中心系统(ChinaUnionPay System)
CVM	持卡人验证方法（Cardholder Verification Method）
CVR	卡片验证结果(Card Verification Results)
CVN	卡片验证码(Card Verification Number)
DDA	动态数据认证(Dynamic Data Authentication)
DDF	目录数据文件(Directory Definition File)
DDOL	动态数据认证数据对象列表（Dynamic Data Authentication Data Object List）
DF	专用文件(Dedicated File)
DIR	目录(Directory)
DOL	数据对象列表(Data Object List)
GPO	获取处理选项（GET PROCESSING OPTIONS）
EC	电子现金(Electronic Cash)
EF	基本文件(Elementary File)
EMV	Europay MasterCard VISA
FCI	文件控制信息(File Control Information)
fDDA	快速动态数据认证(Fast DDA)
FWI	帧等待时间整数(Frame Waiting time Integer)
IAC	发卡行行为代码(Issuer Action Code)
IC	集成电路(Integrated Circuit)
IC 卡	集成电路卡(Integrated Circuit Card)
iCVN	IC 卡片验证码(Integrated Circuit Card Verification Number)
IDD	发卡行自定义数据(Issuer Discretionary Data)
Lr	响应数据域的长度(Length of Response Data Field)
M	必备(Mandatory)
MAC	报文认证码(Message Authentication Code)
MDK	主密钥(Master DEA Key)

MF	主文件(Mater File)
n	数字型(Numeric)
O	可选(Optional)
P1	参数 1(Parameter 1)
P2	参数 2(Parameter 2)
P3	参数 3(Parameter 3)
PAN	主帐号(Primary Account Number)
PBOC	中国人民银行(People’s Bank of China)
PDOL	处理选项数据对象列表(Processing Options Data Object List)
PKI	公钥基础设施(Public Key Infrastructure)
PIN	个人密码(Personal Identification Number)
PIX	专用应用标识符扩展(Proprietary Application Identifier Extension)
RFU	保留(Reserved for Future Use)
RID	注册应用提供商标识(Registered Application Provider Identifier)
R-TPDU	响应 TPDU(Response TPDU)
SAD	签名的静态应用数据(Signed Static Application Data)
SDA	静态数据认证(Static Data Authentication)
SFI	短文件标识符(Short File Identifier)
SW1	状态字 1(Status Word One)
SW2	状态字 2(Status Word Two)
TAC	终端行为代码(Terminal Action Code)
TC	交易证书(Transaction Certificate)
TDOL	交易证书数据对象列表(Transaction Certificate Data Object List)
TLV	标签、长度、值(Tag Length Value)
TSI	交易状态信息(Transaction Status Information)
TVR	终端验证结果(Terminal Verification Results)
UDK	子密钥(Unique DEA Key)
专用的	本规范内未定义或/和超出本规范范围的
必须	表示强制的要求
应该	表示推荐的要求

5 终端选择与认证

本章帮助收单行选择受理终端，提供终端认证程序的相关背景信息，包括以下内容：

—— 终端选择标准
—— 遵守规范
—— 银联终端推荐
—— 银联供应商计划
—— 终端认证
—— 执行活动
—— EMV 功能模块化

5.1 终端选择标准

在与供应商会谈以及评估其产品之前，收单行需要启动制订终端要求的程序，针对具体受理环境决定最小/必须/推荐的终端要求。

本节对收单行终端选择标准所涉及的信息进行一个概述：

—— 向供应商描述对于以下范畴的终端要求，确保其产品支持它们：

- EMV 要求
- PBOC 要求

收单行必须确保 EMV/PBOC 兼容终端：

- 能够读磁条。
- 能够读芯片。如果卡片上存在 EMV/PBOC 兼容芯片，不允许可读芯片终端故意跳过芯片授权控制而使用磁条；仅在芯片不兼容 EMV/PBOC 或芯片/芯片读写器不可操作时，才允许使用磁条进行交易。
- 支持私有要求。
- 支持交易类型要求，例如：预授权、撤销、退货等。
- 支持磁条终端要求，例如：Fallback 处理、识别服务代码的兼容要求。
- 支持其它应用要求，例如：积分计划、储值方案。
- 支持持卡人账户选择。

—— 确定支持的终端类型，例如：分体式终端、集成式 POS、ATM、手持 POS 终端、无人值守终端。

—— 确定终端是否仅联机、仅脱机、或者具备联机/脱机能力。

—— 确定对基于终端的异常文件的要求。

—— 确定对应用选择的要求（目录选择与 AID 列表选择方法）。

—— 针对目标市场，确定对持卡人验证的要求（联机 PIN、脱机明文/密文 PIN、签名等）。

—— 基于设备的功能、硬件、软件、保证条款、服务支持协议，评估产品价格。

—— 确保终端通过 EMV Level 1 和 Level 2 认证

—— 决定对终端配置的商业要求，例如：是否要求独立的芯片受理设备、或外接密码输入部件，这些设备应该符合银联要求。

—— 验证产品性能。

—— 决定对交易速度的要求，评估支持的交易量。

—— 决定商户整个配置的哪些部分受芯片影响，并确定：

- 通过软件改造实现的部分；
- 要求新增硬件的部分；
- 所有相关的供应商。

—— 判断现有设备能否升级、或者要求新增设备。

—— 决定任何额外的技术功能要求，例如：射频支持、手机功能、或互联网连接。

—— 决定芯片对于最低限额的影响，可以为芯片和磁条设置不同的最低限额。

5.2 遵守规范

PBOC终端必须遵守以下规范：

—— EMV 4.1 Integrated Circuit Card Specifications for Payment Systems

由EMVCo发布的受理借记/贷记卡终端的基础工业规范,PBOC终端必须符合这些规范的描述:EMV Level 1(物理特性)和EMV Level 2（借记/贷记功能）。

—— 中国金融集成电路（IC）卡规范

—— 银联卡业务运作规章

注： 相关规范会周期性地进行修订，请联系银联代表以获取最新文档；EMV最新规范可从EMVCo网站http://www.emvco.com获取。

表1 基本终端功能

功能	描述
磁条阅读能力	终端必须能够读取一磁或二磁的完整信息、能够读取高密和低密磁条。 在向芯片卡迁移的过程中，单纯的磁条卡仍会长期存在，因此这些要求是必须的。在芯片

	卡上保留磁条，也可以在芯片无法阅读时起到后备的作用。
服务代码识别能力	EMV/PBOC 兼容终端在处理磁条时，必须读取扩展的服务代码进行相应处理： ● EMV 芯片存在：2xx 或 6xx ● 联机授权首选：x2x ● 联机 PIN 首选：xx6
PIN 输入	基于编码在芯片内的持卡人验证参数，终端必须能够提示、接受 PIN。PIN 输入要求基于发卡行的选择，可以针对特定的交易类型（如：ATM 交易）。
芯片读写器和磁条读写器之间的逻辑接口	当识别到阅读一个芯片失败，终端应能判断该卡又作为磁条卡发起下一笔交易，设置相应状态（通过 60.2.3 域）并请求联机处理。
静态数据认证(SDA)	SDA 是一种公钥安全验证方法，用于验证卡片数据是由真实的发卡行创建、并且卡内静态数据没有被修改。它是一个脱机芯片风险管理功能，通过在交易点校验关键数据以防止伪造。 SDA 对于所有可脱机终端是强制要求的，但对于仅联机终端是可选的。
动态数据认证(DDA)	DDA 是一种针对脱机环境的基于公钥机制的芯片风险管理功能，它通过在交易点验证卡片生成的动态数字签名以防止“克隆”数据。 DDA 对于所有可脱机终端是强制要求的，但对于仅联机终端是可选的。
根 CA 公钥加载	为了执行脱机数据认证或处理脱机密文 PIN，终端必须加载根 CA 公钥。终端应具备加载新的公钥、删除失效公钥的能力。
可变长账号的受理	终端应该能够接受 13 至 19 位的账号。
服务点输入方式	当“服务点输入方式”为芯片输入时，所有交易数据必须来自于芯片。对于通过芯片发起的交易，终端不应使用磁条上的磁道数据，而应该使用芯片内的“磁条 2 等效数据”。

5.3 银联终端建议

银联描述了一系列建议，以帮助收单行制定终端选择标准。这些建议包括基本功能、推荐功能和其它考虑。

5.3.1 推荐终端功能

收单行可以根据自身需要选择是否支持这些推荐功能。

表2 推荐终端功能

功能	描述
脱机 PIN	所有 PBOC 终端应考虑支持脱机明文 PIN。终端具备成功验证脱机 PIN 的能力有助于更多的 PBOC 交易脱机完成。
持卡人应用选择	多应用是芯片卡的一个重要特性，终端应该能够提供这个功能。当卡片和终端同时支持这个功能时，通过两者交互终端可以向持卡人显示不同的应用，供持卡人确认选择。终端至少应显示 2 行×16 个字符，推荐支持 4 行×20 字符、位图显示。
对芯片/非芯片交易使用不同最低限额(Floor Limit)的能力	由于芯片卡的安全级别显著高于磁条卡，收单行可以考虑对芯片交易和非芯片交易执行不同的最低限额。建议 PBOC 终端应能提供分离的最低限额。
联机能力	终端可以仅脱机、仅联机、联机/脱机。如果终端不具备联机能力，当脱机计数器达到其上限时就只能拒绝交易了；因此，强烈建议所有通用终端应具备联机能力。
联机 PIN 支持	国内使用环境普遍要求联机 PIN，所有 ATM 必须支持联机 PIN。
支持电子现金功能	这个可选功能允许终端对于携带电子现金功能的 PBOC 卡片执行快速脱机交易。
附加应用	处理其它应用的能力，例如：积分计划。

5.3.2 其它考虑

以下描述对于收单行考虑终端的设计选项会有所帮助。

表3　设计选项

功能	描述
处理器	终端完成交易的时间不应让持卡人和营业员感觉到需要过分长的等待。收单行应该与终端供应商交流，了解其产品的处理速度是否能够满足客户服务的要求。
通讯速率	为了保持一个合理的响应时间，通讯速率至少应达到 9600bps。
内存	终端应该具有足够的内存以处理卡内所有应用、支持更长的密钥以及为支持预期的应用保留空间。内存应该支持防火墙隔离以保证跨应用的安全、避免相互干扰。
模块化软件架构	多应用处理必然要求在核心库中建立模块化代码，以供所有应用共同使用。 推荐以下模块： ● 持卡人和营业员的交互接口，如：表单驱动的提示与响应； ● 外围设备的驱动程序，如：集成 POS 以及打印机的接口； ● 通讯报文处理程序。 卡片应确保采用模块化软件架构，使通过 PBOC 认证的核心/软件不受影响。
灵活的系统结构	收单行在构建终端软件程序和管理系统时，应注意保持灵活的系统结构，以便后续变更信息时尽量不需要做大的改造、甚至影响终端的基础架构。
下载能力	更新应用程序、置换应用、加载新应用、增加或删除密钥等事项都要求终端支持下载能力。另外，下载更新应避免为了实现一个小的程序变动而进行完全重载的操作。
复合 DDA/应用密文生成(CDA)	CDA 将动态数据认证(DDA)和应用密文生成结合起来，提供对卡内数据、卡片本身和交易安全的认证。 CDA 对于所有终端都是可选的。
杂项要求	终端应该提供以下组件： ● 用于输入交易金额、选择命令和执行功能的按键键盘； ● 打印交易单据的打印机，根据支付系统要求可以是针式或热敏打印机； ● 能处理脱机交易的终端应配有时钟模块，用来提供当地日期和时间；建议实现这个时钟与收单行主机时间的自动同步。
安全存取模块(SAM)支持	收单行若计划支持电子钱包应用，应要求终端支持销售点终端安全存取模块(PSAM)。

5.4　银联供应商计划

为了促进符合EMV和PBOC安全、互操作性以及功能要求的终端的部署，银联正在与供应商进行合作计划，相关活动包括：

——　执行供应商资质评估；

——　对供应商进行 EMV/PBOC 培训；

——　与供应商交流、探讨终端设置的最佳方案；

——　为银联成员谈判特价计划。

收单行在选择供应商时，可与银联代表联系，了解这个计划对其采购终端活动是否有所帮助。

5.5　终端认证

收单行必须选择通过EMV Level 1和EMV Level 2认证的产品，确保所选终端遵守银联业务规章。

5.6　执行活动

本节概述了收单行选择PBOC终端所涉及的策略、业务和技术活动：

——　策略

- 参考本章所提供的信息，制定终端要求；
- 评估供应商产品是否符合要求，这可以通过一个需求建议书(RFP)流程来实现；
- 确保所选择的供应商产品通过 EMV Level 1 和 EMV Level 2 认证。

研制一款EMV/PBOC兼容终端是一个耗费时间的过程，为了在最短的时间范围内完成PBOC迁移计划，建议收单行选择已经通过认证的供应商。EMVCo认证产品和厂商清单可从http://www.emvco.com上获得，PBOC认证产品和厂商清单可从http://www.bctest.com上获得。收单行应该了解：一个新的供应商研制一款EMV/PBOC终端并通过认证需要4-12个月时间。

—— 业务

支持终端的业务活动在后续章节中描述。

—— 技术

支持终端的技术活动在后续章节中描述。

收单行应该确保所部署的终端符合EMV和PBOC要求，否则可能引发互操作性问题。银联提供PBOC集成测试工具(PBOCIT)帮助收单行验证其终端是否符合这些要求。

由于EMV规范的灵活性以及客户化选项的应用，EMV Level 1和EMV Level 2认证并不能保证终端的互操作性完全没有问题；而PBOCIT能够在终端部署之前检测并隔离潜在的互操作性问题。

5.7 EMV 功能模块化

终端软件架构应该配置成将EMV应用内核与其它应用相隔离，推荐这种模块化架构是因为：

—— 它有利于保护商业投资。

—— 当基于终端的 EMV Level 1 和 EMV Level 2 功能研发新产品时，可以不要求重新进行 Level 1 和 Level 2 测试。

—— 软件升级更方便。

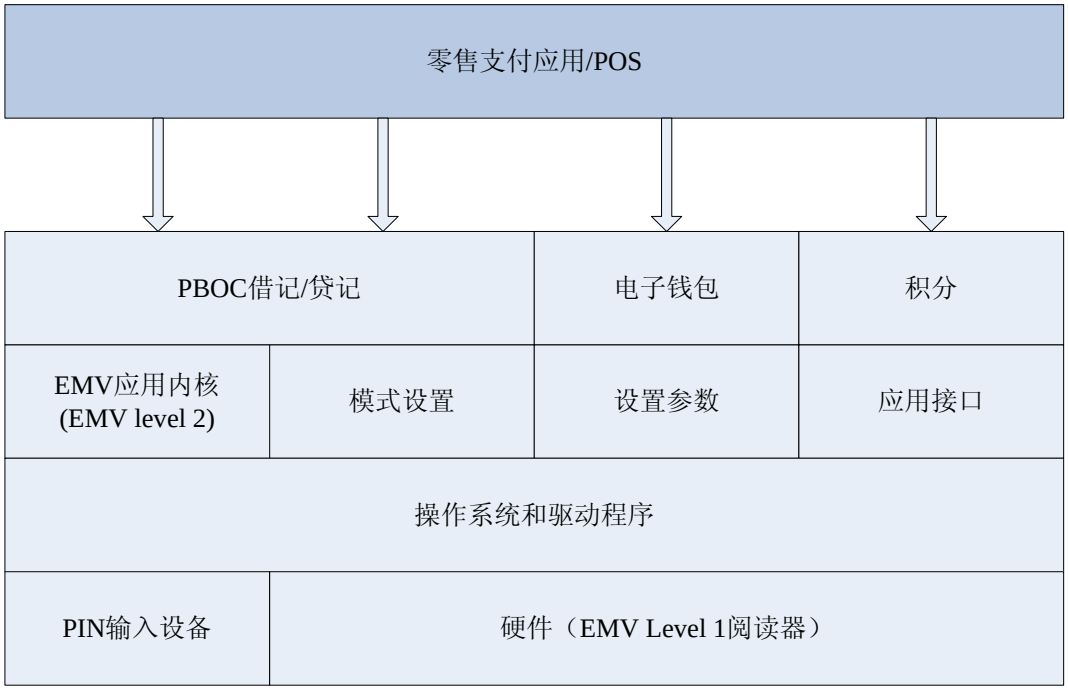
保持EMV功能与非EMV功能的独立性，在发生支付应用需要升级或改造时，EMV功能就不会收到影响。

