Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 042.2—2011
代替Q/CUP 029-2008

中国金融集成电路（IC）卡借记/贷记应用 发卡行实施指南

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

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》借记贷记应用的发卡行实施指南，供发卡银行实施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/贷记应用发卡行实施指南

1 范围

本指南的编写目的是为发卡行实施 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。本指南帮助发卡行改造其主系统和后台架构，以支持 PBOC 迁移；也包含协助发卡行选择卡片参数、个人化 PBOC 卡等信息。

为了便于使用，每章都包含一个“执行活动”节，集中描述发卡行应该完成的策略、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，协助发卡行的实施。

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 0025.10-2005 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)
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)
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 卡片选择与认证

5.1 卡商选择

在与供应商接触、评估其可用产品之前，发卡行应该研究其卡片需求。本节提供以下建议条目，帮助发卡行确立卡片供应商选择标准：

- PBOC 功能
- 其它芯片应用
- 存储容量
- 交易速度
- 密码处理器
- 采购数量
- 集成服务
- 数据传输协议
- 专有要求

5.1.1 PBOC 功能

这些功能包括：

- 磁条数据
  PBOC 应用必须支持目前磁条卡产品的可用功能。
- 授权控制
  发卡行可以设置单独或成组的持卡人限制条件，帮助确定在什么情况下交易需要请求联机处理。这些控制有助于减少高风险账户的暴露，特别是在最低限额(floor limit)设置较高的环境。
- 持卡人验证方法(CVM)
  基于交易个体的特性，芯片可以被个人化最合适的持卡人验证方法，例如：联机 PIN 或签名。签名、身份证件验证可以和脱机 PIN 验证方式结合起来。持卡人验证方法处理被设计为可支持附加的持卡人验证，例如：采用生物识别技术。
- 脱机数据认证
  PBOC 提供在交易点防御伪造的保护，以减少欺诈损失。脱机数据认证有两种类型：静态数据认证(SDA)、动态数据认证(DDA)，DDA 又包括标准 DDA 和复合 DDA/应用密文生成（CDA）两种认证方式。
  脱机静态数据认证（SDA）验证卡片在个人化以后重要的应用数据是否被非法修改。动态数据认证（DDA）验证卡片中的重要数据在发卡后是否被篡改，同时验证卡片是否伪卡。
- 联机卡片认证与发卡行认证
  PBOC 允许卡片进行确认它是与真实的发卡行通讯，还提供数据完整性和有卡交易的检查。
- 发卡行脚本处理
  发卡行可以不用重新发卡而是通过发卡行脚本处理来修改卡片中的个人化数据。脚本处理通过锁定恶意透支和失窃的卡片来控制信用和伪卡风险。可以在不重新发卡的情况下，根据持卡人情况的变化对卡片参数进行修改。

发卡行需要决定准备支持哪些 PBOC 功能，在发卡行做出各种选择时，应该了解这些选项不一定在全球范围的终端上都能支持。在决定支持何种功能时如需协助，请联系银联代表。

5.1.2 其它芯片应用

发卡行应该决定是否支持其它基于芯片的应用，如：积分或储值应用。使用多应用卡，发卡行能够在一个芯片卡项目中赢得更多利益。

5.1.3 存储器

发卡行的卡片需要足够的存储器来处理所有卡内应用，由于芯片卡厂商会持续优化 PBOC 应用代码，推荐的存储器容量不一定够用。通过提供明确需求，发卡行可以和卡片供应商一起确定合适的存储器配置。

注：芯片卡最重要的两种存储器部件是只读存储器(ROM)和电可擦除可编程只读存储器(EEPROM)，EEPROM 相对更贵。为了帮助管理成本，银联和芯片厂商合作确保 PBOC 应用基本放在 ROM 中，保留 EEPROM 用于发卡行个人化以及存放持卡人信息。

5.1.4 交易速度

卡片上不同功能会影响一笔交易的总计时间，发卡行应该考虑向芯片卡厂商描述发卡行对交易速度的要求。

5.1.5 密码处理器

如果发卡行准备使用 DDA 和脱机密文 PIN，需要芯片卡包含密码处理器。银联强烈建议：当发卡行选择这些功能时，应使用包含密码处理器的卡片，因为硬件密码处理器能够显著减少 DDA、脱机密文 PIN 的交易处理时间。

注：PBOC 对脱机密文 PI N 不作要求，具体内容请参见 EMV 第二册 第 7 章。

5.1.6 采购数量

发卡行应该确定向供应商采购卡片的数量，这是影响价格的主要因素之一。

5.1.7 集成服务

发卡行应该说明需要芯片卡厂商提供的服务，例如：制卡、个人化。这些集成服务将影响发卡行的总体价格。

5.1.8 数据传输协议

卡片供应商可能询问发卡行对数据传输协议是否有优先选择要求。EMV 和 PBOC 支持两种数据传输协议，这些协议规定了数据在卡片与终端之间的传输机制，它们是 T=0(字符协议)和 T=1(块协议)，使用何种协议不会影响卡的受理，因为所有支持 PBOC 应用的 EMV 设备必须同时支持两种协议。

5.1.9 专有要求

向潜在供应商描述任何专有要求是必要的。发卡行的专有要求可能需要特别开发，这将影响到成本和时间期限。

5.2 银联要求

PBOC 卡片必须遵守以下规范和章程：

- 《EMV Integrated Circuit Card Specifications for Payment Systems》
- 《中国金融集成电路（IC）卡规范》（2005 版）
- 最低程度，PBOC 应用必须配置支持当前磁条卡产品的功能；
- 卡片检测－在发行卡片之前，发卡行选择的卡产品必须通过银行卡检测中心的 PBOC2.0(借记/贷记)检测。通过检测的卡产品公示在：
  http://www.bctest.com/passed/list.asp?strCode_product=166&strCode=passed_finance
- 银联业务规章－与磁条卡一样，发卡行的芯片卡也需遵守银联业务规章的各项要求。

5.3 银联供应商计划

为了推动 PBOC 卡产品的普及发展，银联正在与供应商进行合作。这些活动包括：进行供应商资格评估、提供 PBOC 培训、共同进行卡产品研究开发、为银联成员谈判特价计划。发卡行在选择供应商时，可与银联代表联系，了解这个计划对发卡行采购芯片卡的活动能否有所帮助。

6 卡片发行

本章描述了发行一张 PBOC 卡所要求的活动。它假设此卡已通过银行卡检测中心的 PBOC2.0 检测，针对以下方面提供了有关供应商活动的高层次信息以及发卡行活动的详细信息：

- 发卡行预个人化活动
  发卡行进行卡片设计，建立个人化输入文件（包含个人化到卡内的全部数据），生成并传递个人化密钥至相关方。关于建立个人化输入文件的信息请参考第 7 章。
- 卡片制造商活动
  卡片制造商将卡面设计置入卡片、连同未编码磁条，嵌入芯片，初始化 PBOC 应用。

  注：“卡片制造商”在这里泛指涉及芯片卡制造过程的供应商，包括：芯片操作系统、芯片模块嵌入、塑料印刷、在芯片中初始化 PBOC 应用。它可能不止一个供应商。
- 个人化活动
  个人化操作在卡上凸印或平印数据、编码磁条数据，在芯片中置入数据。
- 后个人化活动
  在卡片发给持卡人之前，检查卡片确保个人化数据的正确性。

本章是对卡片发行和个人化处理的一个概述。

6.1 概述

向芯片迁移，卡片个人化处理比原来复杂得多。本节汇集了这个过程的变化，帮助发卡行理解 PBOC 个人化的范围。

6.1.1 新型卡片

PBOC 应用必须加载到芯片卡的 ROM 中，供应商需要开发和测试这个应用以确保其符合 EMV、PBOC 标准，完成这些工作需要时间与资源。

6.1.2 更多数据

依据所支持的 PBOC 功能，PBOC 应用在芯片中会要求很多新增数据元；而当前用于凸印、编码的磁条数据仍是要求的。这些新增数据的处理与风险管理，使得个人化更加复杂了。

6.1.3 密钥管理

根据发卡行计划实施的功能，PBOC 依靠公钥算法和 DES 算法进行密钥管理。另外，芯片个人化处理新的安全要求必须使用 DES 算法。这些新的活动要求风险管理办法和新的密钥管理控制、程序。由于密钥管理要求特别的专业技术，如果发卡行内部没有充分的技术储备，建议联系银联代表以获取帮助。

在 PBOC 中使用的 DES 算法，一般建议采用双倍长密钥算法（3-DES）。

6.1.4 多重处理

在一张芯片卡发给持卡人之前，需要实施许多新的活动。这就要求全面的项目协调能力与高超的管理技巧。

6.1.5 更新、升级设备

因为芯片卡个人化的要求，发卡行需要引进新的工具、升级现有个人化设备，对于新工具需要集成到现有系统并进行员工培训。新的工具包括：

- 个人化准备工具
  帮助发卡行建立个人化文件。文件可以提交给个人化部门或导入个人化机器。
- 个人化机器
  用于个人化卡片的设备，必须针对芯片卡个人化升级，要求增加一个读写芯片的模块，将基于芯片的应用数据全部写入芯片中。
- 个人化验证工具
  在卡片分发给持卡人之前，对个人化芯片卡执行质量保证测试。为了确保在个人化过程中芯片数据正确导入，这个工具是需要的。更详细的信息参见 6.5 节“后个人化活动”。

6.1.6 知识曲线

由于磁条卡技术在支付领域已经使用 20 多年了，有足够时间完善其处理流程、培训各参与方。而对于芯片卡，建立专业顺畅的处理流程是需要时间和经验的。银联建议发卡行在项目计划中留出足够的时间对参与实施支持人员进行培训。如有培训要求请联系银联代表。

6.2 发卡行预个人化活动

发卡行在预个人化阶段主要实现以下活动：

- 完成卡片设计并提供给卡片制造商；
- 制定关于个人化的业务策略；
- 建立个人化输入文件；
- 生成、分发个人化密钥。

下述各节解释这些活动。

6.2.1 卡片设计

发卡行完成卡片设计后提供给卡片制造商，以使其应用到塑料卡片上，为了容纳芯片可能会要求卡片设计有所变动。

参考：对于芯片卡的芯片放置及其它修改要求请查阅《银联卡卡片规范》。

注：银联要求审核任何新的或变更卡片设计，确保芯片卡符合要求，例如：芯片和签名条的位置。

6.2.2 个人化输入文件

在个人化之前，发卡行需要建立个人化输入文件。这个文件包含所有卡片要求数据：

- 磁条的编码数据；
- 凸印/印刷数据；
- 需要置入芯片的 PBOC 应用数据；

- 其它芯片数据

  这可以是卡片支持的任何其它应用的芯片数据，例如：积分或储值数据。

注：对于银联标识卡的凸印/印刷、编码的现有要求不受 PBOC 影响。

为了建立个人化输入文件，银联建议采购专业的个人化准备工具。这个工具可以帮助：

- 从各种来源收集数据，例如：从客户资料库获取账号和持卡人姓名；
- 生成卡片要求的芯片数据；
- 通过连接的硬件加密设备(HSM)产生对称与非对称密钥。

个人化输入文件中任何敏感数据都必须使用密钥交换密钥(KEK)进行加密，有关 KEK 的详细信息请查阅：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。

6.2.3 个人化密钥

在个人化过程中需要使用 DES 密钥执行以下安全功能：

- 保护借记/贷记应用安全；

  用于保护在初始化和发往个人化设备期间，卡内借记/贷记应用的安全。

- 保护个人化输入文件数据安全；

  用于在发卡行与个人化设备之间，安全传递个人化输入文件的敏感数据。

6.2.3.1 保护借记/贷记应用安全

在卡片制造商完成卡片设置之后，卡内应用必须被一个 DES 密钥锁闭，以确保在初始化到个人化期间卡片处于安全状态。没有这种保护，可能发生卡片失窃、被未授权方个人化后不正当使用。除了锁闭 PBOC 应用，这个密钥还对个人化过程中装载到卡片的个人化数据进行检验，证实它们完整无损，且没有被修改。称其为 MAC 密钥(K_{MAC})。

另一个数据加密密钥(K_{DEK})，是装载到卡内的。个人化设备传送给卡片的任何敏感数据都使用这个密钥加密，卡片先使用这个密钥解密敏感数据，再将明文数据装载到卡内。