在任何情况下，如果终端的EMV功能受到影响，供应商应该重新提交EMV认证，否则很可能引发互操作性问题。变更功能应该尽量使用参数化配置的方法来实现，对于一个完全采用模块化架构配置的终端，对TAC做一个变动不会影响其EMV兼容性；反之，就可能要求重新进行Level 2认证。

绝大多数EMV功能是强制要求的，终端管理系统不应允许删除任何强制功能；系统可以控制可选功能，提供一套配置装载到终端内。为了确保互操作性，大多数卡片可选的功能对于终端是强制的。

以下是一个EMV终端模块化架构示意图：

图1 模块化架构



6 终端要求

本章将帮助收单行理解部署EMV/PBOC终端的要求，包括在EMV和PBOC规范中描述的安全性、互操作性和功能性要求。本章说明终端要求的每个应用功能、解释实现这些功能所要求的决策、业务和技术活动。

下表描述了本章所涵盖的应用功能：

表4 PBOC 应用功能

功能	描述
应用选择	终端生成卡片和终端共同支持的应用候选列表，决定选择合适的应用来实现交易。
脱机数据认证	终端验证卡片以防止数据篡改及伪造。
处理限制	终端检查应用交易是否允许继续进行。
持卡人验证	执行验证持卡人的合适机制。
终端风险管理	终端检查最低限额、异常文件（如果存在）、以及随机选择交易要求联机处理等。
终端行为分析	终端根据脱机数据认证、处理限制、持卡人验证、终端风险管理的结果以及终端和卡片中设置的风险管理参数决定如何继续交易（脱机批准、脱机拒绝或请求联机处理）。

本章只是对实现每个PBOC功能所要求的活动进行一个概述，更详细的操作请参考EMV和PBOC规范。收单行应该与供应商沟通，明确各自的职责。

注： 收单行应该意识到相关决策是受其所处市场整体驱动的、而不应仅仅是孤立的收单方策略。

6.1 应用选择

在受理一张PBOC借记/贷记卡片时，终端通过比较卡内AIDs和终端维护的AIDs，决定哪些是卡片和终端共同支持的应用。终端使用目录选择方法或AID列表选择方法建立终端和卡片共同支持的应用列表。目录选择方法对于终端是强制要求的，对于卡片是可选的；AID列表选择方法是卡片和终端都是强制要求的。

如果卡片和终端都支持目录选择方法，终端通过一个称为支付系统环境(PSE)的文件读取卡内维护的支付应用列表。终端将 PSE 所列应用和它支持的应用进行比较，建立候选列表－卡片和终端共同支持的终端内部列表。如果卡片没有 PSE，终端转而使用 AID 列表选择方法。

使用 AID 列表选择方法，终端根据终端应用列表依次询问卡片是否其应用列表中包含此应用，终端将共同支持的应用加入候选列表中。

6.1.1 目录选择和 AID 列表选择方法

PBOC 设计了两种不同的方法来实现应用选择：

—— 目录选择方法

这种方法对于终端是强制要求的，对于卡片是可选的；终端首先尝试此方法，从卡片中读取支付系统环境(PSE)文件。对于支持目录选择方法的卡片，PSE 是一个高阶层目录文件，至少包含了卡内全部 PBOC 支付应用的列表。终端用这个列表与它维护的列表进行比较，将卡片和终端共同支持的应用加入其建立的候选列表。接着根据终端是支持持卡人选择应用、还是支持终端自动选择应用，来选择交易的应用。

—— AID 列表选择方法

这种方法对于终端和卡片都是强制的。使用 AID 列表选择方法，终端对其支持的每个应用发一个命令给卡片，询问卡片是否也支持这个应用；如果卡片响应表明卡内包含这个应用，终端将这个应用加入候选列表。接着根据终端是支持持卡人选择应用、还是支持终端自动选择应用，来选择交易的应用。

由于目录选择方法对于卡片是可选的，当卡片不支持目录选择方法时，转而使用 AID 列表选择方法。

终端得到卡片与终端共同支持的候选应用列表后，使用以下方法从中选择一个应用执行交易：

—— 持卡人选择应用

如果终端支持持卡人选择应用，可以采用以下任一方式：

- 持卡人选择

  终端将向持卡人按优先级顺序给出应用列表以供选择，持卡人从列表中选择一个应用。

- 持卡人确认

  终端首先将优先级最高的应用提供给持卡人确认；如果持卡人不确认，终端提供下一个优先级最高的应用，直到持卡人确认或不再有更多的应用为止。

—— 终端自动选择应用

如果终端不支持持卡人选择或持卡人确认，则终端会自动选择具有最高优先级且不要求确认的应用。如果超过一个应用有最高优先级，终端可以选择其中任一应用或按终端所列顺序选择最前面的应用。

6.1.2 应用标识符

终端必须包含其支持的所有芯片支付应用的应用标识符(AID)。假如对于受理卡片的AID，终端使用它支持的任一AID都无法与之匹配，将无法执行芯片交易。

AID 由两部分组成：

—— 注册应用提供商标识(RID)

这个组件标识支付方案。银联 RID 是 A000000333。

—— 专用应用标识符扩展(PIX)

这个组件代表应用。银联 PIXs 见下表所列。

表5 银联专用应用标识符扩展(PIXs)

应用	PIX
借记/贷记应用	0101
借记应用	010101
贷记应用	010102
准贷记应用	010103

终端为每个支持的应用设立一个应用选择指示符（ASI）变量，用来表示该应用是全部名称匹配还是部分名称匹配。建议对于银联AIDs设置ASI支持部分名称匹配。

对于决策者、业务人员以及技术人员，与AIDs相关的活动包括：

—— 策略

决定支持的 AIDs。收单行计划受理哪些卡品牌，其终端就必须支持对应的 AID；例如：收单行准备受理 PBOC 贷记卡，终端就必须支持银联 AID－A000000333010102。

—— 业务

获得终端要求的 AIDs 列表，与技术人员一起将 AIDs 加载到终端并进行测试以保证运作正常。

—— 技术

负责加载 AIDs 到终端，并提供增加 AIDs 和应用到终端的机制。

6.1.3 语言

收单行必须决定为客户提供哪些语言支持。EMV/PBOC终端可以多种语言显示信息，至少应该支持一种语言。

对于决策者、业务人员以及技术人员，与终端支持语言相关的活动包括：

—— 策略

决定终端能够显示的语言。收单行至少应该提供本国语言显示；另外，如果来自特定国家的客户流量很大，可以考虑支持其所用语言。

—— 业务

在操作、培训手册中介绍终端可用语言。

—— 技术

与终端供应商协作，确保终端能够支持所要求的语言。

6.1.4 持卡人选择/确认

银联强烈建议PBOC终端实现持卡人选择应用功能，以便在卡片支持多个支付应用时，持卡人能够选择其想要的应用进行交易。

当受理终端和卡片共同支持多于一个应用时，终端可以通过以下任一方法实现持卡人选择应用：

—— 终端按发卡行定义的优先级显示所有共同支持的应用，供持卡人选择；

—— 终端按发卡行定义的优先级逐个显示共同支持的应用，由持卡人确认是否使用。

当受理终端支持持卡人选择应用功能，并且只存在一个共同支持的应用时：

—— 如果应用要求持卡人确认，终端必须显示这个应用供持卡人确认是否使用这个应用（不确认将导致交易终止）；

—— 如果应用不要求持卡人确认，终端自动选择这个应用。建议终端显示这个应用以告知客户，但无需等待持卡人确认就可以继续处理交易。

对于某些特定受理场所（例如：收费公路、快餐店），收单行可以决定不支持持卡人选择应用。收单行应该意识到，某些发卡行的应用选择强制要求持卡人确认；在这些受理场所，终端将无法受理此类卡片。

与持卡人选择应用相关的活动包括：

—— 策略

决定是否支持持卡人选择应用。对于某些特定场所，收单行可以决定不执行持卡人选择应用功能。只要条件许可，建议终端尽量实现持卡人选择应用以避免因此而拒绝卡片交易。

—— 业务

在操作、培训手册中介绍持卡人选择应用功能。

—— 技术

与终端供应商协作，确保终端能够支持收单行要求。

6.2 脱机数据认证

EMV和PBOC定义了三种脱机数据认证方法：静态数据认证(SDA)，动态数据认证(DDA)和复合数据认证(CDA)。这些方法都使用公钥技术来防止数据伪造，但DDA要比SDA完善得多，它为每笔交易都生成一个动态签名来防止复制芯片数据到伪卡的行为。SDA是与磁条交易的CVN检查相对应的，都可以检测个人化后特定静态数据是否被篡改，但是SDA与CVN检查的不同之处在于：它是在终端脱机执行的、并且也比CVN更加安全。CDA处理提供DDA保护，还能确保交易数据在卡片和终端的传递过程中没有被篡改。

目前，SDA和DDA对于有脱机能力（仅脱机或联机/脱机）的终端是强制要求的，仅联机终端不一定要支持这个功能。因此对于联机ATM或其它设置最低限额为零的商户环境，这些功能是可选的。

除了总是联机的终端，DDA对于其它终端都是强制要求的。

注： 在加载生产密钥之前，收单行应该删除所有测试密钥以避免发生脱机数据认证失败的情况。

与脱机数据认证相关的活动包括：

—— 策略

决定是否支持脱机数据认证，如果支持，是采用哪种方式。通常是否实现 SDA、DDA、CDA（或其组合）是由国家或区域的强制规定来驱动的，PBOC 要求所有终端必须支持 DDA，否则只能完全联机处理交易。银联建议：收单行应与各参与方一起协商，决定支持何种脱机数据认证方法；这需要评估向芯片迁移的市场驱动力、权衡成本与收益情况。

由于向芯片迁移是必然趋势，为了节约升级所花费的成本，建议 PBOC 终端一开始就支持脱机数据认证功能。

—— 业务

与终端供应商合作实现所选择的脱机数据认证方法。

—— 技术

相关开发工作由供应商来完成，基本上不需要内部技术资源。

6.3 处理限制

终端通过处理限制来检查应用交易是否允许继续进行。它检查卡片（应用）是否已经生效、是否已经失效、卡片和终端的应用版本号是否匹配、以及任何应用用途控制(AUC)的约束条件是否有效。发卡行可以使用AUC来限定卡产品用于国内还是国外，或能否用于取现、商品、服务以及返现等交易。

处理限制是EMV/PBOC的一个强制功能，要求所有终端必须支持。

与处理限制相关的活动包括：

—— 策略

无需决策。

—— 业务

确定终端支持的 PBOC 版本所对应的应用版本号，连同支持的其它支付应用的版本号一起加载到终端。

—— 技术

加载合适的应用版本号到终端；当应用版本号升级时，加载新的应用版本号到终端。

6.4 持卡人验证

持卡人验证用于确保持卡人的合法身份、卡片未曾失窃。终端使用卡片提供的持卡人验证方法(CVM)列表，决定执行验证的方式，例如：签名或脱机明文 PIN。CVM 列表建立了持卡人认证方式优先级别，根据终端能力和交易特性提示用户采用特定的持卡人认证方式。如果卡片不支持 CVM 处理，终端应按磁条卡借记/贷记应用中的持卡人验证方法进行处理。如果 CVM 是“无需 CVM”，则终端按照 PBOC 规范规定的对该终端类型的默认持卡人验证处理方法进行；例如：若默认方法是签名，则终端打印带有签名行的凭据。对于某些终端类型（如：ATM），不管在 CVM 列表里是否支持，应该总是支持联机 PIN 输入。

注： ATM不允许脱机PIN。

银联建议商户保留CVM信息至少180天以应对争议处理。CVM信息是与所选择的CVM相对应的，例如：保留交易凭证以证明执行了脱机明文PIN验证。

下表列示了PBOC支持的CVM：

表6 持卡人验证方法

持卡人验证方法	描述
签名	这种方法的操作方式与磁条卡环境一样：持卡人在签购单上签名，商户将其与卡片上的签名进行比较。
脱机明文 PIN	这是一种新的方法：终端提示持卡人输入 PIN，以明文方式传给卡片；卡片将其与卡内存放的脱机 PIN 进行比较。
脱机明文 PIN 和签名	脱机明文 PIN 和签名的组合，使用两种方法进行持卡人验证。
联机 PIN	这种方法的操作方式与磁条卡环境一样：终端使用 DES 技术对持卡人输入 PIN 进行加密，发送联机请求给发卡行验证。
无需 CVM	这种方法的操作方式与磁条卡环境一样：交易授权不依赖于持卡人验证。在某些商户环境中是允许无持卡人验证的，例如：经过挑选的持卡人移动终端。
CVM 失败	这种方法允许发卡行选择将 CVM 处理缺省为失败的情形。
身份证件	终端提示持卡人出示身份证件，并将卡片中得到的证件类型和证件号码显示给营业员，进行持卡人身份比对。

芯片交易能够支持更安全的CVM，例如：脱机PIN提供的脱机持卡人验证能力可以有效推动发卡行向芯片迁移；而且，在PBOC终端使用脱机PIN验证，也可以在发生争议时为收单行提供额外的责任保护。

PBOC强制要求终端支持持卡人验证，通过检查卡片CVM列表（如果存在），决定交易应采用的验证方法。

收单行的终端具体要支持哪些CVM，应基于商业需求、受理卡产品类型、市场策略以及银联要求等因素综合考虑决定。以下所列的通用规则可以帮助收单行决定其终端实现哪些CVM：

—— 除了 ATM 等各类自助终端，要求继续支持签名方式；

—— 要求终端必须支持“脱机明文 PIN”方式；

—— 要求终端必须支持“联机 PIN”方式；

—— 在某些市场，可能对于超过某个金额的 POS 交易除了需持卡人签名外，还要求输入持卡人脱机 PIN；

—— 所有 EMV/PBOC 兼容终端必须支持“无需 CVM”方式；

—— 所有 EMV/PBOC 兼容终端必须支持“CVM 失败”方式。

6.4.1 未知的 CVM

终端必须能够识别EMV/PBOC定义的CVM，即使它不支持这种CVM。例如：一张PBOC卡片的CVM列表包含脱机明文PIN、签名和“无需CVM”，终端可以支持签名和“无需CVM”、但不支持脱机明文PIN；在这种情形下，终端必须能够识别“脱机明文PIN”方式，以避免触发“未知的CVM”条件。

6.4.2 执行活动

与持卡人验证相关的活动包括：

—— 策略

基于 PBOC 和本地市场要求以及商业考虑，决定终端支持哪些 CVM；

—— 业务

与终端供应商协作，确保支持所处市场强制/建议/可选要求的 CVM；

—— 技术

技术部门需要参与相关分析工作，但开发工作一般由终端供应商来承担；

对于联机 PIN 验证，PBOC 的要求与当前规则保持一致。

6.5 终端风险管理

终端风险管理对于商户控制的终端是强制要求的，它校验：

—— 交易是否超过商户最低限额；

—— 卡片账号是否出现在终端异常文件中；

—— 是否超过连续脱机交易限制；

—— 卡片是否为一张新卡；

—— 是否商户强制交易联机；

—— 交易是否随机选择进行联机。

其中某些功能对于仅脱机或仅联机终端可能不适用。

终端风险管理要求：

—— 终端最低限额：对所有终端都强制要求；

—— 随机交易选择：对同时有联机和脱机能力的终端强制要求；

—— 频度检查：对支持脱机交易的联机终端强制要求；

—— 新卡检查：对所有终端都强制要求。

6.5.1 最低限额

EMV/PBOC强制要求有脱机能力的终端对所有交易执行最低限额检查。

与磁条终端一样，EMV/PBOC兼容终端必须支持最低限额功能。由于通过卡片和持卡人验证，芯片处理可以在交易点提供更高的安全性，某些市场可以设置不同于磁条最低限额的芯片最低限额。如果卡片参数标识交易必须联机处理，则终端会不管最低限额而请求联机处理。

为了提供最大的灵活性，银联建议设置终端支持下述最低限额，即使磁条和芯片交易的取值当前是相同的：

—— 国际磁条交易最低限额
—— 国际芯片交易最低限额
—— 国内磁条交易最低限额
—— 国内芯片交易最低限额

注： 对于降级使用(Fallback)交易总是使用零最低限额。

在终端及其后端管理系统中支持这些独立的最低限额，可以为收单行适应未来需求提供更大的灵活性。银联建议收单行按照AID存储最低限额信息，因为不同卡产品的最低限额取值也会相应变化。

与最低限额相关的活动包括：

—— 策略

- 决定对于最低限额是否有新的要求。
- 强制有脱机能力的终端对所有交易执行最低限额检查，当交易金额大于最低限额时拒绝批准脱机，因为这可能带来风险。
- 类似于磁条终端，EMV/PBOC 兼容终端必须支持最低限额功能。由于通过卡片和持卡人验证，芯片处理可以在交易点提供更高的安全性，某些市场可以设置不同于磁条最低限额的芯片最低限额：对磁条交易维持现有的最低限额，对芯片交易使用更高一点的最低限额。

—— 业务

在业务以及商户培训文档中介绍最低限额的相关内容。

—— 技术

加载合适的 PBOC 最低限额到终端中，在需要时下载更新的参数。即使所处市场目前不要求使用不同的最低限额，收单行终端也应该能够对芯片和磁条交易支持不同的最低限额。

6.5.2 随机选择

随机选择是一个终端随机选择金额低于最低限额的交易请求联机的处理方法，它不依赖于卡片控制参数。这个功能是为了防止罪犯掌握终端的行为规则，使用伪卡连续完成小额交易。随机选择对于同时具有联机和脱机能力的终端是强制要求的。

注： 由于电子现金(EC)功能专用于脱机环境，通过EC参数处理小额交易，它不需要进行随机选择处理。

随机选择交易请求联机处理是基于以下三个参数：

—— 偏置随机选择阈值：取值应在 0 和终端最低限额之间；
—— 随机选择目标百分数：取值在 0 和 99 之间；
—— 偏置随机选择的最大目标百分数：取值有应在随机选择目标百分数和 99 之间。

如需获得设置随机选择参数方面的引导，请与银联代表联系。

与随机选择相关的活动包括：

—— 策略

和所处市场的 PBOC 计划参与者以及银联代表一起决定联机/脱机终端的随机选择参素。

—— 业务

在业务以及商户培训文档中介绍随机选择的相关内容。

—— 技术

加载随机选择参素到终端。终端供应商可能会事先将这些信息加载到终端。

6.5.3 频度检查

卡片个人化参数可以控制在请求联机处理之前允许连续脱机的交易笔数，这种处理方法通常称为频度检查。允许脱机和联机的终端必须支持频度检查。

6.5.4 异常文件

如果终端异常文件存在，则终端检查卡号是否出现在异常文件列表中。

这个功能是可选的。

与异常文件相关的活动包括：

—— 策略

判断是否在终端中需要支持异常文件；如果目前终端支持异常文件，那么至少对于国内和磁条卡交易，应继续在芯片终端里支持异常文件。

—— 业务

需要能够下载并升级异常文件。

—— 技术

和终端供应商合作，确保终端程序能够支持异常文件处理。

6.6 终端行为分析

终端行为分析是强制要求的，根据脱机数据认证、处理限制、持卡人验证、终端风险管理的结果以及终端和卡片中设置的风险管理参数决定如何继续交易（脱机批准、脱机拒绝或请求联机）。卡内存放的规则称为发卡行行为代码(IAC)，它可以通过卡片发送到终端；存放在终端里的支付系统规则称为终端行为代码(TAC)。

与终端行为分析相关的活动包括：

—— 策略

无需决策。

—— 业务

向银联代表了解适用于本地市场的终端行为代码；在业务以及商户培训文档中介绍 TAC 的相关内容；如果终端支持电子现金功能，它可以要求单独的 TACs。

—— 技术

PBOC TACs 以及其他支付系统的 TACs，必须加载到终端中。终端供应商应能预先加载这些信息到终端。另外，终端管理系统应能跟踪 TACs 设置，当需要时通过下载升级设置。

终端可以使用一套独立的 TACs 设置支持电子现金交易。

7 其它终端要求

除了EMV/PBOC的功能配置要求之外，还有一些适用于终端设备的必备或可选的特性可能对市场或业务具有重大的帮助。本章就将讨论这些功能配置要求：

—— 磁条卡终端要求

—— 电子现金功能（可选）

—— 非接触式 IC 卡支付

—— 专有要求

—— 交易类型要求

—— 其他应用要求

—— 交易凭证要求

7.1 磁条卡终端要求

现有对磁条卡交易的规定对磁条卡终端仍然适用，这些规定也适用于在EMV/PBOC终端上进行的磁条卡交易。因此，收单行应该在交易点执行降级使用(Fallback)规则和处理流程，支持新的芯片服务代码。

7.1.1 降级使用

PBOC终端必须能够同时受理芯片卡和磁条卡，因此它有芯片卡读写器和磁条卡读写器。当一张芯片卡插入到该设备上时，设备将用芯片卡读写器而不是磁条卡读写器来读取信息。

但在某些情况下，芯片卡有可能无法在芯片卡设备上使用，比如芯片卡本身坏了、或芯片卡设备上的读写器发生了故障。在这种情况下，芯片卡将使用它的磁条来进行交易，这种交易我们就称之为“降级使用”(Fallback)交易。由于原先由芯片控制的安全管理现在改为由磁条来执行，这种交易被视为具有较低的安全性。

7.1.1.1 降级使用策略

在实际应用中，必须确定如何处理降级使用交易，以及发生降级使用时所采取的具体步骤。

《银联卡业务运作规章》中规定：终端应首先尝试进行芯片交易，当芯片或芯片读写器不能正常工作时方可进行降级使用交易。

刚实施芯片迁移的市场应该遵守这个基本规范，而对于那些已有芯片实施体验的市场，可以制定更严格的策略来避免某些类型Fallback交易的发生。

7.1.1.2 降级使用的预防与处理

在EMV/PBOC终端中应有相应的软件来保证当芯片卡读写器正常时不会发生降级使用，当芯片卡从磁卡读写器中刷过时，应有提示信息提醒持卡人和商户使用芯片卡读写器。

这可以通过在芯片卡的磁条中使用一个特殊的芯片服务代码（2xx或6xx）来实现，当该芯片服务代码被磁条读写器读到时，则终端不执行该交易，并可显示提示信息。这就能保证在EMV/PBOC终端上处理的芯片卡交易的确是用芯片来实现的。

在《银行卡联网联合技术规范》中，可以通过以下数据信息的组合识别一笔 Fallback 交易：

—— “服务点输入方式码（PAN 输入方式）”不是 05 或 95，表明是一个非芯片卡读取方式。

—— “终端读取能力”是 5，表明是可读取芯片卡的终端。

—— “服务代码”首位是 2 或 6，表明卡片上有芯片存在。

虽然上述Fallback的防止方法目前不是强制需要的，但却是强烈推荐的，因为这将会成为终端设备的一个必备功能。

收单行应该制定一个机制，在芯片卡或芯片读写器发生故障时让磁条读写器能够接纳芯片卡。

比较好的做法是，在读芯片卡失败超过规定次数后，终端即启动磁条读写器，同时向发卡行请求联机处理；如果不支持联机处理，商户可选择打电话人工获得授权；如果磁条卡损坏或者磁条读写器无法工作，则可采取手工输入账号来继续交易。

如果一笔Fallback交易未使用磁条，如：语音交易；商户应清楚表明这是Fallbakck交易，以便发卡行采取合适的动作。

7.1.1.3 执行活动

与降级使用相关的活动包括：

—— 策略

遵循《银联卡业务运作规章》。和本地市场参与者以及银联共同制定国内的 Fallback 策略。应对商户进行 Fallback 操作的培训。详情请查阅 “商户培训”相关章节。

—— 业务

与技术人员和终端供应商协作，确保终端能够提示商户通过芯片读写器读取芯片卡信息。

—— 技术

确认终端能改造成可向商户提示使用芯片进行交易的信息。实施 Fallback 策略，也许需要在终端中添加代码。终端如果支持 Fallback 功能，就应该包含磁条读写器和芯片读写器之间的逻辑转换，以实现在芯片无法读取时，调用 Fallback 功能。

有关识别、实现Fallback交易所涉及终端与收单行的接口以及收单行主系统的改造信息，请参考第9章“收单行系统改造”。

7.1.2 服务代码

PBOC导入了新的服务代码取值，PBOC卡片所包含的服务代码首位必须是以下两个取值之一：

—— 2－国际使用

指明卡片有集成电路芯片，如集成电路芯片可以使用，金融交易应由集成电路处理。

—— 6－国内使用

指明卡片有集成电路芯片，如集成电路芯片可以使用，金融交易应由集成电路处理。

现行的PBOC规则要求所有的具有联机功能的终端能读取服务代码进行交易。收单行必须确保新的服务代码不会在仅支持磁条的终端上被拒绝，这并非一个新的规定，如果现有终端不符合这种要求，则需要对其程序进行改造。

7.1.3 执行活动

在磁条卡终端上支持芯片服务代码所要求的活动包括：

—— 策略

收单行必须确保支持磁条的所有服务代码、以及芯片的等效处理要求。

—— 业务

收单行应在理解新的服务代码取值的影响的基础上，调查分析现有终端。收单行可以向商户发布一个自测工具，或者安排一个工作小组去商户现场测试。为了协助收单行的终端检测活动，银联可以提供使用新服务代码的测试卡。如果已经布放的终端存在兼容性问题，业务部门应与技术人员、终端供应商一起制定并实施一个改造计划。

—— 技术

如果需要，进行终端软件改造以支持新的服务代码，并测试相关功能的正确性。

7.2 电子现金功能

电子现金(EC)是 PBOC 的一个可选功能。通过这个功能，发卡行可以发展主要进行小额现金交易的商户，开拓 PBOC 卡的受理范围，为持卡人提供更多应用以及便捷服务，从而增加 PBOC 卡产品的发行量。因为电子现金交易是脱机完成的，不需要任何联机授权的费用；这种好处、以及交易速度的优势，有助于促进传统使用（小额）现金交易的商户转向接受卡片交易。

电子现金功能与电子钱包的最大不同是：电子现金是基于 PBOC 借记/贷记应用的，使用其非对称密钥体系；而电子钱包采用的是对称三级密钥体系，其密钥传递、更新流程复杂，PSAM 卡安全管理的风险较大。

注： 除非特别指出，否则本文所提到的PBOC、小额支付(EC)应用缺省对应接触式交易方式。

7.2.1 要求概述

支持EC功能的终端首先必须是EMV/PBOC兼容终端。在标准PBOC的基础上，支持EC功能只需要很小的改动。以下大致描述EC终端涉及的改造：

—— 必须认可卡片发起 EC 交易请求，并向其提供一个适当的响应；

—— 建议包含独立的 EC TACs，并对 EC 交易使用它进行处理；

—— 必须能够识别 EC 交易的标志－电子现金发卡行授权码；

—— 对于 EC 交易的终端风险管理，不应该执行随机选择；

—— 可以维护一个独立的 EC 最低限额（可选）；

—— 可以显示或在凭条上打印电子现金可用余额（可选）。

收单行还可以考虑增强其后台系统功能，为了统计和记账目的将 EC 交易从标准 PBOC 交易中区分出来。例如：由于 EC 交易对基础设施的要求较少，相关收单行和发卡行的交易成本会有所降低，因此可以考虑执行一个较低的费率以激励商户。

7.2.2 涉及数据元

电子现金方案在 PBOC2.0 的基础上制定，其卡应用与普通的 PBOC 借贷记卡大致相同。然而为了方便应用，在电子现金方案中新增了一些 PBOC 中没有的数据元，其中终端数据详见下表：

表7 电子现金专有数据元

数据元名称	要求	描述
电子现金终端支持指示器 （EC Terminal Support Indicator）	条件 如果支持 EC	用于指示该终端支持电子现金功能。
电子现金终端交易限额 （EC Terminal Transaction Limit）	可选	终端使用此数据元（如果存在的话）判断一个交易是否以电子现金方式处理。

实现电子现金功能，对 PBOC 原有数据元的使用也会有所不同，有些数据元必须使用，如：交易货币代码。受电子现金影响的终端数据元详见下表：

表8　电子现金影响数据元

数据元名称	要求	描述
授权金额	条件 如果支持 EC	如果支持 EC 功能，卡片会通过 PDOL 要求终端提供数据元：授权金额，用于卡片判断交易金额是否满足 EC 交易条件。
交易货币代码	条件 如果支持 EC	如果支持 EC 功能，卡片会通过 PDOL 要求终端提供数据元：交易货币代码，用于卡片判断是否同币种。

7.2.3　电子现金交易流程

在具备EC受理能力的终端与支持EC功能的PBOC卡片之间的交互包括以下步骤：

1. 在PBOC应用选择阶段，支持EC的卡片会返回PDOL，请求EC终端支持指示器、交易金额和交易货币代码。
2. 终端判断交易类型、是否支持EC、交易金额等因素，设置EC终端支持指示器，提供PDOL请求数据，发送GPO命令给卡片。
3. 卡片判断EC终端支持指示器如为1，则进行以下检查：
   - 交易货币代码是否等于应用货币代码?
   - 交易金额是否小于等于 EC 可用余额?
   - 交易金额是否小于等于 EC 单笔交易限额（如果存在）?
   - 前一笔联机交易的发卡行认证是否成功?
   - 脱机 PIN 尝试数是否没有超限?
4. 如果上述条件都是肯定的，卡片标识本次交易为EC交易，返回EC AIP和AFL给终端。
5. 如果上述任何条件不符合，卡片返回PBOC AIP和AFL给终端。
6. 终端读取相应的应用记录，如果终端发现EC发卡行授权代码存在，就使用EC TACs进行后续处理；否则使用PBOC TACs,后续按标准PBOC流程进行.
7. 在终端行为分析阶段，对于EC交易除了执行原有的处理逻辑，还检查：
   - EC 余额是否小于 EC 重置阈值?
   - 终端是否支持联机?

   终端综合决定请求的密文类型：TC 或 ARQC 或 AAC。
8. 在卡片行为分析阶段，卡片判断是EC交易，按请求的密文类型分别处理：
   - 如果请求 TC，从 EC 余额中扣除交易金额，返回 TC;
   - 如果请求 AAC，返回 AAC;
   - 如果请求 ARQC，返回 ARQC。

   对于配置EC功能的PBOC应用,应该通过发卡行应用数据(Tag‘9F10’)的发卡行自定义数据(IDD)返回 EC 余额。
9. 终端按标准PBOC流程继续处理。
10. 终端在提交的EC清算信息中应包含EC发卡行授权码。

7.2.4　执行活动

实现EC功能所需要的活动包括：

——　策略

- 决定是否支持 EC;
- 决定是否支持独立的 EC 最低限额;
- 决定是否支持 EC TACs;
- 评估和决定选择哪些商户提供这种服务。

—— 业务

与终端供应商交流对 EC 的要求。向供应商描述清楚需求是十分重要的，因为有些供应商的应用软件目前不支持这个功能。

—— 技术

实现 EC 功能，终端必须支持前面描述的一些数据元，如：EC 终端支持指示器。

7.3 非接触式 IC 卡支付

非接触式新技术的发展给现有的金融交易方式和技术环境带来了挑战和变革。为了兼顾持卡人的用卡习惯，并防止交易被中断，关键是在保证交易顺利进行的同时使交易时间尽可能缩短。

《中国银联非接触式IC卡支付规范》（以下简称：非接触规范）提供了两种非接触式界面支付方式：一是磁条非接触式支付(Magnetic Stripe Data，MSD）；二是快速借记/贷记（qPBOC）方式。适用于非接触式界面交易完成时间要求高的场合。

7.3.1 通用要求概述

7.3.1.1 Level 1 要求

符合非接触规范的PBOC终端应满足Level 1要求：

—— 终端应符合《中国金融集成电路（IC）卡规范第 8 部分：与应用无关的非接触式规范》，同时支持 ISO 14443 Type A 和 Type B；

—— 对于 Type B 协议，终端应支持 MBLI=0 和 MBLI=1；

—— 对于 Type A 卡，终端应支持值为 8 的 FWI 和附加的值为 x'B'的 ATS-TB(1)。

7.3.1.2 基本要求

符合非接触规范的PBOC终端应满足的基本要求包括：

1. 终端应支持qPBOC和MSD之一，或同时支持两者。
2. 具有脱机能力的终端应同时支持SDA和DDA。如果卡片支持DDA，则终端应执行DDA。
3. 终端应支持PBOC定义的数据对象列表(DOL)。
4. 终端应通知收单行交易是通过非接触界面完成的，该信息应区别是MSD还是qPBOC交易，并且应包含在授权和清算报文中。

   收单行可通过正确填写联机报文中的强制项－“服务点输入方式码”来提供此信息。
5. 如果卡片返回应用认证密文(AAC)来拒绝交易，交易不应再通过其它界面方式进行。
6. 当进行接触式或磁条刷卡的交易初始化时，终端应下电关闭非接触式界面。
7. 当进行接触式或磁条刷卡的交易初始化时，如果非接触式交易正在进行，终端应终止非接触式交易，放弃从卡片得到的所有数据，然后重新启动其他界面进行交易。
8. 对于非接触交易，终端应明确通知持卡人和商户：
   - 出卡
   - 交易过程
   - 交易结果－批准、拒绝或终止