这两个密钥是由一个主 DES 密钥派生的，称其为发卡行主密钥(KMC)。发卡行负责生成 KMC，并传递给卡片制造商和个人化部门。发卡行可以使用个人化准备工具来生成这个密钥，也可由银联或第三方代表发卡行生成这个密钥。

6.2.3.2 保护个人化输入文件数据安全

由于个人化输入文件包含机密信息，这些敏感数据必须加密后在各方之间传输。

为了实现这点，发卡行必须生成一个密钥交换密钥(KEK)，并传递给个人化设备。发卡行可以使用个人化准备工具来生成这个密钥，也可授权 PBOC 或第三方代为生成这个密钥。

发卡行传输个人化输入文件的任何敏感数据必须通过 KEK 加密，这些数据包括：

- 持卡人脱机 PIN（如果支持脱机 PIN 功能）；
- ICC 私钥（如果实现脱机密文 PIN 或 DDA 功能）；
- 独有密钥（如果支持联机卡片认证和发卡行认证、或发卡行脚本处理功能）；

个人化设备先使用 KEK 解密个人化文件数据，再使用 K_{DEK} 重新加密之，然后把数据装载到卡内。

6.2.4 执行活动

预个人化阶段要求的活动如下：

- 策略
  - ✓ 建立卡片设计；
  - ✓ 完成个人化数据准备的商务决策；
  - ✓ 决定生成 KMC 的数量；

    银联建议：为每个卡片供应商至少生成一个 KMC。
  - ✓ 决定生成 KEK 的数量。

    银联建议：为每个个人化厂商至少生成一个 KEK。
- 业务

- ✓ 完成卡片设计，获得银联批准后传递给卡片制造商；
- ✓ 生成合适数量的 KMC 和 KEK；
- ✓ 建立个人化输入文件，确保其中敏感数据使用 KEK 加密；
- ✓ 将 KMC 安全传递给卡片制造商和个人化厂商；
- ✓ 将 KEK 安全传递给个人化厂商

- 风险管理

  根据是将个人化外包给专业厂商、还是自己实施，发卡行需要决定在哪里生成密钥。

6.3 卡片制造商活动

本节对必须由卡片制造商执行的活动做一介绍。

6.3.1 先决条件

在生产卡片之前，卡片制造商必须：

- 通过银联标识卡产品企业资格认证；

  接受银联资格认证办公室的现场考察和卡片检测。
- 通过银行卡检测中心的 PBOC(借记/贷记)认证；
- 接收发卡行卡片设计；
- 将发卡行主密钥(KMC)导入硬件安全模块(HSM)，这个密钥用来派生三个密钥；

  K_{MAC}—用来锁闭 PBOC 卡的应用区，并对个人化过程中装载到卡片的个人化数据进行检验，证实它们完整无损，且没有被修改。

  K_{ENC}—用来生成 IC 卡密文和验证主机密文。

  K_{DEK}—用来加密在个人化过程中写入卡片的保密数据。

  KMC 对每个发卡行是独有的，而 K_{MAC}，K_{ENC} 和 K_{DEK} 对每张卡是独有的。

6.3.2 执行活动

在制作芯片卡过程中，卡片制造商一般执行以下步骤：

1. 将卡片设计制作到白卡上。
2. 在塑料卡基上嵌入芯片。
3. 初始化借记/贷记应用，例如：将卡内计数器置0、设置基本数据元。
4. 确定卡内文件结构，创建文件，决定哪些数据元放进哪些记录。
5. 由KMC派生一个独有密钥K_{MAC}，每个PBOC应用要求一个K_{MAC}。
6. 使用K_{MAC}锁定借记/贷记应用，这个处理确保PBOC应用从初始化直到个人化期间保持安全。也用于确保在个人化过程中数据不被篡改。
7. 使用KMC派生K_{DEK}，并装载到卡内；这个密钥用于在个人化操作中加、解密装载到卡内的敏感数据。
8. 安全传送卡片至发卡行，或在发卡行同意的情况下直接发给卡片个人化厂商。

6.4 个人化活动

发卡行可以自己进行个人化处理，或外包给第三方个人化厂商。本节提供了一个对个人化处理的概述。

6.4.1 先决条件

在开始个人化处理之前，必须先升级个人化系统以支持芯片卡个人化。如果发卡行由第三方个人化厂商提供服务，这个个人化厂商必须通过银联标识卡个人化企业资格认证。当然，如果发卡行在内部对自己的卡片（或属于同一集团的）进行个人化操作，不需要通过银联认证。

个人化系统的硬件安全模块(HSM)应该包含以下 DES 密钥：

- 发卡行主密钥(KMC)－个人化系统使用 KMC 派生以下密钥：
  - ✓ K_{MAC}—用来锁闭 PBOC 卡的应用区，并对个人化过程中装载到卡片的个人化数据进行检验，证实它们完整无损，且没有被修改。
  - ✓ K_{DEK}—用来加密在个人化过程中写入卡片的保密数据。
- 密钥交换密钥(KEK)－个人化系统使用 KEK 解密个人化输入文件中的敏感数据。

6.4.2 执行活动

以下是卡片个人化厂商执行的个人化步骤：

1. 从发卡行或卡片制造商处接收卡片。这个应该是已经包含卡片设计、初始化了PBOC应用的芯片、被K_{MAC}锁定、K_{DEK}存储在卡内、磁条还未编码。

2. 从发卡行接收个人化输入文件。这个输入文件应该包含所有卡片数据：凸印数据（如适用）、印刷数据（如适用）、磁条的编码数据、芯片的PBOC数据，以及其它任何芯片应用数据，例如：积分或储值数据。文件中任何敏感数据应该使用KEK加密。

3. 将芯片卡和个人化输入文件装入个人化系统。

4. 使用KMC为每张卡派生K_{MAC}和K_{DEK}。

5. 使用K_{MAC}解锁芯片卡的PBOC应用。

6. 使用KEK解密个人化输入文件的所有敏感数据。

7. 使用K_{DEK}重新加密这些敏感数据。

8. 装载明文数据和使用K_{DEK}加密的密文数据到芯片内，在每个文件放置合适的数据。芯片使用K_{MAC}验证个人化数据没有被篡改，接着使用K_{DEK}解密密文数据，以明文形式安全地存放在芯片内。

   制造商所设计的芯片架构，可以做到安全存储敏感数据，确保虽然数据是明文形式，但是未授权方无法存取它。卡片制造商（或芯片制造商）有责任在芯片中建立这种安全机制，发卡行不需要对此采取任何行动。如果有兴趣了解更多细节，请查阅EMV和PBOC规范。

9. 从PBOC应用中删除K_{MAC}和K_{DEK}。

   这样做是为了防止任何未授权方进一步个人化卡片，但是不排除通过“发卡行脚本处理”来实现发卡行授权的发卡后变更。

注：对于技术细节，请查阅《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》

6.5 后个人化活动

在卡片个人化之后，银联建议发卡行或其服务商在分发卡片给持卡人之前，检查个人化卡片的正确性。

建议执行的后个人化活动包括：

1. 决定是否要求执行个人化质量验证活动；

   银联强烈建议发卡行在卡片发行之前执行质量验证处理，确保个人化卡片的正确性。这个检查对于避免持卡人遭遇因个人化错误引发的用卡故障，是十分必要的。

2. 描述对个人化质量验证处理的需求；

3. 决定实现方式：内部自建个人化质量验证工具，或购买现成产品，或让个人化厂商完成这个任务；

   对于多数发卡行，购买工具比自建一个要更加可行，因为有许多专做卡片质量验证工具的国际或本地厂商可供选择。如果计划购买工具，发卡行应该评估各种产品，选择最符合自己要求的工具。银联的PBOC测试工具包中也提供类似工具。

4. 安装并测试工具，确保卡片个人化的正确性；

银联建议发卡行对于首批个人化卡片进行广泛、详细的测试，在此基础上，对后续各批个人化卡片进行抽测。

7 个人化要求

本章目的是帮助发卡行建立个人化输入文件。个人化输入文件是发卡行提供给个人化厂商或个人化员工进行芯片卡个人化的信息文件。

本章关注于策略和操作活动，提供深层次的技术信息。

本章内容假设发卡行已经决定支持 PBOC 功能，因此对每个功能的背景信息和益处就不在此讨论了。

发卡行应该意识到，其产品成功与否是受整体决策影响的，而不只是个别决定；因此做好决策是十分重要的。银联可以提供协助，卡片或个人化厂商对于许多业务和技术活动也可以提供协助。对于发卡行要求的其它活动，发卡行可以和服务商一起来评估：哪些由厂商提供支持、哪些由发卡行内部处理。

7.1 应用选择

面对一张 PBOC 借记/贷记卡片，终端要通过比较卡内 AIDs 和终端维护的 AIDs，决定哪些是卡片和终端都支持的应用。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都支持的应用列表。目录选择方法对于终端是强制要求，对于卡片是可选的；AID 列表选择方法是卡片和终端都强制要求的。

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。

接着要从候选列表中选择一个应用进行交易，根据终端能力可采用以下方式之一：

- 持卡人选择应用
  - ✓ 终端支持持卡人确认
    终端根据发卡行定义的优先级顺序逐条显示共同支持的应用，供持卡人确认使用。
  - ✓ 终端支持持卡人选择
    终端根据发卡行定义的优先级顺序一次性全部显示共同支持的应用，供持卡人选择使用。
- 终端自动选择应用
  终端使用应用优先权指示符自动选择具有最高优先级的应用。

发卡行可以安排了解市场上各类终端，关注几个方面：显示类型、存储能力、终端完善性和商户场所。

发卡行必须设置卡片应用支持应用选择。本节描述了实现应用选择的相关决策、业务和技术活动：

- 应用选择数据－个人化数据。
- 持卡人确认
  对于卡内每个应用，发卡行必须决定是否没有持卡人确认应用不能选择，或者是否允许终端自动选择具有最高优先级的应用。
- 目录选择方法和 AID 列表选择方法

卡片必须支持 AID 列表选择方法，目录选择方法对于卡片是可选的，发卡行需决定是否想要卡片支持这个功能。

7.1.1 应用选择数据

发卡行应该确保设置应用选择的合适数据，这些数据包括：

- 应用标识符(AID)
- 应用标签
- 应用首选名称
- 发卡行代码表索引（如果有应用首选名称）
- 应用优先指示器
- 首选语言

7.1.1.1 应用标识符

应用标识符(AID)是代表应用类型的一串数值，在应用选择中用到。终端将卡内所列 AIDs 和它支持的 AIDs 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。对于卡内每个应用，必须通过个人化对应分配一个 AID。

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1 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

如果一张卡片中有超过一个应用使用相同的 AID（例如：两个贷记应用），卡片 AID 必须要有一个后缀以示区别。后缀提醒终端卡片中有超过一个应用使用相同的 AID，确保在候选列表中所有应用都分配一个单独的 AID。

后缀是加在 AID 末尾的 2 位数字，例如：发卡行的卡片支持两个贷记应用，可以使用以下格式个人化这两个应用的 AID：

- A0000003330101020**1**－第一个PBOC贷记应用
- A0000003330101020**2**－第二个PBOC贷记应用

注：这个后缀不确定应用优先级。

7.1.1.2 应用命名

终端可以显示应用名称给持卡人，以便其选择想要的应用进行交易。这个名称是持卡人识别卡内应用的媒介，通过两个数据元实现之：应用标签和应用首选名称。本节提供的指导方针将帮助发卡行清楚认识 PBOC 应用怎样支持、促进应用选择。

7.1.1.2.1 应用标签

应用标签是强制数据元，必须在卡内设置。这个数据元标识应用，在应用选择过程中会显示这个应用名称给持卡人，除非卡内存在应用首选名称。应用首选名称将在下节解释。

应用标签必须包含“PBOC”这个词语和对支付功能、产品或两者的清晰说明，以便区别卡内这些应用。它可以使用空格，这也应该被正确识别。

7.1.1.2.2 应用首选名称

应用首选名称作为一个可选项，可以在卡内设置，它是应用的首选命名约定。如果终端具备显示应

用的能力，它将搜索应用首选名称；如果应用首选名称不存在，终端显示应用标签。

如果应用首选名称存在，终端检查卡内另一个数据元－发卡行代码表索引，判断它是否支持这个应用首选名称所对应的字符集（ISO 8859 定义），以便向持卡人正确显示其名称。如果终端不支持发卡行代码表索引中定义的字符集，终端就不能正确显示应用首选名称；在这种情况下，终端显示应用标签。