   推荐的终端信息有：
   - 出卡
   - 读卡成功
   - 处理中
   - 再次出卡（如果交易未完成）
   - 交易批准
   - 交易拒绝
   - 出示单一卡片（防冲突）
   - 插卡或刷卡

   当提示出卡时，终端应显示交易金额(Tag '9F02')。

如果卡片提供“脱机消费可用余额”(Tag ‘9F5D’)时，终端应显示该金额，以表示读卡操作成功，并可能打印在交易凭条上。

7.3.2 快速借记/贷记支付应用

qPBOC 基于 EMV 概念，使用现有的 PBOC 系统和操作规则。通过减少命令和响应次数，qPBOC 降低了终端和卡片之间的处理时间。它还提供了脱机快速小额支付特性、脱机数据认证、以及使用现有密文算法（版本 01）或新的精简算法（版本 17）的联机卡片认证。

为了满足引入了非接触式接口而产生的交易速度上的要求，需要对标准的借记/贷记应用流程进行调整和优化。qPBOC 对指令和交易流程进行了优化，主要体现在：

—— 把多条 EMV 命令压缩成尽可能少的命令，以减少交易的时间；

—— 将卡片和终端的交互过程集中完成，当卡片离开读写器的通讯范围后，终端再进行脱机数据认证、终端风险管理和终端行为分析，并允许卡片离开读卡感应范围之前或之后进行密码操作，使卡片在读写器感应范围内停留的时间尽可能短。

qPBOC 有两大特点：

—— 联机交易采用联机卡片认证；

—— 脱机交易采用脱机数据认证。

7.3.2.1 要求概述

除了对于所有非接触应用的通用要求外，支持 qPBOC 的终端还应当符合下面这些要求：

1. 终端应当支持qPBOC交易预处理。
2. 仅支持qPBOC的终端不应当查询AIP来决定卡片是请求MSD或qPBOC，而应默认qPBOC处理。
3. 支持qPBOC的终端应当按EMV规则读记录，并处理记录或PDOL中不认识的Tag编码的数据元素。
4. 如果qPBOC强制数据元没有被GPO返回，支持qPBOC的终端应当拒绝交易。
5. 如果EMV必需但qPBOC不要求的数据元不存在，支持qPBOC的终端不应当拒绝交易。
6. 支持qPBOC的终端应当在任何要求磁道数据的qPBOC联机报文中提供“磁条2等效数据”。
7. 如果卡片中未提供“卡片交易属性”(Tag ‘9F6C’)数据元，支持签名的终端应该假设卡片要求签名；如果终端要求CVM，应当在单据上打印签名行。
8. 支持超过一个CVM的终端应当查询卡片交易属性的字节1位8和位7决定卡片选择哪个CVM。
   - 如果位 8＝’1’，终端应当执行联机 PIN 校验，不再查询位 7；如果位 8＝’0’，终端应当查询位 7；
   - 除非终端支持联机 PIN，卡片不会设置第 8 位；当前的卡片逻辑不会将位 8 和位 7 同时设置。不过以后增加的 CVM 也许会要求卡片逻辑改变；
   - 如果位 7＝’1’，终端应当在凭条上打印签名行。
9. 对于支持qPBOC和PBOC的终端，如果AIP中指示MSD支持（字节2位8）的位为0，终端按如下处理：
   - 如果应用密文没有出现在 GPO 响应中，按 PBOC 处理；
   - 如果应用密文出现在 GPO 响应中，按 qPBOC 处理。
10. 在如下的任何情形中，脱机数据认证失败且拒绝交易：
    - AIP 中未指示支持脱机数据认证（SDA 或 fDDA）；
    - 或支持 SDA，但 SDA 要求的数据缺失；
    - 或支持 fDDA，但 fDDA 要求的数据缺失。

7.3.2.2 涉及数据元

qPBOC不要求所有EMV强制数据包含在卡片中，或者如果包含在卡片中，也不要求将其读出。以下对qPBOC新增终端数据元以及受qPBOC影响的终端数据元分别予以说明：

表9 qPBOC 专有数据元

数据元名称	要求	描述
近距离支付系统环境（PPSE）文件名	强制	终端通过 PPSE 文件名’2PAY.SYS.DDF01’选择非接触

		支付应用。
非接触最低限额 （Contactless Floor Limit）	可选	指示终端支持的非接触支付应用的最低限额。
非接触交易限额 （Contactless Transaction Limit）	可选	如果非接触交易金额大于或等于此金额，则交易终止。 这种情况下，允许使用其它交易界面尝试交易。
终端执行持卡人验证方法限额 （Terminal CVM Required Limit）	可选	如果非接触交易金额大于或等于此金额，终端要求执行 CVM 处理。 目前 qPBOC 支持两种 CVM：联机 PIN 和签名。
终端交易属性 （Terminal Transaction Qualifiers）	强制	指示终端的处理能力以及对卡片的要求。

注：qPBOC 可以提供脱机的快速小额支付功能，它在 qPBOC 的交易流程中结合了电子现金特性。相关电子现金终端数据元参见“表 7－电子现金专有数据元”。

qPBOC 不支持 EMV 中的 CDOL、DDOL 或缺省 DDOL。所有卡片处理必需的终端数据在 PDOL 中请求；而且依赖于卡片支持的密文类型（01 或 17）以及是否支持脱机 qPBOC 交易，卡片请求的最基本终端数据会有所不同。

7.3.2.3 qPBOC 交易流程

在具备qPBOC受理能力的终端与qPBOC卡片之间的交互包括以下步骤：

1. 交易预处理
   - 终端获取交易金额；
   - 如果交易金额大于等于非接触交易限额（如果存在），转而尝试其它交易界面；
   - 如果交易金额大于非接触最低限额（如果存在，否则使用终端最低限额），标记“要求联机密文”（对仅脱机终端应终止交易）；
   - 如果交易金额为 0，标记“要求联机密文”（对仅脱机终端应终止交易）；
   - 如果交易金额大于等于终端执行 CVM 限额，标记“要求 CVM”；
   - 终端要求出示卡片。
2. 卡片检测处理

   如果同时检测到多张非接触卡，终端应提示只放一张卡。
3. 应用选择
   - 终端使用 ‘2PAY.SYS.DDF01’选择 PPSE；
   - 终端建立双方共同支持的应用列表；
   - 终端选择优先级最高的应用；
   - 终端判断响应的 PDOL 是否包含 “终端交易属性”（Tag ‘9F66’）数据元,如存在则进入应用初始化处理，否则转而尝试其它交易界面。
4. 应用初始化
   - 终端组织 PDOL 要求的数据，向卡片发送 GPO 命令；
   - 卡片接收 GPO 命令，设置中断保护；
   - 如果卡片支持 qPBOC 并且“终端交易属性”标识支持 qPBOC，卡片进行 qPBOC 交易处理；
   - 执行 qPBOC 卡片风险管理；
   - 根据风险管理结果，卡片可以要求终止、拒绝、联机或批准；对应不同的要求，卡片格式化 GPO 响应，返回给终端。
5. 如果终端接收到GPO终止响应（如：状态字=x’6985’），终端终止交易。
6. 如果终端接收到正确的GPO响应，基于密文类型，判断交易联机、脱机拒绝或脱机批准。
   - 如果返回 ARQC，终端请求联机处理：

- 终端应提示持卡人和商户－卡片可以移开，交易正在请求发卡行处理；
- 终端执行所需的 CVM（如：输入联机 PIN）；
- 终端根据发卡行响应批准或拒绝交易。

- 如果返回 AAC，终端脱机拒绝交易；

  注：终端不应再尝试使用其它交易界面进行处理。
- 如果返回 TC：
  - 终端使用 GPO 响应的 AFL，读取附加数据；
  - 如果应用失效日期早于终端交易日期，终端应脱机拒绝交易；
  - 如果应用 PAN 在终端异常文件（如果存在）中出现，终端应脱机拒绝交易；
  - 终端执行脱机数据认证（SDA 或 fDDA），如失败继续判断应联机处理、终止还是脱机拒绝；
  - 如果脱机数据认证通过，终端脱机批准交易。

7.3.2.4 执行活动

实现qPBOC功能所需要的活动包括：

—— 策略

- 决定 qPBOC 终端的具体能力和风险管理要求；
- 决定是否使用非接触最低限额、非接触交易限额、终端执行 CVM 限额；

  由于这些数据元给予收单行对 qPBOC 交易更强的风险控制，银联建议在终端内使用这些数据元。
- 评估和决定选择哪些商户提供这种服务。

—— 业务

- 根据实现功能，与终端供应商交流需要支持的数据元；
- 确定终端交易属性的具体设置；
- 设置非接触最低限额、非接触交易限额、终端执行 CVM 限额（如果支持）。

应与终端供应商充分交流对 qPBOC 的要求。向供应商描述清楚需求是十分重要的，因为有些供应商的应用软件目前不支持这个功能。

—— 技术

实现 qPBOC，终端必须支持前面描述的一些数据元，如：终端交易属性。

7.3.3 磁条非接触式支付应用

MSD 利用从芯片中获得的二磁道等效数据，通过非接触界面来实现磁条式的支付服务。MSD 在磁条支付规则下运营，同时可以增加动态 CVN(dCVN)和密文版本 17 所定义的可选风险管理特性;MSD 无法利用芯片卡可以脱机交易的优势，因此只是一种过渡性解决方案。

本指南不对MSD的实现进行具体描述，收单行如需了解MSD的详细信息，请联系银联代表。

7.4 专有要求

如果要求支持一些专有品牌的卡产品,收单行应规划好怎样在EMV/PBOC兼容终端的框架里实现这些功能。这需要收单行与所处市场相关专有品牌发行机构进行广泛的讨论。

此外，移植到基于芯片的体系架构提供了理想的时机来重新考虑终端的功能和需求，可以与商户、银联一起回顾历史遗留问题。

与专有终端功能相关的活动包括：

—— 策略

和市场上的专有品牌发行机构一起决定任何专有的终端需求。

—— 业务

与技术团队一起确认对专有需求的支持。

—— 技术

改造终端实现和测试专有程序，可由终端供应商提供支持。

注： 银联测试和主机认证的范围不涉及专有功能，测试专有功能由收单行、终端供应商来负责。

7.5 交易类型要求

因为现在还是磁条卡占主导地位的时代，芯片卡终端必须支持各种类型的交易。对于绝大多数交易类型，芯片卡交易与磁条卡交易的处理规则是一样的；在个别情况下，它们有所不同。本节重点描述这些不同之处。

7.5.1 冲正/撤销

如果单信息交易在收到发卡行批准响应后无法完成，需要发起冲正；这对磁条卡和芯片卡交易都是适用的。除了磁条卡交易现有的触发条件，对于芯片卡交易还有新的触发条件。如果发卡行联机批准交易，而随后卡片脱机拒绝该交易，在单信息交易环境中应发起一个冲正。

如果收单行需要处理单信息交易，必须让终端供应商清楚地了解这种新的触发条件要求冲正处理。无需其他的策略、业务和技术活动了。

收单行也应考虑如何处理双信息交易的冲正、恢复持卡人的“授信额度”。

7.5.2 退货

因商品退回或服务取消而引发的退货交易，可分为联机退货和手工退货两种处理方式。芯片卡的联机退货交易使用简化的EMV流程，POS终端通过芯片卡读取卡号、卡序列号、有效期等相关数据；在这种情形下，只需执行应用选择、应用初始化、读应用数据这些步骤，无需执行脱机数据认证、持卡人验证或终端风险管理等步骤。

如果出现PDOL要求交易金额，建议终端送一个零金额给卡片。

7.5.3 信息通知

对于芯片支付应用中产生的一些异常或特殊处理信息，可能要求通知发卡行。例如：

—— IC 卡信息文件

CUPS 制定的 IC 卡信息文件中包含如下两个方面的信息：

- 基于 PBOC 卡失败的脱机交易的记录数据；
- 基于 PBOC 卡虽然卡片验证 ARPC 错误但仍然同意该交易成功的记录数据。

IC 卡信息文件仅做为风险信息参考，与清算无关。

—— IC 卡脚本处理结果

当一笔 PBOC 交易包含发卡行脚本时，收单行需要将发卡行脚本的执行结果以通知报文的方式上送。

与实现信息通知相关的活动包括：

—— 策略

收单行如有特殊的信息通知需求，请与银联代表联系。

—— 业务

在业务手册中描述有关信息通知的要求。

—— 技术

与供应商合作，确保终端支持相应功能。

7.6 其它应用要求

除了PBOC应用，收单行也可以支持其它芯片卡应用。如果准备这样做，收单行应该使其终端有能力正确处理这些应用。

与实现其它芯片卡应用相关的活动包括：

—— 策略

决定准备支持的其它应用类型，例如：积分或储值应用。

—— 业务

在业务手册中描述其它应用及其要求。

—— 技术

与供应商合作，确保终端支持相应功能。

7.7 交易凭证要求

PBOC卡的交易凭证应该包括应用标识符(AID)和交易证书(TC)。

8 完全迁移与部分迁移

PBOC为主机系统改造提供了两种选项：

—— 完全数据选项（简称：Full 选项）

收单行需将终端上送的 PBOC 数据传递到发卡行。选择 Full 选项，从计划的开始就需要对主机系统进行全面的改造。

—— 初步数据选项（简称：Early 选项）

收单行可以在启动 PBOC 迁移计划时，只用 PBOC 终端替换、升级原有设备，暂时不对主机系统进行大的改造；在 Early 选项阶段只需对系统做最小程度的改造，将来升级到完全迁移系统还需要做相应的系统改造。

注： 不论选择哪种改造方式，终端必须满足EMV/PBOC标准。

8.1 概述

PBOC对于授权类、金融类以及清算类交易要求一些新的芯片数据。这些新增数据提供：

—— 在交易点卡片和终端之间的风险管理活动产生的结果，例如：

- 通过脱机数据认证检查伪卡的结果；
- 通过脱机 PIN 进行持卡人验证产生的结果。

—— 数据完整性和数据“克隆”保护的密文信息。

—— 争议处理保护，有利于减少调单和退单请求。

为了使用这些有价值的数据，需要改造收单行主机系统。收单行可以选择开始就支持全部新增数据（Full选项），或者开始仅支持一个最小数据集、在以后某个时间点实现对全部数据的处理（Early选项）。这些选项帮助收单行控制其芯片迁移计划。

《银联卡业务运作规章》要求：受理银联芯片卡的收单机构应实现完全迁移（Full选项）。

8.2 Full 选项

对于Full选项，新的芯片数据域通过终端发送给收单行，并由收单行转发给发卡行。

Full选项有助于在芯片支付服务中取得更好的竞争优势。这些优势包括：

—— 允许发卡行在决定批准或拒绝交易的过程中，使用脱机处理、联机卡片认证的结果进行判断。

—— 减少欺诈

- 允许卡片执行发卡行认证；
- 提供卡片和终端交互的审计凭证；
- 保护数据完整性。

—— 增强客户服务

- 减少调单、退单以及再请款的请求；
- 在交易点提供对交易更深入的观察。

—— 利用供应商的系统优势和可用资源，为实施提供支持。

—— 如果发卡行的基础架构也能支持 Full 选项，那么作为一个整体市场，就可以完全获得芯片卡在风险管理、客户服务等方面的好处。

—— 可以适应已强制要求 Full 选项的国内或国际市场。

—— 激励机制，例如：对于完全数据传送，提供一个较低的交换费率或责任保护。

—— 在一个项目中高效地完成支持芯片数据的改造，尽可能使未来的改造最小化。

8.3 Early 选项

选择Early选项，方便快速推动向芯片卡的迁移，并有助于资源管理。Early选项可以保证PBOC计划对主机系统改造的影响最小化，而将大部分主机系统的改造工作，推迟到以后向Full选项迁移的阶段。收单行Early选项是向Full选项转换的过渡步骤，可以根据具体情况，来选择完全实现PBOC计划的时机。因此，PBOC主机系统的改造可以作为一个长期的升级计划，这样有助于收单行的实施和成本控制。

新的芯片数据提供了交易点发生活动的可见性，以及数据“克隆”和争议保护。实现Early选项，收单行将在终端层或主机层截去芯片数据；因此，Full选项所提供各种好处对于Early选项是不可用的。