应用首选名称的数据应该与应用标签一致；但是，PBOC 不对应用首选名称的命名规则作明确要求，发卡行可以使用这个数据域放置自己的品牌名称。

7.1.1.3 应用优先指示器

当卡片支持超过一个支付应用时，必须对每个应用指定应用优先指示器来区分其优先级。这个优先级指示器决定在持卡人选择过程中，向持卡人显示终端和卡片共同支持应用的顺序。如果终端不支持持卡人选择，终端会自动根据应用优先指示器选择共同支持的应用。

发卡行可以对多个应用分配相同的优先级。但是，对于不支持持卡人应用选择的终端，将由其决定选择哪个应用，这可能造成持卡人的混淆。

注：如果使用应用优先指示器，在磁条中有映射的芯片支付应用必须设置为最高优先级。如果同时具有非银联应用，要求银联支付应用的优先级应高于非银联应用。

7.1.1.4 首选语言

为了在交易点向持卡人提供客户化体验，终端有能力做到用持卡人的首选语言显示交易信息。发卡行可以通过“首选语言”这个数据元个人化卡片，设置一个或多个首选语言；最多可以支持 4 个语言。如果要提供超过一个语言，必须分配每个语言的优先次序。

注：“首选语言”数据元按照 ISO 639 进行编码，这些代码使用小写字母表示语言，在卡内编码首选语言必须用小写。

7.1.1.5 执行活动

对于应用选择相关卡片数据元需要执行的活动包括：

- 策略

  因为应用首选名称、应用优先指示器和首选语言都是可选项，发卡行需要决定是否在卡内使用之。

  由于这些数据元给予发卡行对应用选择更强的控制，提供更贴近持卡人的体验，银联建议在卡内使用这些数据元。

- 业务
  - ✓ 决定卡内驻留何种应用；
  - ✓ 确定在应用选择中如何向持卡人显示应用名称；
  - ✓ 当支持多个支付应用时，使用应用优先指示器区分 PBOC 应用的优先次序；在磁条和卡面凸印/印刷对应的账户，应该设置为最高优先级；
  - ✓ 如果支持首选语言，决定在卡内支持何种语言；当支持超过一种语言，需确定其优先次序。
- 技术

  发卡行应该在个人化文件中包含以下数据元，确保这些数据元被个人化：
  - ✓ 如果卡内两个应用使用相同的 AID，要在 AID 末尾添加一个唯一的后缀；
  - ✓ 应用标签；
  - ✓ 应用首选名称和发卡行代码表索引（如果支持）；
  - ✓ 应用优先指示器（当支持超过一个支付应用时）；
  - ✓ 首选语言（如果支持，并且如果提供超过一种语言时区分优先次序）。

7.1.2 持卡人确认

发卡行可以设置 PBOC 应用要求持卡人确认。实现这个选项，要求持卡人在交易点与终端进行交互；持卡人被要求对于终端显示内容，按键选择应用。

发卡行将持卡人确认作为一个客户服务选项，有助于客户了解是在使用哪个应用进行交易。

注：如果卡片仅支持一个 PBOC 支付账户，持卡人确认是不要求的。

对于持卡人确认，要求决策者、业务部门、技术人员做的包括：

- 策略

  对于卡内每个 PBOC 支付应用，决定是否要求持卡人确认选项。

  发卡行可以选择设置 PBOC 应用要求持卡人确认。如果终端不支持持卡人确认，那么要求持卡人确认的 PBOC 应用将不被其支持。终端自动选择具有最高优先级且不要求确认的应用。这种终端不允许持卡人选择应用进行交易，也不能选择要求持卡人确认的卡内应用。

  如果发卡行有这样的市场需求，要求卡片支持持卡人确认、设备支持持卡人选择应用，请联系银联代表了解发卡行的市场需求。

  因为不是所有终端支持这个功能，如果卡内只有一个支付应用，发卡行不应该要求对此应用进行持卡人确认。对于多应用卡，银联建议对于首要应用（在磁条中所映射的应用）不支持持卡人确认，这样在终端仅支持持卡人选择应用的情况下，可以尽量避免出现受理问题。

- 业务

  如果需要，将持卡人确认作为一个需求提交给卡片供应商。

- 技术

  在个人化文件中加入持卡人确认参数，确保这些参数被个人化。

7.1.3 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

  这种方法对于卡片是可选的，对于终端是强制要求；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

  这种方法对于卡片和终端都是强制的。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。

与目录选择方法和 AID 列表选择方法相关的活动包括：

- 策略

  决定发卡行的卡片除了强制的 AID 列表选择方法，是否支持目录选择方法。

  银联认为，仅支持 AID 列表选择方法一般就足够了，除非发卡行所处市场的终端支持许多应用。虽然影响交易时间的因素很多，但在终端支持许多应用的情况下，目录选择方法确实可以减少应用选择过程的持续时间。

- 业务

  定义对于应用选择方法的要求，与供应商合作确保卡内包含合适的功能。如果计划实现目录选择方法，向供应商提出明确要求是十分重要的，因为一些供应商的卡片目前不提供这个功能。

- 技术

  如果计划实现目录选择方法，卡片必须包含 PSE。反之，则不需要在卡内建立 PSE。关于 PSE 的技术细节请参考 EMV 和 PBOC 文档。

7.2 应用初始化

在终端选择应用之后，必须请求卡片读取该应用的应用数据。根据交易特性，卡片有可能指示不同的数据或支持功能。例如，对于国内或国际交易可以设置不同的持卡人验证方法，卡片可以发送不同的持卡人验证方法(CVM)列表给终端。关于 CVM 列表的信息，请参考 7.5.1 节“持卡人验证定制”。

基于某个应用的国内/国外使用要求，允许检查、中断交易。例如，应用设置为限于国内使用，当卡片在国外环境中使用时，交易将被中断；终端返回应用选择阶段，选择另一个应用进行交易。

与应用初始化相关的活动包括：

- 策略

  决定不同的处理规则（如果有的话，如：基于终端类型、商户环境、跨地区使用等对交易的不同影响）。

  决定是否需要限制卡片在国内或国外使用。

- 业务

  与供应商沟通发卡行的特殊处理需求。明确需求是什么重要的，因为有些供应商目前不一定支持这种功能。

- 技术

  如果发卡行希望根据交易特性，卡片有可能向终端指示不同的数据或支持功能，或基于国内/国外使用的控制而中断交易，发卡行的卡片必须包含处理选项数据对象列表(PDOL)。PDOL 包含终端传送给卡片的数据对象的标签，这个处理所要求的任何终端数据都在 PDOL 中指定，例如：为了实现国内和国外的检查，PDOL 必须包含终端国家代码的标签。

7.3 脱机数据认证

通过公钥技术，可以在交易点验证卡内数据，这个验证称为脱机数据认证。脱机数据认证保护卡内数据、避免被篡改，帮助发现伪卡。

PBOC 有两种脱机数据认证类型：静态数据认证(SDA)和动态数据认证(DDA)。DDA 又包括标准 DDA 和复合 DDA/应用密文生成（CDA）两种认证方式。SDA 可以确保卡片在个人化之后，发卡行选定的数据不会被篡改。相较 SDA，DDA 还可以防御在脱机环境中复制芯片数据，因为卡片生成一个唯一的密文供终端进行验证。由于 DDA 需要在卡内进行更多的加密运算，卡片配置密码处理器是必要的。CDA 把动态签名生成与卡片的应用密文生成相结合，确保卡片行为分析时返回的应用密文来自于有效卡。

卡片是否支持 SDA、DDA 和 CDA 是可选的。如果卡片支持 DDA 或 CDA，就必须支持 SDA；这样在不支持 DDA 或 CDA 的终端上，可以进行 SDA 处理。

如果卡片不支持任何脱机数据认证方法，所有交易都发送联机授权请求。

本节从以下几方面着手，帮助发卡行实现脱机数据认证：

- 整体决策
- SDA 执行业务和技术活动
- DDA 执行业务和技术活动

7.3.1 整体决策

本节描述支持脱机数据认证的决策要求：

- 需要验证数据

  决定在 SDA 或 DDA 中需要验证的数据。

- 脱机数据认证交易点动作

  决定在交易点根据脱机数据认证结果应该采取的动作（脱机批准、脱机拒绝、上送联机）。

- 公钥策略

  为了实现脱机数据认证，制定一系列公钥机制的决策。

7.3.1.1 需要验证数据

SDA 验证一个数据集，确保其自卡片发行之后没有被修改。发卡行应该确定哪些数据元需要验证。

PBOC 建议：如果卡片也支持 DDA，将 AIP 加入静态认证数据集。

使用 DDA，卡片可以要求终端数据参与签名的生成。这个数据增加了签名的可变性，提供防御复制数据的保护。卡片要求的终端数据必须包含不可预知数；当然，也可以要求其它终端数据，例如：交易金额。标准 DDA 通过 DDOL 指定参与签名的终端数据元，而 CDA 会使用 CDOL、PDOL 指定的终端数据元参与签名。

DDA 也验证卡内静态数据，它与 SDA 验证的是同一套静态数据。PBOC 要求应用交易计数器参与动态签名的生成，以增加签名的可变性。

发卡行还可以包含另外的数据元，以适应风险管理的需要。

7.3.1.2 脱机数据认证风险管理检查

针对脱机数据认证的处理结果，可以在终端行为分析阶段进行一系列风险管理检查。对于每个检查，发卡行需要决定当风险管理条件被触发时，基于自身利益应该执行什么动作。这些动作是脱机批准、脱机拒绝或上送联机。发卡行通过发卡行行为代码(IACs)设置这些检查点，并个人化至卡内。

如果决定上送联机，还需决定当不能联机时，应该执行什么动作：脱机批准或脱机拒绝。

下表给出了银联对于这些策略的推荐动作：

表2 脱机数据认证风险管理检查

条件	描述	推荐动作
未进行脱机数据认证	在脱机数据认证过程中，SDA 或 DDA 未执行。当终端不支持脱机数据认证时就会发生这种情况。	上送联机；如果不能联机，脱机拒绝。
脱机静态数据认证(SDA)失败	终端执行 SDA 失败。	上送联机；如果不能联机，脱机拒绝。
脱机动态数据认证(DDA)失败	终端执行 DDA 失败。	上送联机；如果不能联机，脱机拒绝。
IC 卡数据缺失	终端检查支持脱机数据认证所要求的卡片数据，发现缺失部分或全部数据。这可能发生在以下情况：卡片个人化异常、欺诈罪犯删除了部分或全部与脱机数据认证相关的卡片数据。	上送联机；如果不能联机，脱机拒绝。
复合动态数据认证/应用密文生成（CDA）失败	终端执行 CDA 失败。	脱机拒绝。

7.3.1.3 公钥决策

本节集中描述公钥管理整体的商业、政策和风险管理方面的决定。这些决策影响发卡行实现脱机数据认证、脱机密文 PIN。

使用公钥技术进行验证的参与方都必须生成一个或多个 RSA 发卡行公钥对。公钥对包含一个公钥和一个私钥，它们是数学相关的，使用一个密钥加密（或签名）信息，可以使用另一个密钥进行解密（或验证）。

发卡行将其公钥发给银联认证中心(根 CA)，生成发卡行公钥证书。认证中心是分发和回收证书的可信任的管理机构，自愿保证其发布的证书与对应密钥的一致性。一个发卡行证书（也称为发卡行公钥证书），是根 CA 使用其私钥对发卡行公钥进行签名所生成的。

注：对于每个使用公钥技术的 PBOC 应用要求独立的公钥。

在向认证中心申请公钥证书之前，发卡行需要对密钥管理制定一系列决策，它们包括：

- 需要产生的发卡行公钥数量；

- 产生的密钥的长度；
- 每个密钥的失效期；
- 密钥的指数；
- 当从认证中心收到多个发卡行公钥证书时，选择合适的证书加载到卡片中。

发卡行风险管理人员必须分析、权衡成本与收益，决定最佳的风险管理模式。银联在本节所提供的建议，有助于发卡行的决策。

除了这些建议，银联提请发卡行注意追踪公钥技术的最新发展、咨询公钥技术专家。

7.3.1.3.1 需要生成的发卡行公钥数量

发卡行必须决定需要生成的公钥数量；通常，公钥越多，安全性越高。可是，生成的每个密钥都需要管理费用。发卡行应该考虑：所有密钥的安全存放、监控装置的安装需要、管理公钥失效日期、存档失效密钥。