选择Early选项的收单行，推迟了主机系统的改造，并且可以从在销售点部署EMV/PBOC终端中取得好处。这些好处包含如下几点：

—— 在交易点利用脱机 PIN 和脱机数据认证，可以防御失窃卡、伪卡交易。

—— 通过芯片终端系统架构，向商户提供增值服务，例如：积分计划和电子礼券。

—— 在限制收单行主机系统改造范围的情况下，能够尽快推出 PBOC 终端。

- 快速反应市场需求；
- 有助于提高与终端部署相关的市场激励机制。

—— 在项目工程的第一个阶段集中致力于终端的部署，而延迟大部分主机系统的改造工作。

Early 选项也存在一些局限性，包括：

—— 无法提供最高级别的欺诈保护。

—— 无法提供联机卡片认证保护。

—— 当卡片请求联机处理时，无法将检查结果提供给发卡行；从而使欺诈风险管理复杂化了。

—— 当发生争议时，采用 Early 选项的一方处于弱势地位。

8.4 PBOC 交易流程

标准PBOC交易流程一般包括以下步骤：

1. 初始化交易

   芯片卡插入芯片读写器、或通过磁条读写器刷卡。如果刷卡，终端检查磁条中的服务代码，判断是否一张芯片卡：

   - 如果服务代码表明其并非芯片卡，终端按磁条卡交易继续处理；
   - 如果服务代码表明是芯片卡，终端提示营业员使用芯片。

2. 应用选择

   终端将卡片支持的应用与其支持的应用进行比较：

   - 如果卡片和终端没有共同支持的应用—交易中止；
   - 如果卡片和终端只有一个共同支持的应用、并且不要求持卡人确认—选择这个应用；
   - 如果卡片和终端共同支持多个应用、或者只支持一个应用但要求持卡人确认—终端显示应用列表供持卡人选择、或基于发卡行优先级列表进行选择（不管是否要求持卡人确认）。

   应用选择完成。

3. 应用初始化处理

   终端通知卡片交易开始，卡片发送数据和风险管理信息给终端以供交易过程中使用。在响应中，卡片执行了以下步骤：

   - 限制检查（可选）

     卡片可以检查是否交易发生环境是其不允许的。如果该应用不支持这种交易，卡片指引终端选择另一个应用。

   - 卡片发送 AIP 和 AFL 给终端（强制）

     卡片可以基于交易环境返回不同的 AIP 或 AFL，AFL 指定了终端应该从卡片读取哪些记录。例如：卡片可以为国内/国际交易返回不同的 AIP 和 AFL。

   - 读应用数据

     终端读取处理交易所需的卡片数据，准备脱机数据认证需要使用的数据。

4. 脱机风险管理

执行脱机交易检查（如果卡片支持），决定交易应该脱机（批准/拒绝）还是联机处理。如果交易必须联机处理，终端将发起联机交易请求。

以下脱机处理检查可以按任意顺序执行：

- 脱机数据认证

  脱机数据认证可以执行以下三种方式之一：

  - 静态数据认证(SDA)
  - 动态数据认证(DDA)
  - 复合 DDA/应用密文生成(CDA)

  脱机数据认证结束，终端将处理结果记录到 TVR 中；如果脱机数据认证没有执行，交易必须请求联机处理。

- 处理限制

  终端执行以下检查：

  - 有效期检查
  - 失效期检查
  - 应用用途控制检查
  - 应用版本号检查

- 持卡人验证

  终端读取卡片的 CVM 列表，选择最合适的 CVM 用于本交易。终端和商户验证持卡人的合法性、以及卡片并未失窃。

  PBOC 支持以下持卡人验证方法：

  - 无需 CVM
  - CVM 处理失败
  - 脱机明文 PIN
  - 脱机明文 PIN 和签名
  - 联机 PIN
  - 签名
  - 出示身份证件

- 终端风险管理

  终端基于收单行风险控制特征执行一系列检查：

  - 最低限额检查
  - 异常文件检查
  - 频度检查
  - 随机选择

  其检查结果供终端行为分析来决定交易将脱机批准、脱机拒绝、或请求联机。

5. 终端行为分析

终端针对脱机处理结果(TVR)使用卡片和支付系统设置的行为规则(IAC/TAC)决定如何继续交易，终端相应请求一个密文：

- 脱机批准—交易证书(TC)
- 脱机拒绝—应用认证密文(AAC)
- 请求联机—授权请求密文(ARQC)

6. 卡片风险管理

允许卡片代表发卡行执行频度检查和其它风险管理检查，判断是否同意终端的决定。

卡片可以执行以下检查：

- 新卡检查

- 上次交易检查
- 频度检查

一旦卡片完成风险管理检查，它将使用以下三种密文之一响应终端的密文请求：

- 脱机批准—TC
- 脱机拒绝—AAC
- 请求联机—ARQC

卡片可以返回与终端请求类型不一样的密文，如终端请求脱机批准，卡片可以返回联机处理或脱机拒绝；终端请求联机处理，卡片可以返回脱机拒绝；但如果终端请求脱机拒绝，卡片只能返回脱机拒绝。

7. 联机处理

通过终端行为分析和卡片行为分析，卡片和终端决定交易请求联机处理。卡片为联机处理生成一个 ARQC 并传递给终端，终端获取 ARQC、芯片用于生成这个密文的原始数据以及脱机风险管理检查的结果，将这些数据联机发送给收单行。

实现 Full 选项的收单行将这些数据按规定格式组装到交易报文中，转发至 CUPS。

8. CUPS处理收单行交易请求

如果是发往一个 Early 状态发卡行，CUPS 将删除所有芯片数据（23、55 域）、代为校验 ARQC（双方需签订相关协议），并将检验结果发送至发卡行。

如果是发往一个 Full 状态发卡行，所有芯片数据将转发至发卡行；Full 状态发卡行也可以选择 CUPS 代检验服务。

9. 发卡行接收交易请求

如果发卡行处于 Early 状态，它需要分析 CUPS 代检验 ARQC 的结果。

Full 状态发卡行需要：

- 检验 ARQC（联机卡片认证）
- 分析 CVR
- 分析 TVR
- 分析其它脱机处理结果

发卡行做出交易决定后，发送响应报文给 CUPS。响应内容可以包括：

- 授权响应密文(ARPC)—由卡片进行检验（可选）
- 发卡行脚本（可选）

10. CUPS处理发卡行响应

如果响应报文来自一个 Early 状态发卡行且要求代检验服务，CUPS 代为生成 ARPC，发送至收单行供卡片执行发卡行认证。

11. 收单行处理发卡行响应

收单行将响应信息发给终端，终端将发卡行授权响应结果、发卡行脚本发给卡片进行处理，其中将涉及一系列计数器的重置。

卡片使用授权响应决定批准或拒绝交易：

- 卡片检验 ARPC，确保响应来自一个有效的发卡行；
- 卡片验证并执行发卡行脚本命令（如果存在）。

卡片生成最终密文：批准交易为 TC、拒绝交易为 AAC，TC 及计算 TC 的相关数据可以作为交易确认依据。

12. 清分与清算

对于联机批准和脱机批准的交易，卡片都会生成一个最终密文—交易证书(TC)。

- 如果交易被脱机拒绝，卡片生成一个 AAC。

  脱机拒绝交易的详细信息通过“IC 卡信息文件”传送给发卡行。

- 收单行提交脱机批准交易给 CUPS 进行清分、清算。
  脱机批准交易的详细信息通过“IC 卡脱机消费文件”传送给发卡行。

注： 以上交易流程对应Full状态收单行。Early状态收单行对于联机请求报文将在终端层或主机层截去芯片数据（23、55域），后续联机处理同磁条卡交易。

9 收单行系统改造

收单行系统改造的具体内容包括：

—— 终端管理系统

—— 终端与收单行接口

—— 主机系统

注： 本章节适用于所有的销售点终端。

9.1 终端管理系统

为了实现PBOC和其它芯片卡计划，需要对原有的终端管理系统进行升级改造。对于PBOC，收单行应该具备在完成部署后校验终端数据、升级终端数据要素的能力。

为了能够在不对系统架构进行大改动的情况下实现系统改造，原有终端管理系统需要具有足够的稳定性和灵活性。原有终端管理系统的灵活性越好，就越容易扩展并适应将来的业务需要。

在终端部署后需要校验、更新的数据元一般包括：

—— PBOC 根 CA 公钥

- 支持根 CA 公钥安装、跟踪、撤回（用于支持 SDA、DDA 或 CDA 的终端），终端必须具备存取、增加、移除公钥的能力；
- 确保终端能够安全地存储最多 6 个 PBOC 根 CA 公钥（及其关联数据）；
  目前有效的公钥长度在 1024 比特与 1984 比特之间。有关公钥的更多信息，请参见《金融 IC 卡借记/贷记应用根 CA 公钥认证规范》；

—— 磁条卡/芯片卡交易最低限额；

—— 应用标识符（AIDs）；

—— 应用版本号；

—— 随机选择参数（用于同时具备联机和脱机能力的终端）；

—— 处理限制参数。

9.1.1 Full/Eearly 选项参数

如果收单行目前实施部分迁移（Early选项），并且在终端就截去新的芯片数据；建议收单行在终端管理系统中通过一个参数来管理这些数据。这样做的话，当收单行实施完全迁移（Full选项）时，只需修改这个参数即可将芯片数据发给收单行主机系统，而无需逐个对终端或MIS商户系统进行改造。

除了PBOC，依据对芯片迁移的商业策略，收单行可以改造终端管理系统以支持其它芯片应用、或其它支付系统应用。

9.1.2 执行活动

终端管理系统改造具体实现的业务和技术活动包括：

—— 业务

终端管理系统能够在终端部署后对终端数据元进行校验。为了适应当地市场、PBOC 改造和其它芯片应用的需要，终端管理系统必须对终端数据元做相应调整。

—— 技术

扩展终端管理系统体系结构，以保证支持芯片数据元（对于 PBOC 和其它芯片应用）和终端部署后的数据校验的灵活性。在内部资源不是很充足的情况下，可与供应商协同对终端管理系统进行改造。

9.2 终端与收单行接口

PBOC为终端与收单行接口导入新的数据元。终端必须能受理有效的卡片和交易数据，并将数据按照接口数据格式进行转换。

终端与收单行接口的改造量取决于选择Early选项还是选择Full选项。本章节的信息假设你已经对选择Early选项还是选择Full选项作出了决定。相关信息请参考第5章“完全迁移与部分迁移”。

除了终端和收单行接口数据格式外，Early选项和Full选项与终端功能是相互独立的。尽管Early选项允许数据在终端或收单行主机被截除以最小化系统改造，但是这两种选项都要求遵循EMV/PBOC规范的终端具有传输完全芯片数据的能力。

可以根据当地市场情况，确定终端与收单行接口信息需求。但是收单行与CUPS的接口必须符合《银行卡联网联合技术规范》的要求。

9.2.1 Full 选项

如果支持Full选项，必须升级终端与收单行接口报文，以支持新增数据。由于这些接口信息对各个银行来说是专有的，银联不介入这个处理过程。为了帮助收单行理解这些报文所要求的数据，EMV和PBOC对终端与收单行接口数据给出了最小集定义。

建议收单行通过借鉴、分析CUPS报文所要求的数据，确定其终端与收单行接口需要进行的改造。

相关活动主要涉及技术支持部门：

—— 技术

与 PBOC 计划的参与者协同决定如何生成新的终端与收单行接口报文。系统改造后，建议对终端与收单行接口以及与 MIS 商户系统的接口进行测试，确保交易正确处理。

9.2.2 Early 选项

对于Early选项，收单行可以选择在终端层或者主机系统层截去新增芯片收据；不管是哪一种情况，都必须正确传递最小要求的Early数据值。

—— 策略

决定在终端层还是在主机层截去新增芯片数据。

推荐 Early 选项收单行在主机层进行数据截除，如果选择在终端层进行数据截除，推荐的做法是在终端管理系统中使用参数对数据截除进行管理。详细信息请参考第 8.1 节 “终端管理系统”。

在终端层进行数据截除推迟了终端与收单行接口的改造，但是当系统迁移到 Full 选项时，需要对终端进行改造。而在主机层进行数据截除，当迁移到 Full 选项时，就不需要对终端进行改造了。

—— 业务

在操作和技术手册、培训材料中对数据截除进行描述。

—— 技术

这项工作主要由技术支持部门来承担；根据在终端层或主机层截去数据，工作内容有所不同：

- 在终端层进行数据截除

  需要与终端供应商协同落实改造任务。通过分析第 9.3 节“主机系统”对 Early 选项数据处理的要求，可以帮助明确终端与收单行接口的数据要求，决定在终端层截去哪些数据。改动完成后，需要测试终端与收单行或 MIS 商户系统接口以保证交易被正确执行。

- 在主机层进行数据截除

  Early 选项和 Full 选项对于终端与收单行接口改造的要求是一样的。主机系统必须能够接受终端数据，但没必要将终端数据填加到发送给 CUPS 的报文中。在主机层进行数据截除的相关技术实现，请参考 9.3.1 节“Full 选项”。

9.2.3 Fallback

当芯片卡在芯片处理终端上通过磁条信息进行交易时，发生的交易被认为是降级使用(Fallback)交易。这种交易被认为安全性较低，因为磁条卡受理避开了芯片卡受理所提供的控制和风险管理保护。

需要在终端与收单行接口信息中明确标识降级使用交易。由于这些信息格式是专用的，必须结合本地市场的需要确定如何改变。终端与收单行接口格式需要包含足够的信息，以便在收单行与CUPS的接口信息中能够正确标识降级使用交易。

通常，必须在终端与收单行接口报文格式中包括以下信息，以标识出降级使用交易：

—— 交易是由磁条发起的（22 域）

—— 交易是在芯片受理终端上发生的（60.2.2 域）

—— 由卡片的磁条发起交易的服务代码是 2xx 或 6xx（35 或 45 域）

请查阅9.3.3节获得“降级使用”的详细内容。

相关活动主要涉及技术人员：

—— 技术

进行系统改造，以便在终端与收单行接口报文中识别 Fallback 交易。

9.3 主机系统

本节提供了Early选项和Full选项相关主机系统的改造概要。关于选择Full选项或Early选项的各自利弊，请参见第8章“完全迁移与部分迁移”。

9.3.1 Full 选项

Full选项要求的系统改造工作比Early选项广泛的多，但它能够提供更有价值的收益，例如：“克隆”和争议保护。收单行主机系统需要对交易报文、清算文件支持一些新的数据域。

在CUPS中，对于联机交易报文，绝大多数新增数据集中存放在“IC卡数据域”（55域）中；对于清算信息，绝大多数新增数据存放在“段2－基于PBOC 借/贷记标准的IC 卡特征信息”中。

表10 新增 PBOC 数据元

域名	描述	转接系统（域/Tag）	文件系统（段/位移）
服务点输入方式码	持卡人数据（如 PAN 和 PIN）的输入方式。	22	段 2，16-18
卡序列号	用于区别具有相同 PAN 的不同卡。只在 IC 卡交易时使用。	23	段 2，19-21
应用密文	由 IC 卡生成的应用密文（TC，ARQC 或 AAC）	55－9F26	段 2，0-15
密文信息数据	表明卡片返回的密文类型并指出终端要进行的操作。	55－9F27	段 2，198-199
发卡行应用数据	在一个联机交易中，要传送到发卡行的专有应用数据。 第 1 字节是 PBOC 自定义数据长度。 格式内容： 长度（07）（1 字节） 分散密钥索引（1 字节） 密文版本号（1 字节） 卡片验证结果（CVR）（4 字节） 算法标识（1 字节） 如果由发卡行自定义数据。在上述数据后跟一个发卡行自定义数据长度字节和 1-15 字节的发卡行自定义数据。	55－9F10	段 2，56-119
不可预知数	包含一个随机数，用于生成应用密文，以提供可变性和唯一性。	55－9F37	段 2，40-47
应用交易计数器	记录个人化以后交易处理的次数。由卡片中的应用维护。	55－9F36	段 2，120-123
终端验证结果	用于记录终端执行各 PBOC 功能处理结果的一	55－95	段 2，30-39

	组指示位。例如：脱机数据认证结果。		
交易日期	交易授权的本地日期	55－9A	段 2，128-133
交易类型	根据 ISO 8583:1987 定义的处理码前 2 位表示的金融交易类型	55－9C	段 2，181-182
授权金额	存储当前交易的金额	55－9F02	段 2，183-194
交易货币代码	根据 ISO 4217 规定的交易货币代码	55－5F2A	段 2，195-197
应用交互特征	一个列表，说明此应用中卡片支持指定功能的能力。	55－82	段 2，124-127
终端国家代码	根据 ISO3166 表示的终端国家代码	55－9F1A	段 2，134-136
其它金额	与交易相关的第二金额，表示返现金额	55－9F03	段 2，200-211
终端性能	表示终端的卡片数据输入、CVM 支持和安全能力	55－9F33	段 2，24-29
持卡人验证方法结果	表示最后一次持卡人验证方法执行的结果	55－9F34	段 2，212-217
终端类型	指示终端环境、通讯能力和操作控制	55－9F35	段 2，218-219
接口设备序列号	厂商分配给终端 IFD 的唯一、永久的序列号	55－9F1E	段 2，48-55
专用文件名称	根据 ISO7816-4 规定的 DF 的名字	55－84	段 2，220-251
应用版本号	支付系统给应用分配的版本号	55－9F09	段 2，252-255
交易序列计数器	终端维护的每笔交易递增一的计数器	55－9F41	段 2，256-263
发卡行认证数据	用于发卡行认证的数据，从发卡行传来由终端送入卡片。 本版本中，发卡行认证数据包括两部分： ARPC（8 字节） 授权响应码（2 字节）	55－91	－
发卡行脚本模版 1	模板中包括在第二次生成应用密文指令前，传送给卡片的发卡行专有脚本数据。	55－71	－
发卡行脚本模版 2	模板中包括在第二次生成应用密文指令后，传送给卡片的发卡行专有脚本数据。	55－72	－
发卡方脚本结果	记录卡片对发卡行脚本指令处理的结果，此结果要包括在清算报文和下次联机授权中。	55－DF31	段 2，137-178
终端读取能力	该值是一个十进制数字代码，在 IC 卡交易中表明终端是否能够读取 IC 卡。	60.2.2	段 2，23-23
IC 卡条件代码	表示当在 IC 卡终端上使用 IC 卡的磁条信息时，IC 卡终端的 IC 卡读写能力是否可用。根据该域的值可以判断卡片或终端有无损坏，同时也可判断是否是伪卡交易。	60.2.3	－
IC 卡验证可靠性标志	在 IC 卡交易中表明该卡验证的可靠性。受理方在商户或终端碰到问题时会设置该值；或者由 CUPS 在受理方或发卡方都不能执行该卡的验证时设置该值。	60.2.7	－

注： 此表也包含针对PBOC增加新的取值或子域的原有数据域（如：22域、60域）。

收单行主机系统支持Full选项所要求的活动包括：

—— 技术

技术团队需要评估完全迁移对主机系统的影响。收单行或是内部开发、或是雇佣主机系统供应

商、或是依靠第三方处理商，不同的情况决定采用不同的技术支持：

- 内部开发—实现完全迁移对于收单行意义重大，需要启动一个正式的项目计划。首先必须从每个人员较多的技术部门抽调人员建立一个具有各方面代表性的技术团队，并把一个项目经理和这个团队分配给这个项目。同所有正式项目一样，项目计划、定期会议、会议时间、会议议题列表都必须有一个完整的制订流程。业务需求、技术需求、设计文档、以及测试和质量保证过程都是必须的。开发时间期限取决于收单行的具体情况。附录 A 中提供了项目实施计划模板。
- 主机系统供应商—大多数收单行都使用主机系统供应商提供定制的软件来满足他们的特定需求。这些收单行需要安装供应商软件，然后对系统做些调整来满足其需求。完成软件定制后，建议必须彻底地测试整个系统。
- 第三方处理商—通过第三方处理商进行收单，需要对其处理系统进行测试。

开发完成后，必须测试系统以确保交易处理过程的正确性。

无论特定的实现过程如何，所有实现完全迁移的收单行都必须通过 CUPS 的主机认证。详细内容请参考第 11 章 “收单行主机认证”。

9.3.1.1 电子现金交易

标准 PBOC 下的电子现金交易都是脱机消费交易，其上送的清算信息至少应新增数据项：电子现金余额、电子现金发卡行授权码。

支持电子现金功能的 PBOC 终端，执行标准 PBOC 应用请求联机处理时一般应上送数据项：电子现金余额，供发卡行进行自动圈存检查、风险监控等处理。这个数据项存放在原有 Tag-‘9F10’的 IDD 部分，对报文的转接不会产生新的影响。

9.3.1.2 qPBOC 交易

在已经支持标准 PBOC 的基础上，qPBOC 交易处理所要求的系统改造并不大，主要是对已有数据域支持新的取值：

—— 服务点输入方式码

PAN 输入方式 07－qPBOC 输入。

—— 终端读取能力

6－终端有非接触读卡能力。

—— IC 卡数据域

可能增加新的 Tag 或数据。如：对于 qPBOC 联机交易，如果卡片支持返回脱机消费可用余额，将在发卡行应用数据(Tag ‘9F10’)的发卡行自定义数据(IDD)部分收到对应的值；发卡行可以据此监控、分析脱机资金的使用情况，加强风险管理。

9.3.2 Early 选项

Early 选项要求的系统改造是最小限度的。收单行主机系统必须对授权类、金融类交易的现有数据域支持新的取值；另外对于清算文件也需对现有段(BLOCK)支持新的取值。

—— 服务点输入方式码（22 域）

“服务点输入方式码”就是持卡人数据（如 PAN 和 PIN）的输入方式。

- PAN 输入方式 05－集成电路卡，卡信息可靠；
- PAN 输入方式 95－集成电路卡，卡信息不可靠；

—— 终端读取能力（60.2.2 域）

该值是一个十进制数字代码，在 IC 卡交易中表明终端是否能够读取 IC 卡。

- 新值 5－可读取 IC 卡。当“PAN 输入方式”取值 05 或 95 时，该域必须填 5。

收单行主机系统支持Early选项所要求的活动包括：

—— 技术

技术团队需要评估部分迁移对主机系统的影响。收单行或是内部开发，或是雇佣主机系统供应商，或是依靠第三方处理商，不同的情况决定采用不同的技术支持。需要通过内部开发或与主

机系统供应商合作或与第三方处理商合作，来实现在现有域中支持新的数据。

开发后需要测试系统，以确保交易正确处理。

9.3.3 Fallback

当芯片卡在芯片处理终端上通过磁条信息进行交易时，发生的交易被认为是降级使用(Fallback)交易。这种交易被认为安全性较低，因为磁条卡受理避开了芯片卡受理所提供的控制和风险管理保护。

由于发卡行可能对Fallback交易做不同处理，所以收单行需要在发给CUPS的报文中标识Fallback交易。可以通过以下数据域的组合实现这一点：

—— “PAN 输入方式”为 02 或 90（22 域），表示交易是由磁条发起的；

—— “终端读取能力”为 5（60.2.2 域），表示交易是在芯片受理终端发生的；

—— “IC 卡条件代码”为 1 或 2（60.2.3 域），指示磁条上的“服务代码”是 2xx 或 6xx（35 或 45 域），表示卡片上存在 EMV/PBOC 兼容芯片。

与Fallback相关的活动包括：

—— 技术

进行系统改造，以便在收单行主机系统报文中识别 Fallback 交易。

—— 风险管理

收单行应该监控 Fallback 的发生情况，确保避免在一个不完善的终端出现大量 Fallback 交易、以及商户违反业务运作规章甚至串谋作弊的现象发生。

10 公钥管理

本章描述了在收单行终端支持脱机数据认证的公钥管理活动。对于不执行这些功能的PBOC终端，公钥管理活动不是必须的。

注： 在加载生产密钥之前，收单行应该删除所有测试密钥以避免发生脱机数据认证失败的情况。

注： SDA、DDA和CDA都使用同样的RSA公钥技术。

对于PBOC收单行来说，不需要执行新的DES密钥管理活动。另外，已经实现的联机PIN校验处理过程暂时不需要任何的修改。

10.1 PBOC 根 CA 公钥

这些公钥用于支持SDA、DDA和CDA。任何支付方案最多只能有6个公私钥对有效，因此终端管理系统为每个RID最多存储6个公钥。如需获取PBOC根CA公钥，请联系银联代表。

按计划升级至新密钥以及加速回收旧密钥，都要求在所有EMV/PBOC终端能够实现密钥更新；部署后的数据完整性也必须得到检验。

表11 PBOC 根 CA 公钥发布流程

步骤	动作
1	收单行填写“成员机构根 CA 公钥证书申请表”，以加密签名的电子邮件提交。
2	银联根 CA 认证管理部门批复申请。
3	银联审核员以加密签名的电子邮件指导收单行安全员下载根 CA 公钥证书。
4	收单行安全员验证根 CA 公钥证书，并将验证结果通知银联审核员。
5	收单行将有效的 PBOC 根 CA 公钥加载到终端；在传递过程中必须保证公钥信息的数据完整性并进行信息源认证。

注： 有关申请PBOC根CA公钥的详细信息，请参见《金融IC卡借记/贷记应用根CA公钥认证规范》。

10.2 执行活动

与公钥管理相关的策略、业务和技术活动包括：

—— 策略

银联会定期重新评估 PBOC 根 CA 公钥的失效日期，评估的结果可能是：现有密钥需要回收、导入新的密钥和密钥长度、或延长当前密钥的生命周期。一旦发生变动，银联会发布并通知成

员机构相关策略细节，包括：密钥长度、公钥指数、失效日期、按计划回收时间表等。

—— 业务

定位 PBOC 根 CA 公钥以及其它支付方案的公钥，与技术部门一切确保这些密钥正确加载到终端。

注：每一个支付方案都使用自己独立的公钥。

按照 EMV 规范，终端对每个支付方案最多支持 6 个公钥、密钥长度最长可达 1984 比特。目前银联支持 4 种不同长度的公钥（1024/1152/1408/1984 比特），这些密钥必须按正确的格式存放在终端管理系统，终端管理系统应该在下载密钥前确认是与一个有效的终端在通讯。

收单行必须移除失效、回收的密钥。目前 PBOC 根 CA 公钥的失效日期规定如下：

表12 根 CA 公钥长度及其失效日期

公钥长度	失效日期
1024 比特	2009 年 12 月 31 日
1152 比特	2014 年 12 月 31 日
1408 比特	2017 年 12 月 31 日
1984 比特	2017 年 12 月 31 日

因为这些密钥是有生命周期的，一旦失效，它们就应该被移出终端。同样，如果一个密钥发生泄漏，它将被提前回收；泄漏密钥也必须被移出终端。另外，新增密钥需要加载到终端，业务部门必须制订终端实现密钥升级和密钥置换的处理流程。PBOC 定义了密钥置换、回收的基本要求，具体细节参见《中国金融集成电路（IC）卡规范第 7 部分：借记/贷记安全规范》。

收单行应与其供应商一起确保终端支持所有有效的密钥和密钥长度。

—— 技术

- 获得 PBOC 根 CA 公钥证书，进行验证并从中提取 PBOC 根 CA 公钥。
- 在终端部署之前，对其加载 PBOC 根 CA 公钥。
- 如果需要，通过下载方式升级、置换现有密钥。
- 确保下载密钥信息的数据完整性。
- 通过终端维护已配置的密钥状态，例如：确保终端没有丢失任何密钥、也没有多余的密钥、所有的密钥都是有效的。
- 在实施过程中，终端供应商应能支持预先加载密钥到终端。

11 收单行主机认证

本章描述了实现 PBOC 迁移所要求的收单行主机认证。主机认证对于实现 Full 选项的收单行是必须的，对于实现 Early 选项的收单行是可选的。

注：《银联卡业务运作规章》要求：受理银联芯片卡的收单机构应实现完全迁移（Full选项）。

本文未涉及 PBOC 迁移的其它测试事项，如：终端、内部系统、后台处理以及前端处理等。由于 PBOC 迁移涉及范围很广，对各个组成部分有必要进行全面的测试。这些工作也应该包含在收单行测试计划中。

银联提供测试工具协助收单行进行主机认证。如需进一步了解银联测试工具，请联系银联代表。

11.1 认证环境

一旦完成 PBOC 系统改造的内部测试，收单行就需要准备进行银联主机认证。认证过程的第一步是确保所需部件的到位：

—— 银联测试工具；

—— PBOC 认证脚本；

—— 个人化就绪的芯片测试卡；

—— CUPS 的连通；

—— 生产就绪终端。

注： 在加载生产密钥之前，收单行应该删除所有测试密钥以避免发生脱机数据认证失败的情况。

联系银联代表获取认证脚本以及其它认证材料。

银联建议：收单行在预定联机测试之前 1-2 周，使用磁条卡测试交易测试一下与 CUPS 的连通性。这样如果出现连通性问题，就有时间及时解决之。

11.2 认证流程

本节概要介绍了实现 Full 选项的收单行主机认证过程。收单行必须按照认证测试脚本执行一系列交易，以证明收单行主机系统能够发送和接收每个报文的新增数据域。

下表总结了收单行主机认证的重要步骤：

表13 收单行主机认证

步骤	责任方	活动
1	技术	提交收单行主机认证申请表。包括：机构信息表、终端信息表等。 联系银联代表获取这些表格。
2	银联	审批收单行主机认证申请。
3	银联	银联提供测试工具(PBOCIT)和测试卡，包括：测试案例库、相关文档。
4	银联	银联为收单行安排测试培训。
5	技术	使用银联测试工具，执行脱机测试。
6	技术	提交脱机测试报告，银联进行测试评审（5 个工作日）。
7	技术	使用磁条卡交易测试与 CUPS 的连通性。
8	技术	执行通过 CUPS 的联机测试。
9	技术	如果认证通过，收单行将收到银联签发的完成通知（5 个工作日）。如果认证未通过，收单行需要与银联代表联系确定下次认证时间安排。

注： 银联PBOC借记/贷记收单机构入网测试还包括“终端认证”，发卡行每新增一种PBOC终端型号、或PBOC根CA公钥发生变化、或终端硬件/软件变化可能影响到联网通用，都需要进行终端认证。有关终端认证的详细信息，请咨询银联代表。

12 收单行后台系统改造

本章描述了支持PBOC计划的后台功能改造。主要包括以下几个方面：

—— 交换费率
—— 记账
—— 争议处理
—— 报表
—— 内部员工培训
—— 执行活动

12.1 交换费率

请联系银联代表，获取有关手续费和网络服务费的详细信息。

12.2 记账

PBOC迁移计划的实施，不会为收单行带来新的收费种类；银联记账和收费方式也不会发生变化。如需进一步了解相关详细信息，请联系银联代表。

12.3 争议解决

PBOC的新型交易数据及流程对处理客户争议、退单、再请款和仲裁会有影响，需要分析这种变化对后台差错处理过程的潜在影响。差错处理允许收单行通过提供交易凭证对发卡行的退单做出反应、发起再请款。收单行还需要分析相关差错处理和争议解决的改造对主机和客户服务系统所带来的影响。

—— 芯片数据可以用于响应退单交易，所以需要保存更长的时间，需要对系统进行改造以支持数据的保存。比如说一直到 180 天。可以通过访问芯片数据，得到有关争议事项的信息。

—— 评估对芯片数据可能需要的显示方式，比如说以报表的形式或者是在屏幕显示方式。

—— 明确系统需要获取、处理、存档或备份的对争议解决有影响的芯片数据，然后根据需要进行改造。

—— 支持为 PBOC 新增的差错原因码。

表14 新增差错原因码

差错应用码	描述
6308	交易有疑问索取交易证书(TC)及相关的计算数据。
4558	交易证书(TC)验证失败。
4559	不能提供 TC 及相关计算数据。

12.4 报表

本节描述了受理芯片交易对报表的影响。报表的改造涉及以下几点：

—— 芯片交易统计；

—— 降级使用(Fallback)交易；

—— 增强报表功能。

12.4.1 芯片交易统计

建议至少应区分芯片交易和磁条交易，这将有助于监控PBOC迁移计划的发展、商户服务活动的有效性、芯片处理的风险管理优点。而且将有助于满足银联未来对报表提出的需求。

对于大部分报表来说，保持现有格式在同一张报表上提供芯片卡和磁条卡交易信息是比较可行的。应该跟踪芯片交易金额和交易量，这些统计数据在结算、客户服务、仲裁、欺诈以及服务评估等报表中都应有所体现。

可以利用以下数据元素识别芯片卡发起的交易：

—— “PAN 输入方式”为 05 或 95（22 域），表示交易是由磁条发起的；

—— “终端读取能力”为 5（60.2.2 域），表示交易是在芯片受理终端发生的。

12.4.2 Fallback 交易

如果本地市场允许Fallback交易，必须对这种交易进行监控并提供报表。当一张芯片卡以读取磁条的方式在可受理芯片卡的终端上做交易，发生的交易视为Fallback交易。可以通过商户或终端跟踪Fallback交易。大量发生的Fallback交易表明终端存在问题（可受理芯片卡的终端不能正常运行）或商户使用不正确的操作流程（商户在受理芯片卡时使用磁条、而不是使用芯片）。