基于风险管理体系，发卡行需要有一定的灵活性来决定：对于某个卡段的所有卡片使用一个密钥，或使用多个密钥以降低风险。银联不限制发卡行使用的发卡行公私钥对个数，因为发卡行公私钥对的个数并不影响终端对一张 IC 卡的认证。这样发卡行可以根据其业务需求选择使用一个或多个发卡行公私钥对进行它的发卡业务，需要考虑的因素有每一类 IC 卡产品、持卡人所在区域等。然而，为安全性考虑，银联建议发卡行根据发卡行标识代码（BIN）来申请发卡行公钥证书，并使用不同的发卡行公私钥对来对具有不同 BIN 号的 IC 卡进行发卡业务。这种方式能在发生发卡行签名私钥失密时更有效地控制安全和业务风险。因此，银联要求发卡行的公钥证书申请中包括 BIN 号。

7.3.1.3.2 发卡行公钥长度

发卡行必须决定要生成的发卡行公钥的长度。本节概述了决定发卡行公钥长度的相关建议。

注：公钥长度通常按位来表示，例如：1024 位，必须是 8 的整数倍。

通常，公钥越长安全性越高，但较长的公钥需要更多的交易时间；反之，较短的公钥交易速度快了，但安全性弱于较长的公钥。

如果准备支持 DDA，银联建议发卡行与候选卡片供应商一起评估其产品的公钥处理性能，获得准确数据；进而，发卡行可以提出对交易时间的要求。

发卡行公钥必须被根 CA 私钥签名。在满足以下两个条件的基础上，根 CA 使用尽可能多的根 CA 私钥对发卡行公钥进行签名：

- 发卡行公钥失效日期早于或等于根CA公钥失效日期；
- 发卡行公钥长度小于或等于根CA公钥长度。

对发卡行公钥长度的唯一要求是：发卡行生成公钥小于或等于最长的根 CA 公钥。

当前 根 CA 最大公钥长度是 1984 比特，银联会周期性地评估市场的安全风险及相关因素，有计划地引入新的公钥对。如需这方面的最新信息请联系银联代表。

7.3.1.3.3 发卡行公钥失效日期

本节针对如何决定发卡行公钥合适的失效日期，给出建议。

发卡行公钥必须被根 CA 私钥签名。在满足以下两个条件的基础上，根 CA 使用尽可能多的根 CA 私钥对发卡行公钥进行签名：

- 发卡行公钥失效日期早于或等于根CA公钥失效日期；
- 发卡行公钥长度小于或等于根CA公钥长度。

当前根 CA 公钥对的失效日期列于下表：

表3 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

例如，如果发卡行向根 CA 提交一个公钥的失效日期是 2015 年，根 CA 将只使用 1408 比特及更长的私钥对其进行签名（假设这个发卡行公钥长度小于或等于 1408 比特）。

另外，发卡行公钥证书不应该在卡片有效期之前失效。建议个人化设备应该配置成能够验证根 CA、发卡行密钥与卡片失效日期之间的有效关系。

7.3.1.3.4 发卡行公钥指数

每个发卡行公钥有一个指数。用于脱机数据认证从发卡行公钥证书恢复发卡行公钥的 RSA 计算过程。发卡行可以使用以下两个指数之一：

- 3
- $2^{16}+1$

使用指数 3 或 $2^{16}+1$ 的安全强度区别不大，但使用后者所需运算时间明显大于前者。因此，银联建议使用指数 3。使用其它指数并不会有助于交易的安全性。

7.3.1.3.5 发卡行公钥证书

本节帮助发卡行在收到根 CA 多个证书的时候，决定使用哪个证书置入卡内。

如前所述，根 CA 使用所有长度大于或等于发卡行公钥的根 CA 私钥签发发卡行公钥证书（这时，发卡行公钥的失效日期应该是小于根 CA 公钥对的失效日期）。发卡行只有在发卡行公钥长度小于或等于 2 个（及以上）根 CA 公钥对、并且其失效日期小于这些公钥对失效日期的情况下，才会从根 CA 收到多个证书。

根 CA 发送发卡行公钥证书的同时还提供 CA 公钥索引，它用来标识签发这个发卡行公钥证书的根 CA 公钥对。“CA 公钥索引”数据元需要个人化至卡内。

7.3.1.4 决策汇总

有关脱机数据认证的决策包括：

- 决定使用SDA或DDA需要验证的数据。
- 决定在交易点针对脱机数据认证结果进行风险管理检查时希望卡片采取的动作（脱机批准、脱机拒绝、上送联机）。
- 确定公钥管理策略，详见下表：

表4 公钥管理策略

公钥管理决策	推荐策略
决定需要生成的公钥数量。	银联推荐：发卡行对于每个 BIN 生成一个发卡行公钥。
决定发卡行公钥长度。这个密钥长度必须是 8 的整数倍，并且小于或等于最长的可用根 CA 公钥。	银联推荐：发卡行公钥长度大于或等于最小的有效根 CA 公钥。
决定发卡行公钥的失效日期。	发卡行公钥失效日期必须大于或等于 PBOC 应用的失效日期，小于或等于最长的有效根 CA 公钥的失效日期。
决定发卡行公钥指数。	发卡行只能从 3 或 $2^{16}+1$ 中选择一个指数
如果从根 CA 收到超过一个发卡行公钥证书，决定哪个证书置入卡内。	发卡行应该基于其风险管理和客服体系做出决策。银联推荐使用最长的证书。

注：这些策略同样适用于脱机密文 PIN。

发卡行向根 CA 申请签发公钥证书，需向根 CA 提交发卡行公钥证书申请表和发卡行公钥输入文件，根 CA 要求按其规定的格式提供发卡行公钥；如果发卡行公钥输入文件的格式不正确，根 CA 将不能签发证书，需要发卡行重新提交文件，这将会延迟发卡行的项目进度。

银联建议：为了避免延误，发卡行可以在项目早期就向根 CA 提交签发公钥证书申请。

如果支持 DDA，需要使用 RSA 技术生成一个 IC 卡公钥对；对每个 PBOC 应用都需要生成一个公钥对。

注：IC 卡公钥对的长度必须小于或等于发卡行公钥的长度。

7.3.2 SDA 业务和技术活动

SDA 相关活动包括：

表5 SDA 执行活动

步骤	责任方	活动
1	业务	与银联代表讨论公钥和证书的生成事项。这是重要的一步，帮助发卡行明确需求和时间安排，尽量避免延误。
2	技术	基于发卡行所做相关决策：公钥数量、长度、指数值、失效日期，使用 RSA 技术生成发卡行公私钥对。
3	业务	发卡行向根 CA 申请签发公钥证书，需向根 CA 提交发卡行公钥证书申请表和发卡行公钥输入文件，根 CA 要求按其规定的格式提供发卡行公钥；如果发卡行公钥输入文件的格式不正确，根 CA 将不能签发证书，需要发卡行重新提交文件，这将会延迟发卡行的项目进度。
4	银联	根 CA 使用合适的根 CA 私钥对发卡行公钥进行签名，生成发卡行公钥证书。在满足以下两个条件的基础上，根 CA 使用尽可能多的根 CA 私钥对发卡行公钥进行签名： • 发卡行公钥失效日期早于或等于根 CA 公钥失效日期。 • 发卡行公钥长度小于或等于根 CA 公钥长度。
5	银联	银联将签发的发卡行公钥证书返回给发卡行。如果收到多个证书，发卡行应该基于其风险管理和客服体系来决定使用哪个证书置入卡内。
6	技术	为每个 PBOC 应用生成签名的静态应用数据(SAD)，SAD 是通过 SDA 验证的数据使用发卡行私钥签名得到的哈希结果。这个操作是预个人化活动的一部分。 计算这个哈希结果使用的是安全哈希算法 1(SHA-1)，SHA-1 是一个公开算法，在 FIPS 180-1 中被标准化。
7	技术	将发卡行公钥证书、发卡行公钥指数、发卡行公钥余项（如果需要）、CA 公钥索引、签名的静态应用数据与其它个人化数据一起加入个人化输入文件。 应该审慎地管理这些信息，保证合适的证书和 SAD 置入合适的卡片。如果卡片装入不正确的信息，脱机数据认证将会失败，潜在地影响卡片的使用。

7.3.3 DDA 业务和技术活动

DDA 相关活动包括：

表6 DDA 执行活动

步骤	责任方	活动
1-6		参见“表 5 SDA 执行活动”
7	技术	使用 RSA 技术生成一个 IC 卡公钥对；对每个 PBOC 应用都需要生成一个公钥对。 注：IC 卡公钥对的长度必须小于或等于发卡行公钥的长度。
8	技术	为每个 PBOC 应用生成一个 IC 卡公钥证书。发卡行使用发卡行私钥对 IC 卡公钥签名，生成 IC 卡公钥证书。这个操作是预个人化活动的一部分。
9	技术	将发卡行公钥证书、发卡行公钥指数、发卡行公钥余项（如果需要）、CA 公钥索引、签名的静态应用数据、IC 卡私钥、IC 卡公钥证书、IC 卡公钥指数、IC 卡公钥余项（如果需要）、动态数据认证数据对象列表（DDOL）与其它个人化数据一起加入个人化输入文件。 应该审慎地管理这些信息，保证正确的数据置入卡内。 由于 IC 卡私钥是敏感数据，必须加密存放在个人化输入文件中。它与输入文件中其它敏感数据一起，应该使用密钥交换密钥(KEK)进行加密。

7.4 处理限制

终端通过处理限制来检查 PBOC 应用数据，判断交易是否允许继续。检查内容包括应用生效日期、应用失效日期、应用版本号以及其他发卡行定义的限制控制条件，发卡行可以使用应用用途控制(AUC)

来限定卡片用于国内还是国际间，或能否用于现金、购物、服务。

处理限制进行以下检查：

- 应用版本号检查（强制）
- 应用用途控制检查（可选）
- 应用生效日期检查（可选）
- 应用失效日期检查（强制）

以下着重对可选检查项进行说明。

7.4.1 应用用途控制检查

应用用途控制检查和为磁条卡交易执行的服务代码检查类似，芯片数据元“应用用途控制”(AUC)指定卡片能够在哪里（国内或国外）使用什么类型交易。终端检查 AUC 以决定处理是否能够继续。

发卡行需要决定对以下条件的设置并个人化至卡内：

- 国内现金交易有效
- 国际现金交易有效
- 国内商品有效
- 国际商品有效
- 国内服务有效
- 国际服务有效
- ATM 有效
- 除 ATM 外的终端有效
- 允许国内返现
- 允许国际返现

发卡行应该继续使用“服务代码”作为确定用途控制的基础，确保这个数据元在芯片内和在磁条中信息是一致的。

7.4.2 应用生效日期检查

终端将卡内应用生效日期与终端当前日期进行比较。如果支持这个检查，“应用生效日期”数据元必须个人化到卡内，这个日期必须是应用加载到卡内年月的第一天。

对于“应用尚未生效”这种情况，发卡行需要设置发卡行行为代码(IAC)来决定：希望脱机拒绝、还是要求联机；如果不能联机，是否希望脱机拒绝。

7.4.3 处理限制风险管理检查

针对处理限制的结果，可以在终端行为分析阶段进行一系列风险管理检查。对于每个检查，发卡行需要决定当风险管理条件被触发时，基于自身利益应该执行什么动作。这些动作是脱机批准、脱机拒绝或上送联机。发卡行通过发卡行行为代码(IACs)设置这些检查点，并个人化至卡内。

如果决定上送联机，还需决定当不能联机时，应该执行什么动作：脱机批准或脱机拒绝。

下表给出了银联对于这些策略的推荐动作：

表7 处理限制风险管理检查

条件	描述	推荐动作
IC 卡和终端应用版本不一致	终端检查卡片和终端的应用版本号是否不一致。	忽略此条件，继续交易。
应用已过期	终端检查卡片的应用失效日期早于终端当前日期。	上送联机；如果不能联机，脱机拒绝。
应用尚未生效	终端检查卡片的应用生效日期晚于终端当前日期。	上送联机；如果不能联机，脱机拒绝。
卡片不允许所请求的服	终端检查卡片的 AUC，判断当前交易环境是否支持卡片使用。	脱机拒绝。

务		

7.4.4 执行活动

实现处理限制所要求的活动包括：

- 策略
  - ✓ 决定是否支持应用用途控制(AUC)检查；
  - ✓ 决定是否支持应用生效日期检查；
  - ✓ 决定在交易点进行处理限制风险管理检查时希望卡片采取的动作（脱机批准、脱机拒绝、上送联机）。
- 业务

  确定卡片的 AUC 参数。
- 技术

  产生处理限制所需数据，加入个人化输入文件。数据包括：应用版本号、应用生效日期、应用失效日期、AUC 等。

7.5 持卡人验证

PBOC 允许发卡行通过使用卡内的持卡人验证方法(CVM)列表来适应交易环境的持卡人验证要求。除了现有的持卡人验证方法：签名和联机 PIN，PBOC 导入了脱机明文 PIN 验证方法。

实现持卡人验证，需要执行以下活动：

- 持卡人验证定制

  决定卡片支持的持卡人验证方法。
- 持卡人验证结果的终端行为分析

  终端使用持卡人验证结果以及卡片和终端的参数决定交易是否脱机批准、脱机拒绝或上送联机。
- 脱机 PIN

  制定脱机 PIN 的相关策略，例如：允许 PIN 尝试次数。

7.5.1 持卡人验证定制

发卡行必须决定卡片支持的持卡人验证方法。发卡行可以设置卡片支持多种持卡人验证方法，如下表所示：

表8 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：交易授权不依赖与持卡人验证。在某些商户环境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服务员，进行持卡人身份比对。

一旦决定了准备支持的持卡人验证方法，发卡行需要：

- 创建 CVM 列表并编制优先次序

终端在进行持卡人验证时使用这个优先次序列表，依次尝试完成各个 CVM。

- 决定每个 CVM 的使用条件，例如：
  - ✓ 总是执行
  - ✓ 如果终端支持此 CVM
  - ✓ 基于交易金额

    这要求交易使用的是卡片应用货币。例如：可以设置交易金额低于￥200，使用签名；高于￥200，使用脱机明文 PIN。
- 如果当前 CVM 失败了，决定是否执行下一个 CVM。

下面给出一个简单的 CVM 列表的例子，某个发卡行希望按以下优先次序进行持卡人验证：

- 所有 ATM 交易和返现交易使用联机 PIN。
- 如果终端支持脱机 PIN，POS 交易使用脱机 PIN。
- 如果终端不支持脱机 PIN，POS 交易使用签名。
- 如果终端不支持脱机 PIN 或签名，不需要 CVM。

表9　CVM 列表例子

CVM 优先次序	条件	注释
金额 X	0	CVM 列表中不检查金额
金额 Y	0	CVM 列表中不检查金额
CVM 入口 1		ATM 交易使用此 CVM 入口
CVM 条件	01-如果现金或返现	
CVM 类型	000010b-联机加密 PIN 验证	
CVM 代码	1b-如果失败持卡人验证失败	
CVM 入口 2		POS 交易使用此入口 如果终端支持脱机明文 PIN 核对，执行此 CVM
CVM 条件	03-如果终端支持	
CVM 类型	000001b-脱机明文 PIN 验证-	
CVM 代码	1b-如果失败持卡人验证失败	
CVM 入口 3		如果终端不支持脱机明文 PIN 核对，执行此入口。 如果终端支持收集签名，执行此 CVM
CVM 条件	03-如果终端支持	
CVM 类型	011110b-签名	
CVM 代码	0b-如果失败执行下一个 CVM	
CVM 入口 4		如果终端不支持脱机明文 PIN 核对和签名，执行此入口。 CVM 不可能失败
CVM 条件	00-总是	
CVM 类型	011111b-不需要 CVM	
CVM 代码	1b-如果失败持卡人验证失败	

本节概述了进行持卡人验证定制的相关活动：

- 策略

  决定发卡行计划支持的持卡人验证方法。其中签名验证方法是必须支持的，“无需 CVM”这种方法只能在 CVM 列表的最后。如果希望卡片能够在只支持联机 PIN 的 ATM 或其它无人值守设备上使用，发卡行必须将联机 PIN 方法加入 CVM 列表。
- 风险管理

  发卡行应该基于商业评估、市场影响来做出决定：除了现有的 CVM，是否支持其它 CVM。但是，发卡行应该尽量考虑支持脱机明文 PIN 验证方法，以减少失窃卡所带来的风险。
- 业务

  创建 CVM 列表，包括：制定 CVM 优先次序、使用条件等。

- 技术

在个人化中包含 CVM 列表。如果支持脱机明文 PIN，必须将脱机 PIN 相关数据个人化至卡内。

7.5.2 持卡人验证风险管理检查

针对持卡人验证的处理结果，可以在终端行为分析阶段进行一系列风险管理检查。对于每个检查，发卡行需要决定当风险管理条件被触发时，基于自身利益应该执行什么动作。这些动作是脱机批准、脱机拒绝或上送联机。发卡行通过发卡行行为代码(IACs)设置这些检查点，并个人化至卡内。

如果决定上送联机，还需决定当不能联机时，应该执行什么动作：脱机批准或脱机拒绝。

下表给出了银联对于这些策略的推荐动作：

表10 持卡人验证风险管理检查

条件	描述	推荐动作
持卡人验证失败	终端执行卡片支持的任何 CVM 都不成功。	脱机拒绝。
未知的 CVM	终端无法识别 CVM 列表中的一个 CVM。 如果导入一个新的 CVM，而终端没有相应设置以识别它，就会发生这种情况。	忽略此条件，继续交易。
PIN 尝试次数超限	在当前或前一交易，持卡人尝试输入 PIN 次数超限。意味着脱机 PIN 验证失败。	上送联机；如果不能联机，脱机拒绝。
要求输入 PIN 但密码键盘不存在或不工作	卡片和终端支持 PIN 处理，但由于密码键盘未连接终端或无法工作，PIN 不能输入。	上送联机；如果不能联机，发卡行采取什么动作将依赖于对风险控制和客户服务的权衡。
要求输入 PIN，密码键盘存在，但未输入 PIN	卡片和终端支持 PIN 处理，但是持卡人未输入 PIN。	上送联机；如果不能联机，发卡行需要在风险控制和客户服务之间做一权衡，决定采取什么动作。 在 PBOC 应用发行的初期，持卡人可能会不记得他的脱机 PIN；如果发卡行选择“脱机拒绝”，那么即使是真实的持卡人在操作这笔交易，这种交易也被脱机拒绝。
输入联机 PIN	当前交易的 CVM 是联机 PIN，并且输入了联机 PIN。	上送联机；如果不能联机，脱机拒绝。
IC 卡数据缺失	终端检查支持持卡人验证所要求的卡片数据，发现缺失部分或全部数据。这可能发生在以下情况：卡片个人化异常、欺诈罪犯删除了部分或全部与脱机数据认证相关的卡片数据。	忽略此条件，继续交易。

7.5.3 脱机 PIN

本节描述发卡行支持脱机 PIN 的特殊考虑，包括以下内容：

- PIN 的生成
- PIN 的长度
- PIN 的同步
- 发卡后 PIN 的更改
- PIN 尝试限制数

7.5.3.1 PIN 的生成

发卡行需要决定：为持卡人产生 PIN，还是允许持卡人在发卡前选择自己的 PIN。研究证明：持卡人很容易记住自己选择的 PIN，而要记住计算机自动生成的 PIN 就困难得多。

7.5.3.2 PIN 的长度

发卡行需要决定 PIN 的长度是固定的还是可变的。按照 ISO 标准，PIN 可以是 4 至 12 位数字。通常，对于持卡人选择 PIN 采取可变长度，对于自动生成 PIN 采取固定长度。

考虑到目前大多数 ATM 设备不支持超过 6 位数字的 PIN，如果 PIN 的长度超过 6 位数字，有可能使其受理范围收到限制。

7.5.3.3 PIN 的同步

如果支持芯片卡使用脱机 PIN，银联建议：和联机 PIN 保持一致。请注意：如果更改脱机 PIN 值，发卡行也应该开发程序，实现同步更改磁条和芯片的联机 PIN 值。

7.5.3.4 发卡后 PIN 的更改

发卡行需要决定是否允许持卡人在发卡后更改 PIN。如果发卡行不允许持卡人在发卡前选择自己的 PIN，这个功能是十分重要的，持卡人很可能希望定制自己的 PIN 值。

如果发卡行允许持卡人在发卡后更改 PIN，应该确保卡内存放的脱机 PIN 与持卡人的联机 PIN 一致。如果在磁条内使用 PIN 验证码(PVN)，它必须正确映射联机 PIN。芯片内的等同磁条数据也必须相应更改。

注：绝大多数发卡行在磁条内不存放 PVN，也就不存在以上问题。

另外，一旦超过 PIN 尝试限制数，脱机 PIN 自动锁定（联机 PIN 仍可使用）。发卡行应该理清面对这种情况的处理流程，例如：可以通过发卡后更改功能重置 PIN 尝试计数器；这个操作应该在安全的、发卡行控制的设备上执行。

7.5.3.5 PIN 尝试限制数

发卡行需要决定允许持卡人连续输入错误脱机 PIN 的最大次数。可以现有的联机 PIN 尝试限制数为基准来设置脱机 PIN 尝试限制数。可以要求终端在只剩一次尝试机会是显示信息提醒持卡人，如：“最后一次机会”；这对持卡人是一个有效的使用体验，但也要警惕使用失窃卡的罪犯会在脱机 PIN 被锁定之前拿走卡片。

另外，发卡行能够设置：当持卡人超过 PIN 尝试次数时，卡片自动锁定应用。这可以防止有欺诈嫌疑的持卡人到处使用。但是银联不建议这样做，因为芯片锁定脱机 PIN 的机制看来足够了。另外，发卡行有能力以适当的方式解锁 PIN。

银联建议：发卡行设置 3 次脱机 PIN 尝试机会，请注意脱机 PIN 尝试次数是独立于联机 PIN 尝试次数的，因此有 3 次脱机 PIN 尝试机会和 3 次联机 PIN 尝试机会。

7.5.3.6 执行活动

本节描述了支持脱机 PIN 要求的策略、业务和技术活动：

- 策略
  - ✓ 决定产生 PIN 的流程；
  - ✓ 决定是否允许发卡行 PIN 更改；
  - ✓ 决定解锁 PIN 的要求；
  - ✓ 决定是否设置卡片支持终端在只剩一次尝试机会是显示信息提醒持卡人；
  - ✓ 决定脱机 PIN 是否与联机 PIN 保持一致；
- 业务
  - ✓ 依据发卡行的选择，制定自动生成持卡人 PIN、或由持卡人选择 PIN 的处理流程；
  - ✓ 制定发卡后 PIN 更改的处理流程（如果支持）；
  - ✓ 制定解锁 PIN 的处理流程；
  - ✓ 确保脱机 PIN 与联机 PIN 的同步（如果适用）；
  - ✓ 确保如果脱机 PIN 被更改，也更改芯片和磁条内联机 PIN 的相关数据（如果适用）；
- 技术

  产生脱机 PIN 处理所需数据，加入个人化输入文件。数据包括：持卡人脱机 PIN（参考 PIN）、

PIN 尝试限制数。

- 风险管理
  - ✓ 决定 PIN 的长度要求；
  - ✓ 决定在 PIN 被锁定之前，允许的 PIN 尝试次数；

决定当超过 PIN 尝试次数时，卡片是否自动锁定应用。

7.6 终端风险管理

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

这些检查提供在交易点对交易处理更强的控制。帮助决定一笔交易是被脱机批准、脱机拒绝、还是发送联机授权请求。

其中与卡片有关的检查包括：

- 频度检查－PBOC 不推荐但是不排除
- 新卡检查－可选

除了这些可选检查，发卡行可根据市场需要支持其它专有的检查。

风险管理允许在交易金额低于终端最低限额的情况下，卡片寻求主机授权。在设置这些参数时，需要考虑以下因素：

- 国内授权环境
- 多种因素的组合－客户的信用级别、欺诈风险
- 国际交易的预期地点和交易量－目的地的风险高低

发卡行应该针对这些因素（也包括预期使用场所）每个组合的授权要求来配置参数。应该考虑到某些国际（或国内）环境不能可靠支持授权请求，在风险控制和方便使用之间需要谨慎地平衡。