可以利用以下数据域的组合来识别Fallback交易：

—— “PAN 输入方式”为 02 或 90（22 域），表示交易是由磁条发起的；

—— “终端读取能力”为 5（60.2.2 域），表示交易是在芯片受理终端发生的；

—— “IC 卡条件代码”为 1 或 2（60.2.3 域），指示磁条上的“服务代码”是 2xx 或 6xx（35 或 45 域），卡片上存在 EMV/PBOC 兼容芯片。

当报表显示发生了大量的Fallback交易，应该和商户协作进行调查，可能需要就芯片卡受理流程对商户进行再次培训。如果问题依然存在，则需要制定奖惩措施。

请查阅文档中与Fallback交易相关的的其他章节，包括7.1节“磁条卡终端要求”中有关Fallback交易的策略、业务和技术活动、13.4节“商户培训”中关于如何对商户培训Fallback交易、9.3.3节“Fallback”中有关系统改造的描述以及9.2.3节“Fallback”－如何在终端与收单行接口中标识Fallback交易。

12.4.3 增强报表功能

PBOC 交易提供的数据，能够清晰地反映卡片和终端的交互情况。在收单行实现 Full 选项的过程中，正好有机会利用这些数据来增强管理报表的功能。可以考虑增强以下报表：

—— 芯片卡交易报表；
—— 欺诈类报表，突出磁条卡和芯片卡的差异；
—— 商户可疑活动报表；
—— 脱机交易和联机交易的比较统计报表；
—— 商户服务报表（监控商户对芯片终端的支持程度）。

12.5 内部员工培训

应对与商户服务相关的部门进行芯片卡交易处理的培训。对于部署 PBOC 终端的交易点必须进行操作流程的培训。培训的工作量取决于有多少部门和商户服务有关。应对与客户直接交互的部门进行更加广泛的培训。

全面的培训计划有助于保证项目尽快投入运行。培训计划的制定包括以下任务：

—— 制订培训目标
—— 确定培训需求
—— 设计培训课程
—— 编制培训材料、操作指南和帮助指南
—— 依据培训的进展调整部门培训需求
—— 制定培训进度表
—— 需要培训的人员：
- 总部人员
- 分部人员
- 客户服务人员
- 操作人员
- 记账人员
- 系统开发人员
- 相关分支机构人员

在最初的培训完成之后，员工应该知晓通过何种途径来解决问题。如需获得培训方面的支持与建议，请联系银联代表。

12.6 执行活动

本节描述了与交换、记账、争议解决、报表及培训相关的策略、业务、技术活动：

—— 策略
- 分析产品价格结构，决定是否改变收费标准；
- 评估对于新增芯片交易数据的报表需求。

—— 业务
- 确定恰当的交换费率，评估对商户的经济影响；
- 如果需要，向商户通报新的交换费率和价格结构；
- 评估 PBOC 对争议处理业务规则的影响：
  - 设计与规划流程，以适应与芯片相关的变化；
  - 将处理流程的任何变化都告知商户；
  - 确定客户服务和差错处理系统需要进行哪些改造。
- 决定需要改造哪些现有报表，新增哪些报表；
- 制定、实施培训计划，应涵盖所有涉及人员。

—— 技术
- 改造系统以支持新的交换费率和价格结构（如果适用）；
- 增强现有报表功能，设计新增 PBOC 报表；
- 改造客户服务、差错处理系统。

13 商户支持

本章介绍了为使商户支持受理芯片卡需要给予支持的相关任务。PBOC 引入的有关商户支持的范围如下：

—— 商户协议
—— 商户服务
—— 商户系统改造
—— 商户培训

13.1 商户协议

现有的商户协议必须更新以适应迁移到 PBOC 的转变。评估关于芯片处理对商户关系的影响是很重要的，商户协议需要修改的内容：

—— 终端成本和安装，以及价格体系改变。
—— 支持附加的授权和清算信息。
—— 提供新增信息报表。
—— 费用和竞争因素。
—— 商户对转换到受理芯片卡的预期，包括退单责任的评估。
—— 卡片受理流程的变化。

商户协议中关于商业需求作出的调整，需要作出正式的通告；同时法律顾问需要对协议进行审核。

13.2 商户服务

部署支持芯片处理的终端，需要更多的商户服务和支持。为了最大限度地支持受理 PBOC 借记/贷记卡产品，需要有计划地扩大商户服务范围。

13.2.1 商户实施支持

当决定部署芯片处理终端时，计划如何支持商户迁移到 PBOC 变得很重要。商户在迁移过程中经历问题的多少将直接影响到收单行计划的成功与否，因此全面的准备以及对商户给予大力支持和培训，都是十分必要的。需要完成以下工作：

—— 确认如何提供硬件和软件的安装支持
—— 预先估计可能出现的问题和范围，提前制订解决办法。
—— 确保商户服务人员得到培训，能处理商户的请求和问题。
—— 安排对培训师进行培训。
—— 考虑安装热线电话，提供客户咨询。
—— 评价商户环境下潜在的终端改造内容，包括：外观改造、收银台的改变、电气升级，PIN 键盘的放置和线路的改造。
—— 确定商户网络接口对支持芯片数据处理的影响。
—— 确定终端维护方式，如内部支持或第三方支持。

13.2.2 终端安装

终端部署的最后一步，是依据商户情况提供可操作的终端。终端部署计划需要考虑以下内容：

—— 测试所有的终端部件，确保能正常工作。
- 对终端的各个部件进行基本的功能性测试；
- 对终端进行整体的测试，确保各个部件的互操作性。

—— 在发往商户之前，确保终端数据已完全下载，包括：应用标识符(AIDs)、应用版本号、终端行为代码(TACs)以及公钥等，并且终端工作正常。

注：在加载生产密钥之前，收单行应该删除所有测试密钥以避免发生脱机数据认证失败的情况。

—— 确定可行的部署方法。
—— 确定部署的优先顺序，例如：根据地理区域或商户的可信度。
—— 配件交付计划，例如：打印纸，色带和设备面板等。

—— 确认要求的附件。例如：终端底座、电源线等。
—— 制订服务协议、服务台支持和培训。
—— 为商户提供终端使用说明。
—— 决定是否在交易点提供持卡人操作手册。如果提供，手册应该包括提示持卡人是否需要输入 PIN 等内容。

通过现场安装、测试，应能保证PBOC根CA公钥和其他与芯片相关参数已经正确下载。

13.2.3 现行商户服务

商户服务和支持人员必须准备对引入芯片处理终端相关的客户咨询作出反应。为了保证支持的有效性，推荐以下做法：

—— 确定可用资源和咨询类型。
—— 确定终端支持的预期水平。

收单行应该通过热线电话向 PBOC 商户提供咨询，热线电话号码可以通过以下方式提供：

—— 张贴在终端上；
—— 列在商户结算账户对账单上；
—— 包含在商户培训资料或某种信息材料里；
—— 包含在为商户准备的小册子或通讯录里。

13.3 商户系统改造

项目计划中应该考虑芯片数据的应用给商户系统带来的影响。按以下内容对商户系统的改造进行评估：

—— 终端与商户主机接口
—— 终端与零售工作站接口
—— 内部的的终端控制器
—— 商户与收单行主机接口
—— 商户后台系统
—— 规划商户网络规模，以适应处理、获取、记录以及备份交易的需要。

一旦进行了改造，必须安排足够的时间对最后的商户系统配置进行测试。

13.4 商户培训

通过部署EMV/PBOC兼容终端，在交易点引入了新的功能。在培训计划中应该重点关注商户操作流程的改变。

13.4.1 培训主题

培训计划应包括以下主题：

—— 通用芯片受理流程
—— 持卡者应用选择
—— 持卡者身份验证
—— 脱机交易与联机交易
—— 降级使用交易
—— 其它交易
—— 其他应用支持
—— 终端维护

以上的一些特性针对于芯片卡和终端，他们对于商户和持卡人来说是透明的。

以上功能的详细信息，请参照第6章“终端要求”和第7章“其它终端要求”。

13.4.1.1 通用芯片受理流程

必须对商户进行磁条卡交易和芯片卡交易流程差异的培训：

—— 芯片卡插入芯片读写器，在交易的过程中芯片卡一直保持插入状态。这与磁条卡方式不同，

对于磁条卡来说，商户只需要刷一下磁条卡，就可以移走了。

—— 在交易的过程中，芯片卡必须停留在终端中，直到交易结束时才能被移开。如果提前将芯片卡从读写器中移开，交易就会被终止。必须确保在交易结束时，终端能够显示相应的提示信息，商户或客户在看到该提示信息时，才能把芯片卡从读写器中取出。

—— 在由持卡人自己将芯片卡插入读写器的交易场所，商户应对持卡人说明芯片卡的受理流程。另外，无人值守终端（如 ATM 或持卡人激活的终端）必须显示提示信息，指导持卡人完成交易的每个步骤。

由于以上变化，收单行应该评估是否需要为商户制作持卡人使用手册，以帮助持卡人正确完成芯片卡交易。

13.4.1.2 持卡人应用选择

芯片卡通常支持多种应用，如果终端支持多应用，可以提供持卡人选择应用的功能。对商户的培训应包含商户如何向持卡人解释应用选择流程；同时，还要培训商户如何指导持卡人点击适当的按键来选择想要的应用或账户。

持卡人应用选择流程通常取决于发卡行事先在芯片内作出的定义。卡片和终端可以自动选择最高优先级的应用进行交易，也可以对共同支持的应用进行持卡人选择、或者按优先级对应用逐个进行持卡人确认。

商户还需要注意并非所有交易都需要应用选择，通常情况下，只有卡片和终端同时支持多个应用才需要进行选择。例如，当卡片和终端都支持PBOC贷记卡和PBOC借记卡两种应用时，就会要求持卡人对应用进行选择。因此，商户需要明白在一些交易中会发生应用的选择，而在另一些交易中则不会发生，这只是交易方式不同，并不是错误。

13.4.1.3 持卡人验证

商户和持卡人应该了解：在有人值守环境中，持卡人可以通过签名或输入PIN的方式确认一笔交易；在无人值守的环境中，不管是否需要输入PIN，签名方式是没有意义的。

在芯片受理环境中，完成交易所需要的持卡人验证方法(CVM)是由终端和卡片来决定的，使用何种CVM不受商户和持卡人控制。

终端和卡片的交互决策流程和最终的选择是基于特定交易的一些数据要素综合决定的，例如：金额、国内或国际交易、联机或脱机、以及其它交易参数。

以下讨论的CVM包括：

—— 签名

—— PIN

—— 无需 CVM

13.4.1.3.1 签名

《银联卡业务运作规章》规定：PBOC芯片卡应同时携带磁条和签名条。

签名仍然是持卡人进行身份验证的国际性默认方式，也是许多地区卡片交易的默认方式。芯片卡环境下的签名验证和磁条卡环境下的签名验证是一致的。

13.4.1.3.2 PIN

输入PIN确认持卡人身份的方式便捷且安全，这使得这种方式将在PBOC卡交易中获得更为广泛的使用。对于部署PIN输入键盘的场所，培训应该包括以下的要点：

—— 卡片和终端的交互将决定合适的持卡人验证方法(CVM)以及是否提示输入 PIN。

—— 因为是由卡片来决定是否在每次交易中需要输入 PIN，所以若终端没有提示要求输入 PIN 并不是出了某种错误。如果芯片卡要求输入 PIN,终端就会作出提示。商户不应该要求持卡人输入 PIN，除非终端作出此项提示。

—— 当持卡人被要求输入 PIN 时，PIN 输入的过程必须处于保密状态。

—— 如果一笔交易是采用输入 PIN 的方式进行的，建议在收据上不要印出签名行。参照 6.4 节“持卡人验证”以获取更多的信息。商户应该注意到在收据上没有列出签名行的情况下，不应

该要求持卡人签名。

注： 某些地区可能对超过一定交易金额的交易要求脱机PIN验证和持卡人的签名。请联系银联代表，了解本地市场的要求。

13.4.1.3.3 无需 CVM

发卡行可以在不要求持卡人签名或输入PIN的情况下，有能力通过其他的检查机制来完成交易。当终端和卡片都允许“无需CVM”作为持卡人验证选项时，“无需CVM”是一种合法的CVM选项。

这种方式通常应用于无人值守的终端环境下；发卡行为了实现要求快速支付的脱机交易，也可以选择这种方式。不管怎样，即使卡片对于特定类型终端指示“无需CVM”，终端可以选择磁条卡交易的CVM作为其默认CVM（例如：在POS上使用签名、在ATM上使用联机PIN），提供对交易的安全保护。

这种方式可以作为小额支付的首选CVM。

13.4.1.4 脱机&联机交易

在部署有联机/脱机能力终端的商户场所，应该对营业员进行培训，使其理解某些交易是脱机处理的、而另一些交易是请求联机处理的。他们不需要关注联机和脱机处理的差别，也不应该将这种差别视为异常。不过，他们至少应该知道脱机交易比联机交易速度要快。

13.4.1.5 降级使用交易

降级使用(Fallback)交易是指当芯片卡在具有芯片能力的终端上交易，由于芯片卡或芯片终端不能正常工作时，终端指示持卡人通过刷磁条进行的交易。

PBOC终端应该支持正常的芯片卡交易和降级使用交易。终端应该首先尝试进行芯片交易，当芯片或芯片读写器不能正常工作时方可进行Fallback交易。不允许终端设备主动提示使用磁条而跳过芯片认证控制。

在芯片或芯片读写器不能正常工作时，终端将通过磁条读写器读取芯片卡的磁条信息；在这种情况下，终端从磁条信息中读取服务代码，并提示商户按芯片卡来操作。收单行需要对商户进行关于Fallback的培训，必须遵照一定的流程来操作。较为典型的情形是：向收银员提供多次读取芯片的机会；在使用磁条进行Fallback交易前，提示收银员刷卡。

商户必须了解对被拒绝的芯片卡交易不应尝试Fallback。被拒绝的芯片卡交易不能通过磁条或其它任何方式重新进行交易；如果发生这种情况，交易将被发卡行退回。

当发生芯片卡交易被拒绝或失败的情况，商户可以询问持卡人能否采用其它支付方式。

13.4.1.6 其它交易

退货、冲正和撤销等交易的处理流程与现在一样，只是通过芯片而非磁条来实现。如果需要，在交易点必须检查其它卡片安全特性。

13.4.1.7 其它应用支持

如果收单行支持其它芯片应用，例如：积分或储值计划，也应对商户培训这些新的操作流程。收单行需要在其培训计划中包含这些活动。

13.4.1.8 终端维护

培训应该包括对终端的日常维护、保持磁条和芯片读写器清洁、无干扰物等内容。另外，建议对终端进行定期维护、检查，确保各部件运行正常、安装在安全位置，防止意外损害、数据丢失等情况的发生。

13.4.2 商户培训计划

商户培训计划通常包括以下内容：

—— 制定培训目标
—— 确定培训要求
—— 设计培训课程
—— 编制培训教材
—— 对培训师进行培训

13.4.3 培训材料

在培训过程中，需要提供培训支持材料。通常为商户培训提供以下材料：

—— 培训介绍

—— 操作指南

—— 快速参考指南

—— 商户和持卡人常见问题解答。

—— 商户服务部门的联系方式。

客户培训资料有助于商户对持卡人常见问题进行解答。通过初步培训后，商户人员应该懂得对出现的问题通过何种途径寻求解决。

如果发生大量的Fallback交易或反复出现某种操作问题，有必要安排深入培训。

应对商户的培训资料和培训需求进行评估，可以考虑帮助商户建立自己的培训机制。

附 录 A
（资料性附录）
实施计划编制

实现 PBOC 所需执行活动和时间取决于收单行的具体要求，一般情况下实现 PBOC 完全迁移计划需要 9 至 18 个月。在筹备阶段充分理解 PBOC 产品的特性和利益、以及如何促进收单行的商业需求，对整个项目的实施具有重大影响。

PBOC 迁移计划涉及范围很广，会影响到银行员工、商户、终端供应商、业务流程和处理系统。它对项目管理的要求很高，需要组建一个跨部门的团队，应具备同时管理几个并行任务的能力。

本附录用于帮助收单行规划 PBOC 迁移项目，制定一个详细的工作计划，包括：

—— 关键成功因素
—— 项目组织
—— 实施计划
—— 项目任务一览表

A.1 关键成功因素

在规划阶段，应该确定项目的目标、范围以及成功标准。需要确定项目的领导人、主办人、组织架构和参与部门。做好这些工作将为整个项目的顺利实施打下良好的基础。

清晰明确的目标能够引导项目的正确方向，使参与者集中关注主要问题。例如：如果收单行的一个主要目标是为商户提供基于芯片的积分应用，就需要确保所选终端及其软件能够支持这个功能；对与之无关的其它可选功能就不需要投入太多关注了。