在确定合适参数时，应考虑欺诈和信用风险管理。银联风险管理专家可以给予协助。

7.6.1 频度检查

频度检查允许发卡行在一个预先设定的连续脱机交易的数量之后要求进行联机处理。允许脱机的终端必须支持终端频度检查。发卡行可以选择不支持终端频度检查。即在个人化时，连续脱机交易的下限和上限（Tag ‘9F14’和 Tag ‘9F23’）数据不写入卡中。

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

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

7.6.2 新卡检查

执行频度检查的终端也应执行新卡检查，如果上次联机 ATC 寄存器值为 0，则终端将 TVR 中的“新卡”位置“1”。对第一次使用的卡片设置 TVR 中相应标志，要求交易联机处理。根据发卡行认证结果和卡片参数，交易被联机批准后，该寄存器被重新复位。

注意：卡片行为分析中，卡片也可以执行相似的新卡检查。

7.6.3 终端风险管理检查

针对终端风险管理的处理结果，可以在终端行为分析阶段进行一系列风险管理检查。对于每个检查，发卡行需要决定当风险管理条件被触发时，基于自身利益应该执行什么动作。这些动作是脱机批准、脱机拒绝或上送联机。发卡行通过发卡行行为代码(IACs)设置这些检查点，并个人化至卡内。

如果决定上送联机，还需决定当不能联机时，应该执行什么动作：脱机批准或脱机拒绝。

下表给出了银联对于这些策略的推荐动作：

表11 终端风险管理检查

条件	描述	推荐动作
卡片出现在	如果出现终端异常文件，终端就检查卡上的主帐号	上送联机；如果不能联机，脱机拒绝。

终端异常文件中	（PAN）是否列在终端异常文件上。	
商户要求联机处理	在可以联机的终端，商户可以将终端设置为交易应该联机处理。	上送联机；如果不能联机，脱机拒绝。
交易超过最低限额	终端检查交易金额是否超过商户的最低限额。	上送联机；如果不能联机，脱机拒绝。
交易被随机选择联机处理	可以支持脱机和联机交易的终端会随机选择交易进行联机处理。	上送联机；如果不能联机，脱机批准。
超过连续脱机交易下限	终端检查 ATC 减去上次联机 ATC 寄存器的差值是否大于连续脱机交易次数下限	上送联机；如果不能联机，脱机批准。
超过连续脱机交易上限	终端检查 ATC 减去上次联机 ATC 寄存器的差值是否大于连续脱机交易次数上限	上送联机；如果不能联机，脱机拒绝。
新卡	终端检查卡片是否第一次使用。	上送联机；如果不能联机，脱机批准。

7.6.4 执行活动

实现终端风险管理所要求的活动包括：

- 策略
  - ✓ 决定是否支持终端频度检查；
  - ✓ 决定是否支持终端新卡检查；
  - ✓ 决定在交易点进行终端风险管理检查时希望卡片采取的动作（脱机批准、脱机拒绝、上送联机）。
- 业务

  确定卡片的频度参数。
- 技术

  产生终端风险管理所需数据，加入个人化输入文件。数据包括：连续脱机交易下限(LCOL，Tag ‘9F14’)、连续脱机交易上限(UCOL，Tag ‘9F23’)、上次联机 ATC 寄存器等。

7.7 卡片行为分析

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

- 上次交易的行为
- 新卡
- 交易频度计数器

7.7.1 卡片风险管理

下表总结了卡片行为分析阶段所有卡片风险管理检查，并标明这些检查是否强制或可选，同时描述了检查的结果。

表12 卡片风险管理检查

风险管理检查	执行条件	结果（如果条件满足）
联机授权没有完成（上次交易）	有条件－－如果支持发卡行脚本命令或发卡行认证则执行	请求联机处理，设置 CVR 指示位
上次交易发卡行认证失败(或上次交易发卡行认证强制但是没有执行)	有条件－－如果支持发卡行认证则执行	设置 CVR 指示位 检查 ADA 如果指明则请求联机处理
上次交易 SDA 失败	有条件－－如果支持 SDA 则执行	设置 CVR 指示位
上次交易 DDA 失败	有条件－－如果支持 DDA 则执行	设置 CVR 指示位

上次联机交易发卡行脚本处理	有条件——如果支持二次发卡（post-issuance）则执行	在CVR中保存脚本命令的个数 如果脚本处理失败（使用卡片内的发卡行脚本失败指示位），设置CVR指示位。ADA中的设置决定交易是否联机处理
连续脱机交易下限频度检查	可选——如果上次联机ATC寄存器和连续脱机交易下限（Tag‘9F58’）存在，卡片执行此检查。	如果限制数超过，请求联机处理 设置CVR中指示位
连续国际脱机交易（基于货币）频度检查	可选——如果应用货币代码、连续脱机交易计数器（国际-货币）、连续脱机交易限制数（国际-货币）存在，卡片执行此检查	如果限制数超过，请求联机处理 设置CVR中指示位
连续国际脱机交易（基于国家）频度检查	可选——如果发卡行国家代码、连续脱机交易计数器（国际-国家）、连续脱机交易限制数（国际-国家）存在，卡片执行此检查。	如果限制数超过，请求联机处理 设置CVR中指示位
使用指定货币的累计脱机交易金额频度检查	可选——如果应用货币代码、累计脱机交易金额、累计脱机交易金额限制数存在，卡片执行此检查。	如果限制数超过，请求联机处理 设置CVR中指示位
累计脱机交易金额（双货币）频度检查	可选——如果应用货币代码、第二应用货币代码、货币转换因子、累计脱机交易金额（双货币）、累计脱机交易金额限制数（双货币）存在，卡片执行此检查。	如果限制数超过，请求联机处理 设置CVR中指示位 如果使用的货币是第二货币，需要先进行货币转换
新卡检查	可选——如果上次联机ATC寄存器、应用缺省行为(ADA)存在，卡片执行此检查。	如果以前没有请求过联机本次可以申请联机 设置CVR中指示位
脱机PIN验证没有执行（PIN尝试限制数超过）	可选——如果支持脱机PIN，数据元应用缺省行为存在，卡片执行此检查。	设置CVR中如果本次交易脱机PIN验证没有执行而且PIN尝试限制数在之前已经超过指示位 ADA中设置这种情况下交易拒绝或请求联机

7.7.2 执行活动

实现卡片行为分析阶段卡片风险管理所要求的活动包括：

- 策略
  - ✓ 确定针对“上次交易行为”各项检查的条件是否满足；
  - ✓ 决定是否支持卡片新卡检查；
  - ✓ 决定是否支持各项卡片频度检查；
  - ✓ 决定在交易点进行卡片风险管理检查时希望卡片采取的动作（脱机批准、脱机拒绝、上送联机）。

- 业务
  - ✓ 根据实现功能，与卡片供应商交流需要支持的数据元。
  - ✓ 确定卡片的频度参数。
- 技术

  产生卡片风险管理所需数据，加入个人化输入文件。数据包括：连续脱机交易下限（Tag '9F58'）、连续脱机交易限制数（国际-货币）、连续脱机交易限制数（国际-国家）、累计脱机交易金额限制数、累计脱机交易金额限制数（双货币）等。

7.8 联机处理

在交易处理过程中，卡片可以生成一个授权请求密文(ARQC)，用于联机卡片认证。当交易上送联机时，这个密文传送给发卡行进行验证，它提供了数据的完整性。

发卡行也可以在响应报文中返回一个授权响应密文(ARPC)，用于联机发卡行认证。卡片校验响应是否来自真实的发卡行（或其代理）、其完整性是否收到威胁。

这些密文是使用应用密文(AC)密钥生成的，AC 子密钥(UDK)存放在卡内，AC 主密钥(MDK)存放在发卡行主系统中。本节描述设置卡片支持联机卡片认证和发卡行认证所需要的活动；涉及主系统的活动，请参见第 8 章“发卡行主系统改造”。

7.8.1 决策

本节描述与联机卡片认证和发卡行认证相关的决策：

- 需要生成的主密钥数量；
- 支持发卡行认证作为强制项、还是可选项；
- 根据发卡行认证结果，卡片应该采取的动作。

7.8.1.1 生成主密钥数量

发卡行应该决定需要生成的主密钥数量。MDK 是一个双倍长的 DES 密钥；与决定需要生成的公钥数量类似，支持 MDK 越多，整个交易流程的安全性就越高。当然，维护太多的密钥会导致额外的开销。银联建议：发卡行为每个 BIN 生成一个主密钥。

每个主密钥有一个对应的分散密钥索引(DKI)，用来明确使用哪个主密钥分散得到卡片中的子密钥；DKI 作为 PBOC 专有数据需要个人化至卡内，其值不能为 0。

7.8.1.2 发卡行认证强制&可选

发卡行可以设置卡片对发卡行认证的支持是强制的或可选的。如果支持发卡行认证，它只有在发卡行（或其代理）响应报文中提供 ARPC 的情况下才会执行。

- 强制

  如果发卡行认证是强制的，只有在发卡行认证执行成功的情况下才重置相关计数器和指示器。

  如果发卡行认证是强制的，不应该设置应用缺省行为(ADA)的“如果发卡行认证必需但没有收到 ARPC，拒绝交易”位。
- 可选

  如果发卡行认证是可选的，不管发卡行认证结果如何，都将重置相关计数器和指示器。

发卡行认证（强制&可选）与卡片参数、发卡行脚本更新的协同关系如下表所示：

表13 对批准交易重置计数器 [1]

发卡行认证	发卡行认证结果		
	成功	失败	未执行
强制	重置计数器	不重置计数器	不重置计数器
可选	重置计数器	不重置计数器	重置计数器
不支持	—	—	重置计数器 [2]

1—相关计数器和指示器包括：

- 频度计数器

- 发卡行认证失败指示位
- 联机授权指示位

2－如果不支持发卡行认证，相关计数器根据批准响应进行重置。

7.8.1.3 发卡行认证风险检查

针对发卡行认证的处理结果，可以在交易结束阶段进行一系列风险管理检查。对于每个检查，发卡行需要决定当风险管理条件被触发时，基于自身利益应该执行什么动作。

下表给出了银联对于这些策略的推荐动作：

表14 发卡行认证风险管理检查

条件	推荐动作
决定如果发卡行认证失败，卡片应该采取的动作	脱机拒绝，即使发卡行批准交易；下笔交易必须联机。
如果发卡行认证是强制的，但没有收到 ARPC，决定卡片应该采取的动作。	继续进行交易，不拒绝。

7.8.2 决策汇总

本节汇总了实现发卡行认证需要做的决策以及建议。

表15 发卡行认证决策建议

决策	建议
决定需要生成的 MDK 数量	至少为每个 BIN 生成一个 MDK。
决定支持发卡行认证的方式：强制或可选。	如果发卡行认证时强制的，卡片希望每笔联机交易都收到 ARPC；如果未收到 ARPC，不重置计数器。
对于发卡行认证的处理结果，决定有关采取的动作	参见表：发卡行认证风险管理检查

7.8.3 业务和技术活动

设置卡片支持联机卡片认证和发卡行认证的相关活动包括：

表16 联机卡片认证和发卡行认证的 DES 密钥管理活动

步骤	责任方	活动
1	技术	基于发卡行决策，生成合适数量 MDK。
2	技术	为每个 MDK 分配一个分散密钥索引(DKI)，DKI 指明是用哪个 MDK 分散得到 UDK 的。
3	技术	使用 MDK 为每个 PBOC 应用派生一个 UDK，这是预个人化活动的一部分。 注：PBOC UDK 是双倍长的，出于安全考虑应该使用双倍长 KEK 加密。
4	技术	将 UDK 和 DKI 加入个人化输入文件。UDK 必须使用 KEK 加密后放入个人化输入文件。
5	技术	在个人化过程中，将 UDK、DKI 和其它个人化数据一起加载到卡内。 加载合适的 UDK 和 DKI 是十分重要的；如操作有误，可能导致联机卡片认证和发卡行认证失败。