收单行可以依据项目范围来决定实现此计划的方法。收单行应根据设备、资金以及市场的规模来确定合适的实现方法；在2家自助餐厅试用500张卡肯定要比实现2500台终端和5万张卡的计划简单的多。

在项目的启动阶段就应该定义其成功标准，并获得所有参与方和主要领导的一致同意。在项目的每个阶段，成员可以依据这些标准参与疑难问题的解决、确定沟通要求。成功标准也是实施质量保证、用户验收的一个基础；在产品发布、准备结项时，这个标准将用于鉴定成功与否。最后，使用这个标准对项目进行总结，衡量项目是否取得全面成功。

不管项目组织的规模如何，有几个关键成功因素应该考虑到：

- 领导者与执行者
  必须拥有一名优秀的领导者，他应该有能力管理不同的团队、充分调动各方的积极性来保证项目的成功。具有强大执行能力的主管人员，对于项目组织也是十分重要的。
- 角色与职责
  整个项目组织涉及多个领域；因此在启动实施过程之前，应该定义每个领域的角色及其职责。很多活动有交叉依赖关系或继承关系，因此每个团队需要清楚其在整个项目中所承担的角色。
- 准备工作
  要成功实施 PBOC 迁移计划，充分的前期准备工作是至关紧要的。许多活动的开展依赖于业务策略的确定。
- 决策与管理委员会
  由于这个项目涉及到银行内多个业务部门，在讨论业务需求的过程中，有可能会出现争执不下的情况。因此，成立一个专门的决策与管理委员会，有利于集中协调、裁决棘手问题，避免对项目进度造成影响。
  银联建议：管理委员会应存在于项目的整个生命周期。管理委员会应该包括相关各方负责人，

他们不需要每天都参与到项目中，而是主要对于项目实施提供指导，对项目组无法决定的策略进行仲裁，并提供项目所需资金、资源等方面的支持。

A.2 项目组织

大多数成员行成立一个专责工作组来管理从开始规划到产品发布的所有方面。这个小组由银行内受PBOC迁移影响的各个部门的代表组成。每个工作组成员在各自领域提供专业意见，承担所负职责。项目所需要的各方面专家应该尽早参与到项目中来；当然，并不需要所有成员完全投入到项目中。下面描述一个典型的PBOC迁移计划工作组的功能、角色和职责。

A.3 项目经理

项目经理负责项目的整体运作、里程碑、时间线，还需负责日常管理、协调各个小组的问题、跟踪项目活动和任务、维护及分发项目文档、安排会议等事项，以及对管理委员会的汇报、协调。项目经理也承担对银联主要联系人的角色，为了确保项目经理能够集中精力解决主要问题，可以考虑为其配备助理，分担其部分职责。

A.4 项目团队

项目团队成员向项目经理汇报，项目团队一般需要以下各个方面的成员：

- 卡受理产品经理
  卡受理产品经理从业务角度把握迁移计划的格局，决定准备实现的受理功能及其业务策略。卡受理产品经理也负责联系、管理供应商，有可能还需负责新增密钥管理方面的活动。
- 市场
  市场营销人员基于将要实现的产品服务，针对持卡人、商户进行市场前景分析并提交相关报告，制定市场营销策略。
- 法律
  PBOC 迁移计划一般会要求修改与商户的合作协议，另外也会涉及到与供应商签订新合同、或修订原有合同，这些工作由法律部门来承担。
- 安全与风险管理
  安全与风险管理人员负责提供风险控制与信息安全方面的专业知识，管理对称和非对称密钥，监控生成密钥的正确性、安全性，确保密钥的安全传递。
- 系统开发
  系统开发人员负责实施与 PBOC 迁移相关的系统改造。
- 系统与网络管理
  系统与网络管理人员负责测试环境、生产环境的安装、改造、维护等事项。这部分工作应该及时安排实施，以免影响项目进度。
- 业务管理
  业务管理人员负责制定 PBOC 涉及的业务流程，如：争议处理、客户服务。
- 商户营销和服务
  商户营销和服务人员负责联系商户，发展特约商户参与这个计划。在整个实施过程中，负责协调和协助商户的工作。
- 培训
  培训人员负责制订培训计划、编制培训材料，给予不同岗位的员工有针对性的培训。
- 文档
  文档管理人员负责编写、修订业务和技术文档。
- 质量管理
  质量管理人员执行所有必需的测试，确保改造后的系统运行无误。
- 用户验收

用户验收人员执行测试，确保改造后的系统满足最终用户的业务需求。

A.5 实施计划

工作组根据项目目标制定实施计划，这个计划应该涵盖整个项目生命周期内所发生的活动。虽然各个银行计划的具体格式、内容会有所不同，但一般应包括以下方面：

- 期望达到的主要里程碑；
- 需要解决的主要问题；
- 关键事件的实现顺序以及时间点；
- 实施任务的合理陈述。

在完成实施计划后，工作组评估每个主要的功能模块，编制一整套细分的任务，通过工作计划将这些任务分配到每个项目组成员,并明确责任和时间要求。

后续的“项目任务一览表”可以帮助收单行制定PBOC迁移实施计划。

A.6 项目任务一览表

步骤	任务
1	项目前活动
1.1	获取主要领导同意，成立管理工作组
1.2	确定管理工作组的职权范围
1.3	任命管理工作组，开始运作
1.4	与银联代表讨论 PBOC 迁移所带来的影响
1.5	对工作组成员进行 PBOC 和 EMV 相关知识的培训
2	决策
2.1	定义商业机会
2.1.1	描述现有卡产品业务模式－受众、流程、技术
2.1.2	确认 PBOC 应用的业务模式和组织价值
2.1.3	判定技术条件是否成熟（内部&外部）
2.1.4	定义业务目标
2.1.5	描述可能收益
2.1.6	明确业务需求
2.1.7	说明商业机会与风险
2.1.8	描述市场环境与外部影响
2.1.9	说明 PBOC 业务要求
2.2	寻求批准
2.2.1	向主要领导汇报 PBOC 迁移计划
2.2.2	认可管理工作组的建议
2.2.3	申请预算资金、人力资源
2.3	组建筹备工作组
2.3.1	挑选合格的业务、技术人员加入项目组；如果需要，可以补充第三方厂商、外包厂商、银联或外部咨询顾问
2.3.2	确定筹备工作组的职权范围
2.3.3	获取 PBOC 和 EMV 相关文档
2.3.4	培训工作组成员
3	准备（规划与启动）

3.1	分析业务解决方案
3.1.1	描述业务解决方案的选项与建议－受众、流程、技术
3.1.2	定义 PBOC 安全策略
3.1.3	描述实施方式－自主完成、定制、外包、或混合方式
3.1.4	进行 PBOC 迁移对原有业务的影响分析
3.1.5	描述可能利益－直接经济收益、业务流程、客户认知度、组织创新
3.1.6	获取银联提供的 PBOC 迁移实施计划模版
3.2	制定项目管理计划
3.2.1	确定实施预算－人员、技术、第三方厂商、设备、工具以及其它花费
3.2.2	定义关键成功因素
3.2.3	制定一个量化的业务方案
3.2.4	描述如何管理、评估、统计新的利益
3.2.5	定义内外沟通、培训策略
3.2.6	定义检测、试验策略
3.2.7	进行风险分析
3.3	项目规划
3.3.1	评估业务模式与业务方案
3.3.2	确定项目目标与范围
3.3.3	确定工作流
3.3.4	确定所需资源（包括如何获得资源）
3.3.5	描述项目管理方法
3.3.6	评定变化及其预期难度的等级
3.3.7	进行项目风险评估，制定风险管理计划
3.3.8	制定沟通、培训计划
3.3.9	制定检测、试验计划
3.3.10	综合上述内容，形成项目管理计划
3.4	启动项目
3.4.1	分配工作流资源
3.4.1.1	正式组建项目团队
3.4.1.2	培训项目组成员
3.4.1.3	执行项目管理方法
3.4.1.4	执行计划控制流程
3.4.1.5	制定沟通计划
3.4.1.6	制定单元测试、集成测试、认证测试、用户验收测试等计划
3.4.1.7	制定项目干系人管理方法
3.4.1.8	执行风险、突发问题管理方法
3.4.2	制定效益模型
3.4.3	执行效益管理方法
3.4.4	启动各个工作流
4	收单行完全迁移
4.1	供应商选择
4.1.1	制定并发布招标书、方案征询书（RFI/RFP）

4.1.2	评估返回信息
4.1.3	选择供应商
4.1.4	谈判、决标
4.1.5	管理供应商
4.1.6	接收供应商交付产品
4.2	终端选择
4.2.1	确定对终端功能、安全要求
4.2.2	分析终端规格是否满足各项要求
4.2.3	终端供应商提供终端质量管理服务
4.2.4	确认终端供应商通过银行卡检测中心认证
4.3	收单行系统改造
4.3.1	交易处理系统改造
4.3.1.1	终端管理系统改造
4.3.1.2	终端与收单行接口改造
4.3.1.3	主机系统改造
4.3.2	业务处理系统改造
4.4	获取 PBOC 根 CA 公钥
4.4.1	向银联申请 PBOC 根 CA 公钥
4.4.2	安全传递、验证根 CA 公钥
4.4.3	加载根 CA 公钥（生产/测试）到终端
4.5	系统入网测试-终端测试
4.5.1	终端脱机测试(TFT)
4.5.1.1	使用银联测试卡进行测试
4.5.1.2	提交测试记录
4.5.1.3	银联对测试结果进行评审
4.5.2	终端集成测试(TIT)
4.5.2.1	使用银联测试卡、仿真器进行测试
4.5.2.2	提交测试日志
4.5.2.3	银联对日志进行评审
4.6	系统入网测试-主机测试
4.6.1	脱机测试部分
4.6.1.1	使用银联测试卡、仿真器进行测试
4.6.1.2	提交测试日志
4.6.1.3	银联对日志进行评审
4.6.2	联机测试部分
4.6.2.1	进行联机测试认证
4.6.2.2	银联出具测试报告
5	内部测试
5.1	确定测试策略
5.2	制定详细测试计划
5.3	单元测试/集成测试/用户验收测试
5.3.1	制定验收标准

5.3.2	准备测试工具
5.3.3	编制测试案例
5.3.4	准备测试数据
5.3.5	搭建测试环境
5.3.6	执行测试计划
5.3.7	检查、验证测试结果
5.3.8	进行回归测试
5.3.9	通过验收
6	商户支持
6.1	确定实现迁移的现有商户，发展新商户
6.2	商户实施支持
6.3	MIS 商户系统改造（如果需要）
6.4	商户培训
7	产品发布
7.1	确定产品发布策略
7.2	制定产品发布计划
7.3	制定设备交付计划
7.4	准备技术环境
7.4.1	网络连通
7.4.2	环境测试
7.4.3	系统安装
7.5	投产准备
7.5.1	规划并实施投产预演
7.5.2	导入投产数据
7.5.3	操作培训
7.5.4	测试灾备系统
7.6	投产
7.6.1	制定投产方案、预期结果
7.6.2	准备验证数据
7.6.3	执行投产计划
7.6.4	验证 PBOC 应用的正确性
7.6.5	通过业务部门验收
7.6.6	移交给日常运维部门

附 录 B
（资料性附录）
分发 PBOC 根 CA 公钥至终端基本原则

B.1 基本原则

为了确保收单行将收到并验证的根 CA 公钥信息安全地传递到终端，收单行必须遵守下列规则：

1. 在根CA 公钥由收单行传递给终端时，终端设备必须验证传输的公钥信息的数据完整性并进行信息源认证，比如在传输过程中使用数字签名或使用MAC认证码。
   收单行可以选择授权机构管理部分终端。授权机构可以是与一个收单行有业务协议并管理一部分终端或终端的接收数据装置，或一个与收单行有相关业务协议授权的机构负责维护管理部分终端或终端数据接收装置。
   根 CA 公钥在由收单行传输到授权机构过程中，必须验证传输的公钥信息的数据完整性和进行信息源认证。根 CA 公钥由授权机构传输到终端也必须验证传输的公钥信息的数据完整性和信息源认证。终端数据接受装置在接收根 CA 公钥数据，或由人工控制过程中，必须进行有效的访问控制。
2. 验证过的根CA 公钥在传输到终端的过程中，必须保证数据完整性。
   这个规则确保终端收到的验证过的根 CA 公钥数据是完整的。比如验证公钥信息的哈希值，或实施有效的校验和验证。
3. 确保新引入的根CA 公钥信息在公钥生效日期前装载到每个终端。
   必须确保新引入的根 CA 公钥在使用该根 CA 公钥的金融 IC 卡的流通日期前装载到每个终端，以便保证使用该根 CA 公钥的金融 IC 卡在其生效时即可使用。收单行对这个要求必须能够审计。
4. 确保到期或撤销的根CA 公钥在到期或撤销的6个月内移出每个终端或停止在终端使用。
   终端能够鉴别过期或已撤销的根 CA 公钥。收单行对这个要求必须能够审计。
5. 收单行必须能够在合理的时间期限内确认在其每个终端中，哪些IC卡支付系统根CA公钥正在使用。
6. 收单行必须能够报告其每一个终端当前能够支持的密钥长度。
   其当前支持的密钥长度必须保持与中国银联公布的所有在生效期内的根 CA 公钥长度同步，以便支持在银联金融 IC 卡公钥体系内的所有 IC 卡的使用。同时，终端必须有效防止使用过期根 CA 公钥的金融欺诈。

B.2 其它建议

1. 为了达到最佳运作效率，当需要下载或移出一个密钥时，终端管理系统应该能够自动通知所有受影响的终端。
   为了减少人工更换密钥的花费，应该实现密钥更换的自动通知。这个通知可以通过授权响应、批量结算确认或日终响应等方式实现，也可以由终端管理系统直接发起。另外，终端可以主动向终端管理系统请求一个明显的更新。
2. 终端和终端管理系统应该为受影响的密钥安排自动更新。
   对大量终端的密钥实行人工管理是十分困难的，因此建议一旦收到通知，自动执行一个预定的处理流程、及时完成密钥更新。
3. 发卡行应该遵循银联对于IACs的推荐设置。

如果卡片要求一个密钥而终端却没有，将会发生 SDA/DDA 失败的情况；交易将基于 IACs 采取下一步动作，发卡行决定了交易将如何继续下去。在这个例子中，IACs 的最佳设置应该是指示交易请求联机处理。

附 录 C
（规范性附录）
中国银联 IC 卡收单入网工作流程

入网收单机构要开通 IC 卡功能，其流程与磁条卡收单类似，入网机构需要先通过 IC 卡功能入网测试（脱机测试和联机测试），再进行入网开通申请。

C.1 入网测试流程

收单行的 IC 卡入网测试流程如下：

1. 入网机构提出脱机测试申请
   入网机构填写入网脱机测试表格（表格由上海信息中心、IC 卡应用部共同提供），提出测试申请。上海信息中心与 IC 卡应用部对申请表进行审查并将审查结果通知入网机构，上海信息中心针对入网机构进行参数设置，IC 卡应用部分发用于脱机测试的入网测试工具。
2. 入网机构进行脱机测试
   入网机构利用测试工具进行按照脱机测试案例进行系统脱机测试，包括芯片个人化数据的正确性与完整性验证、终端程序的验证和系统主机联机授权系统的验证。
3. 脱机测试结果评估
   在完成脱机测试后，入网机构将脱机测试日志提交至 IC 卡应用部，IC 卡部对日志进行评估，并将评估结果反馈给入网机构。
4. 入网机构进行联机测试
   在脱机测试日志评估通过后，入网机构提出联机测试申请，通过上海信息中心审查后，入网机构将系统接入上海信息中心进行联机测试。
5. 联机测试结果评估
   上海信息中心对入网机构的测试结果进行评估，通过后出具联机测试报告并通知业务管理部。

C.2 入网开通流程

收单行的 IC 卡入网开通申请流程相对较简单，在上海信息中心完成联机测试出具测试报告、通知业务管理部后，收单行就可以开通受理银联 IC 卡。

C.3 特别说明

对于银联IC卡收单入网工作流程，有几点需要明确：

1. 入网机构的脱机测试包括：终端测试和系统主机测试。
2. 入网机构的脱机测试不包括清算文件、差错处理的测试；联机测试需要对机构开通的所有交易进行完全测试、包括清算文件和差错处理。
3. 在主机测试中，脱机测试案例和联机测试案例基本保持一致。
   - 脱机测试案例提供比较完整的入网机构调试内容，检验入网机构 IC 卡应用、是否符合规范标准的能力；
   - 联机测试案例主要测试卡片所包含的功能在联机跨行网络上能正确转接与处理。