7.9 交易结束

在交易结束处理过程中，如果请求了联机处理但是终端不支持联机或者联机授权没有完成，卡片执行另外的风险管理决定交易是接受还是拒绝。

7.9.1 卡片风险管理

下表总结了交易结束阶段的卡片风险管理检查，并标明这些检查是否强制或可选，同时描述了检查的结果。

表17 卡片风险管理检查

风险管理检查	执行条件	结果（如果条件满足）
连续脱机交易上限频度检查	可选－－如果上次联机 ATC 寄存器和连续脱机交易上限(Tag‘9F59’)存在，	如果限制数超过，脱机拒绝 设置 CVR 中指示位

	卡片执行此检查。	
新卡检查	可选——如果上次联机 ATC 寄存器存在，卡片执行此检查。	视 ADA 中“如果是新卡，当交易无法联机时拒绝交易”位的设置，决定脱机批准或拒绝 设置 CVR 中指示位
PIN 尝试限制数超过	可选	如果支持脱机 PIN，建议设置 ADA 中“如果 PIN 在前次交易中锁定，拒绝交易”位为 1；脱机拒绝 设置 CVR 中指示位
累计脱机交易金额（上限）频度检查	可选——如果累计脱机交易金额和累计脱机交易金额上限存在，卡片执行此检查。	如果限制数超过，脱机拒绝 设置 CVR 中指示位
累计脱机交易金额上限（双货币）频度检查	可选——如果累计脱机交易金额（双货币）和累计脱机交易金额上限存在，卡片执行此检查。	如果限制数超过，脱机拒绝 设置 CVR 中指示位

7.9.2 执行活动

实现交易结束阶段卡片风险管理所要求的活动包括：

- 策略
  - ✓ 决定是否支持卡片新卡检查；
  - ✓ 决定是否支持各项卡片频度检查；
  - ✓ 决定在交易点进行卡片风险管理检查时希望卡片采取的动作（脱机批准、脱机拒绝）。
- 业务
  - ✓ 根据实现功能，与卡片供应商交流需要支持的数据元。
  - ✓ 确定卡片的频度参数。
- 技术

  产生卡片风险管理所需数据，加入个人化输入文件。数据包括：连续脱机交易上限（Tag ‘9F59’）、累计脱机交易金额上限等。

7.10 发卡行脚本处理

发卡行脚本处理允许发卡行不用二次发卡就可以更改驻留在芯片的账户参数。这些更新帮助发卡行加强风险管理、优化客户服务。例如：锁定拖欠账户；更改频度检查计数器，对优质客户提供更好的、限制更少的使用条件，而对高风险客户收紧控制。

7.10.1 命令

发卡行需要决定支持的脚本命令。下表给出了这些命令及其定义、使用背景。

注：对二次发卡应用加载的支持，不在本文描述范围。

表18 发卡行脚本处理命令

命令	定义	使用情景
应用锁定	这个命令允许发卡行锁定一个指定的 PBOC 应用。	发卡行可以使用这个命令关闭选定应用。当获报某卡失窃或是拖欠账户时，可以使用它。这个命令可以防止欺诈账户在低于最低限额、或只可脱机环境的使用。
解锁应用	这个命令允许发卡行解锁一个指定的 PBOC 应用。	发卡行可以使用这个命令解锁 PBOC 应用。当一个欺诈账户恢复为正常时，需要用到它。仅在发卡行指定的特殊终端设备上支持此功能，如：发卡行的 ATM 或其营业网点的柜台终端。
卡片锁定	这个命令允许发卡	发卡行可以使用这个命令关闭卡内所有芯片应用。因为这个命令的作用等同于剪卡，

	行锁定整个卡片。	应该只在最严重的情景下使用此命令。 一旦卡片被锁定，将无法解锁；如果账户恢复正常，必须重新发卡。 只有当卡片已报失窃时，发卡行可以考虑使用这个命令。如果对一张多应用卡（发卡行并非唯一的应用提供商）使用此命令，发卡行应该与其它应用提供商一起制定这个命令的使用条款；另外，发卡行应该建立一个机制，当卡片被锁定时，通知其它应用提供商。
PIN 修改/解锁	这个命令允许发卡行解锁脱机 PIN 或解锁 PIN 加同时修改 PIN 值。	当超过 PIN 尝试限制数，卡片锁定脱机 PIN。对这种情形可以使用 PIN 修改/解锁命令进行补救： • 当持卡人记得 PIN、进行了正确的验证，解锁脱机 PIN 并保持原 PIN 值； • 当持卡人忘记 PIN，解锁并修改脱机 PIN 值。 如果持卡人想要换一个新 PIN，也可以使用此命令修改脱机 PIN。 仅在发卡行指定的特殊终端设备上支持此功能，如：发卡行的 ATM 或其营业网点的柜台终端。
设置数据	这个命令允许发卡行修改一些基本数据对象的值，如：与频度检查相关的数据元。	发卡行在发卡后可以使用这个命令修改频度控制参数，以便更好地定制持卡人的风险控制模型。 例如：可以增加“连续脱机交易上限”值由 3 至 5。
修改记录	这个命令允许发卡行修改文件中一条记录的内容。	当修改 PIN 时，可能需要使用这个命令修改芯片内磁条数据（“磁条 2 等效数据”和“磁条 1 自定义数据”）的 PVN 信息。

注：除了这套命令，发卡行还可以实现其它的命令，只要发卡行的卡片和主系统能够支持它。

7.10.2 安全

必须使用安全报文传送发卡行脚本。

7.10.3 需要生成的密钥数量

安全报文机制用到了两种 DES 密钥：

- 报文认证码(MAC)密钥
  这个密钥用于保护发卡行脚本处理的安全，对于任何发卡行脚本命令都必须使用。用于确认数据没有被篡改过（完整性），同时可以确认命令发出的发卡行是否是合法（发卡行认证）；MAC 主密钥(MAC MDK)存放在发卡行主系统，由其分散得到 MAC 子密钥（MAC UDK）存放在卡内。
- 数据加密(ENC)密钥
  这个密钥用来加密脚本中的敏感数据，如脱机 PIN 等。ENC 主密钥(ENC MDK)存放在发卡行主系统，由其分散得到 ENC 子密钥（ENC UDK）存放在卡内。

发卡行需要决定准备支持的 MAC MDK 和 ENC MDK 数量。与 AC MDK 类似，银联建议：发卡行对每个 BIN 支持至少一个 MAC MDK 和一个 ENC MDK。

注：对于 MAC UDK 和 ENC UDK 没有决策要求，因为他们是应用级密钥；发卡行必须为每个 PBOC 应用派生一个 MAC UDK 和一个 ENC UDK。

7.10.4 发卡行脚本处理风险管理检查

对于发卡行脚本处理结果，有两个风险管理检查：

表19 发卡行脚本处理风险管理检查

条件	推荐动作
上次交易执行发卡行脚本处理失败。	请求联机授权。

发卡行脚本处理失败（在最后的生成应用密文命令后）	继续进行交易，下一交易请求联机授权。

7.10.5 执行活动

对于发卡行脚本处理，发卡行需要作出以下决策：

- 决定准备支持的发卡行脚本命令。发卡行应将这些命令的需求与供应商充分交流，因为供应商不一定完全支持这些命令。
- 决定是否准备以后支持另外的发卡行脚本命令。

与支持发卡行脚本处理相关的 MAC 和 ENC 密钥活动包括：

表20 发卡行脚本处理 DES 密钥管理活动

步骤	责任方	活动
1	技术	生成合适数量的 MAC MDK 和 ENC MDK。
2	技术	决定关联 MAC UDK/ENC UDK 与 MAC MDK/ENC MDK 的方法。 建议：对于 MAC/ENC 密钥和 AC 密钥一样，使用同一个 DKI；或者使用 BIN 和 PBOC 应用失效日期来定位 MAC 和 ENC 密钥。
3	技术	使用 MDK 为每个 PBOC 应用派生一个 UDK，这是预个人化活动的一部分： • 使用 MAC MDK 分散得到 MAC UDK； • 使用 ENC MDK 分散得到 ENC UDK。
4	技术	将 MAC UDK、ENC UDK 和 DKI（如果适用）加入个人化输入文件。MAC UDK 和 ENC UDK 必须使用 KEK 加密后放入个人化输入文件。
5	技术	在个人化过程中，将 MAC UDK、ENC UDK、DKI（如果适用）和其它个人化数据一起加载到卡内。 加载合适的 MAC UDK、ENC UDK 和 DKI 是十分重要的；如操作有误，可能导致联机卡片认证和发卡行认证失败。

8 其它卡片要求

8.1 磁条数据

在 PBOC 迁移过程中，磁条提供的功能仍是支付服务的基础。发卡行需要在个人化磁条数据至芯片内。

8.1.1 PBOC 应用与磁条的关系

为了适应受理环境，银联要求 PBOC 卡应继续保留物理磁条。发卡行应将与磁条信息相对应的 PBOC 借贷记应用设置为最高优先级，称为首要借贷记应用。需要注意物理磁条数据与首要借贷记应用数据的一致性：

- PBOC 卡内首要借贷记应用的失效日期应与物理磁条内的失效日期一致。
- 如果 PBOC 卡卡片正面印制了有效期，则芯片卡内首要借贷记应用的失效日期以及物理磁条内的失效日期应与卡片正面的有效期一致。
- PBOC 卡芯片信息内的持卡人姓名必须和卡面上印制的持卡人姓名一致。
- PBOC 卡物理磁条的服务代码设定为“2XX”或“6XX”；第二磁道中主账号、有效期、服务代码等信息应体现在芯片内首要借贷记应用中的相关数据元中。
- 为了更好的控制风险，发卡行可以选择让存储在芯片内的 iCVN 不同于物理磁条中的 CVN。

8.1.2 IC 卡片验证码

除了现有的对物理磁条进行卡片验证码(CVN)检查，银联对 PBOC 交易推荐备选的 IC 卡片验证码(iCVN)检查；它的作用是防止利用芯片内磁条数据伪造磁条卡。物理磁条内的 CVN 与芯片内的 iCVN 值是不同的。

iCVN 与 CVN 使用同样的计算方法，除了用”999”替换真正的服务代码，其它计算要素：DES 密钥、主账号、失效日期仍保持不变。如果发卡行原来就支持 CVN 生成和验证，那么支持新的 iCVN 对于系

统造成的影响很小。可以通过以下方法决定使用 CVN 或 iCVN：

- 如果 PAN 输入方式为 90，表示磁条发起交易，进行传统的 CVN 验证。
- 如果 PAN 输入方式为 05，表示芯片发起交易，用”999”替换服务代码进行 iCVN 验证。

如果一笔磁条发起交易收到的是 iCVN，CVN 验证将失败；这将导致发卡行（或代理）拒绝这笔交易。这种检查有助于揭示伪卡、可疑商户等问题。

8.1.3 执行活动

与磁条数据相关的活动包括：

- 策略
  - ✓ 决定 PBOC 应用与磁条的关系。
  - ✓ 决定是否支持 iCVN。
- 业务
  - ✓ 确保个人化的芯片内磁条数据与物理磁条的编码数据、以及卡面印制数据的一致性。
  - ✓ 与供应商交流 CVN/iCVN 处理需求。
- 技术
  - ✓ 生成物理磁条的等效数据加入个人化输入文件。
  - ✓ 如果支持 iCVN，使用”999”替换服务代码计算获得 iCVN；修改发卡行主系统以支持 iCVN 验证。

8.2 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。

8.2.1 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，其中卡片数据详见下表：

表21 电子现金专有数据元

数据元名称	要求	描述
电子现金余额 （Electronic Cash Blance）	条件 如果支持 EC	该数据元保存了可供脱机消费的剩余总额，对于每一笔成功的电子现金交易，从中减去相应的交易额。一旦交易额超过了电子现金余额，则所有交易必须通过联机授权。
电子现金余额上限 （Electronic Cash Blance Limit）	条件 如果支持 EC	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。发卡行可修改此上限值。
电子现金发卡行授权码 （EC Issuer Authorization Code）	条件 如果支持 EC	卡片上用于标识批准电子现金交易的代码。在脱机批准交易中，该代码被存放在清算报文的授权码。格式为“ECCxxx”，其中 xxx 是发卡行定义的编号。
电子现金单笔交易限额 （EC Single Transaction Limit）	可选	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。在个人化时由发卡行写入，并可由发卡行重新设置。

电子现金重置阈值 （EC Reset Threshold）	可选	触发卡片进行自动充值的可用余额下限。当卡片上的脱机可用余额低于该阈值时，卡片即请求联机并自动进行充值。

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：PDOL、应用货币代码；有些数据元可以设置区别于标准 PBOC 的值，供 EC 交易单独使用，如：AFL、AIP 等。这些受电子现金影响的数据元详见下表：

表22　电子现金影响数据元

数据元名称	要求	描述
处理选项数据对象列表（PDOL）	条件 如果支持 EC	如果支持 EC 功能，卡片必须设置 PDOL 数据元，其至少应要求终端提供以下数据元：电子现金终端支持指示器、授权金额以及交易货币代码。
应用货币代码	条件 如果支持 EC	PBOC 专有数据。根据 ISO4217 编码。EC 交易要求应用货币代码与交易货币代码相匹配。
应用文件定位器（AFL）	条件 如果支持 EC	对于 EC 交易，指出和 EC 应用相关的数据存放位置(短文件标识符和记录号)。其指向的文件记录应该包含电子现金余额、电子现金发卡行授权码等 EC 专有数据。它还可以指定其它记录以使用与非 EC 交易不同的数据，如：CVM 列表。
应用交互特征（AIP）	条件 见描述	用于 EC 交易的 AIP，说明针对 EC 卡片支持指定功能的能力。发卡行可以选择区别于非 EC 交易的功能。
持卡人验证方法(CVM)列表	条件 见描述	如果发卡行希望对于 EC 交易执行不同于非 EC 交易的持卡人验证方法，就需要个人化单独的 CVM 列表。
IC卡公钥证书	条件 见描述	如果对于 EC 交易支持 DDA、并且其签名数据与非 EC 交易有所不同，就需求个人化单独的 IC 卡公钥证书。
发卡行行为代码（IAC）	条件 见描述	如果发卡行对于 EC 交易的 IAC-拒绝/联机/缺省的设置条件与非 EC 交易有所不同，就需要个人化单独的 IAC。
签名的静态应用数据（SAD）	条件 见描述	如果对于 EC 交易支持 SDA，并且签名数据与非 EC 交易有所不同，就需要个人化单独的 SAD。

8.2.2　风险管理

与对于大额交易持续加强风险控制不同，基于电子现金的小额特性以及快速处理的要求，发卡行对于 EC 可以灵活地实现一个简化的风险控制功能。EC 风险控制功能可以相对独立于标准 PBOC。例如：支持不同的脱机数据认证方法、不同的持卡人验证方法。

8.2.3　执行活动

实现 EC 功能需要执行以下活动：

- 策略
  - ✓ 发卡行决定是否实现 EC 功能；
  - ✓ 定义卡片为电子现金发卡行授权码－“ECCxxx”生成唯一编号的方法，例如：可以是随机产生或象 ATC 一样顺序产生的数字；
  - ✓ 决定对于 EC 交易是否使用数据元“电子现金单笔交易限额”；
  - ✓ 决定对于 EC 交易是否使用数据元“电子现金重置阈值”；
  - ✓ 决定对于 EC 交易采用的风险管理方法，如：脱机数据认证方法、持卡人验证方法。

- 业务
  - ✓ 与卡片供应商交流对于 EC 的要求；
  - ✓ 根据持卡人的风险记录、账户状态等情况，定义其电子现金余额上限；
  - ✓ 设置电子现金单笔交易限额、电子现金重置阈值（如果支持）。
- 技术

  产生电子现金功能所需数据，加入个人化输入文件。数据包括：电子现金余额上限、电子现金单笔交易限额、电子现金重置阈值等。

8.3 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。

8.3.1 通用要求概述

非接触式支付对于卡片的基本要求包括：

- 卡片应同时支持 qPBOC 和 MSD；
- 卡片应最少支持 ISO 14443 协议定义的 Type A 或 Type B 的一种；
- 如果接触式界面被激活，卡片不宜响应非接触式界面；
- “磁条 2 等效数据”对于 MSD、qPBOC 是强制的；
- 具有脱机能力的卡片 (qPBOC) 应支持 SDA 或 DDA（建议支持 DDA）；
- 为了用目前的芯片满足时间要求，推荐卡片密钥采用中国余数定理模式。

8.3.2 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：

1. 把多条EMV命令压缩成尽可能少的命令，以减少交易的时间；

2. 将卡片和终端的交互过程集中完成，当卡片离开读卡器的通讯范围后，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，使卡片在读卡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。

8.3.2.1 要求概述

除了所有非接触程序的卡片需求外，qPBOC 还应当遵守下面的要求：

- 一收到 GPO 命令，卡片应当立即设置发卡行应用数据的 CVR 部分为’03000000’。

  CVR 位于发卡行应用数据的第 4—7 字节：
  - ✓ CVR 字节 2，位 8、7、4、3、2、1 未使用，仍保留设置为 0。
  - ✓ CVR 字节 3，位 8、4、3、2、1 未使用，仍保留设置为 0。
  - ✓ CVR 字节 4 未使用，所有位仍保留设置为 0。
- 卡片应当在计算密文和动态签名之前增加 ATC 的值。
- 如果卡片的脱机消费可用余额（Tag ‘9F5D’）被个人化为 1，则卡片应当允许读取该数据元素。

卡片的行为应当在个人化时指明并存储在内部卡片指示器中。

- 如果授权金额为 0，卡片应当请求联机处理。
- 对于联机或拒绝交易，卡片应当在 GPO 响应中返回应用密文 ARQC/AAC，以及规定的其它数据元。
- 对于脱机交易，卡片应当在 GPO 响应中返回应用密文 TC，以及规定的其它数据元。
- 如果 ICC 密钥长度小于等于 1024 位，应当生成动态签名并在 GPO 响应中返回。
- 如果 ICC 密钥长度大于 1024 位，卡片应当在 GPO 时生成动态签名并在 READ RECORD 命令中返回。

  注：如果 ICC 密钥长度大于 1024 位，GPO 响应中没有足够空间返回动态签名。
- 为了确保 GPO 响应能成功传送给读卡器，对于 ICC 密钥等于 1024 位的情形，AFL 包含的分支不应当超过 4 个。

  注：如果 ICC 密钥长度更短，可能会有足够空间包含更多的分支。如果 ICC 密钥长度更长，签名在记录中传送，也会有足够空间传送更大的 AFL。

8.3.2.2 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。在 qPBOC 处理中，PBOC 计数器和指示器，以及其它本文档中未涉及到的变量，不会受到影响。以下对 qPBOC 卡片新增数据元以及受 qPBOC 影响数据元分别予以说明：

表23 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）	强制	可以通过非接触界面访问的应用所支持的应用标识、应用标签和应用优先指示器的一个列表，该列表包括所有目录的入口，由卡片在 SELECT PPSE ('2PAY.SYS.DDF01')响应的 FCI 中返回。
脱机消费可用余额 （Available Offline Spending Amount）	可选	一个计算域，用来允许读写器打印或显示卡片的离线交易额度。 除非此标签被个人化为'1'，否则卡片将不会允许此标签被包括在可被读写器读出的记录中或对 GPO 的响应中。 对于此数据元的个人化并不影响它包含在发卡行自定义数据中。
卡片附加处理 （Card Additional Processes）	条件 如果支持脱机并且小额选项不是缺省 EC 或没有卡片风险管理选项被支持。	指出卡片处理需求和参数选择。 详细描述参见 8.1.3.1 节。
卡片持卡人验证方法限额 （Card CVM Limit）	可选	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 （Card Internal Indicators）	强制	用于控制 qPBOC 卡片内部过程。
卡片交易属性 （Card Transaction Qualifiers）	可选	主要用于向终端指明卡片要求的 CVM。

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。相关电子现金数据元参见“表 21－电子现金专有数据元”。

表24　qPBOC 影响数据元

数据元名称	要求	描述
处理选项数据对象列表（PDOL）	强制	qPBOC 卡片必须设置 PDOL 数据元，根据支持的密文版本类型（01 或 17）、是否支持脱机的情况，PDOL 会要求不同的基本终端数据元。
应用货币代码	条件 如果支持卡片附加处理	PBOC 专有数据。根据 ISO4217 编码。qPBOC 卡片附加处理要求货币匹配检查。
应用文件定位器（AFL）	需要	对于 qPBOC 交易，指出和 qPBOC 应用相关的数据存放位置（短文件标识符和记录号）。当卡片请求联机处理或拒绝时，不会返回 AFL；只有当卡片脱机批准时，才会返回一个指示脱机数据认证要求数据的 AFL。
应用交互特征（AIP）	强制	用于 qPBOC 交易的 AIP，说明针对 qPBOC 卡片支持指定功能的能力。发卡行可以选择区别于标准 PBOC 交易的功能。 注：非接触规范新定义了 AIP 字节 2—位 8“支持 MSD”。
发卡行应用数据	需要	如果卡片支持返回脱机消费可用余额，将通过发卡行应用数据的发卡行自定义数据部分返回对应的值；发卡行据此监控脱机资金风险。
IC卡公钥证书	条件 见描述	如果 qPBOC 应用支持 fDDA、并且其签名数据与标准 PBOC 应用有所不同，就需求个人化单独的 IC 卡公钥证书。
签名的静态应用数据（SAD）	条件 见描述	如果 qPBOC 应用支持 SDA，并且签名数据与标准 PBOC 应用有所不同，就需要个人化单独的 SAD。

8.3.2.3　应用选择

对于非接触应用的选择使用近距离支付系统环境(PPSE)目录选择方法。针对非接触应用选择，卡片个人化应注意：

- 使用文件名“2PAY.SYS.DDF01”将 PPSE 个人化到所有的非接触卡片中。
- 在具有 PBOC AID 的单个卡片应用中，同时支持 MSD 和 qPBOC 路径。
- 如果一个以上的应用被个人化到 FCI 中，则应用优先指示器应被个人化到所有的应用中；应用优先指示器 Bits 8-5 应设为“0000”。
- 卡片中的非接触金融应用的 AID，应在 SELECT PPSE 命令响应的 FCI 中返回。
- 所有 PBOC 非接触应用的个人化都应存在 PDOL，该 PDOL 至少要包含数据元“终端交易属性”（Tag ‘9F66’）。

8.3.2.3.1　处理选项数据对象列表

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。

卡片请求终端交易属性以便非接触应用能决定使用哪个卡片路径（MSD 或 qPBOC）。不可预知数，授权金额，与卡片的 ATC 一起，用于计算密文（01 或 17 版本）。不可预知数和 ATC 也用于在脱机交易中计算动态签名。

一个卡片应用包含单一的 PDOL，PDOL 包含了与所有路径（MSD，qPBOC 以及 PBOC）相关的 Tag，也

可以包含规范未描述的 Tag 来作为最低需求。发卡行应当在使用 PDOL 请求附加数据带来的好处，和附加数据传输和处理对交易性能带来的影响之间权衡利弊。

qPBOC 中的 PDOL 最基本内容依赖于支持的密文类型（01 或 17），以及卡片是否支持脱机 qPBOC 交易。

表25　应用 17 密文、仅联机 qPBOC 的最基本 PDOL 内容

PDOL 中的 Tag	数据元名称
9F66	终端交易属性
9F02	授权金额
9F37	不可预知数

注：如果支持卡片附加处理，则交易货币代码（Tag '5F2A'）也应该包含在 PDOL 中。

表26　应用 17 密文、联机/脱机 qPBOC 的最基本 PDOL 内容

PDOL 中的 Tag	数据元名称
9F66	终端交易属性
9F02	授权金额
9F37	不可预知数
5F2A	交易货币代码

表27　应用 01 密文、联机/脱机 qPBOC 的最基本 PDOL 内容

PDOL 中的 Tag	数据元名称
9F66	终端交易属性
9F02	授权金额
9F03	其它金额
9F1A	终端国家代码
95	终端验证结果（TVR） 注：TVR 会被 qPBOC 终端填为 0。
5F2A	交易货币代码
9A	交易日期
9C	交易类型

8.3.2.3.2　执行活动

与 qPBOC 应用选择相关的活动包括：

- 策略
  - ✓ 决定支持的非接触应用个数；
    银联推荐：如果可能，在 FCI 中只列出一个应用。否则，应用的数量也应尽可能少。
  - ✓ 决定采用的密文版本（01 或 17）。
- 业务
  - ✓ 根据实现功能，与卡片供应商交流需要支持的数据元；
  - ✓ 如果 PPSE 包含多个非接触应用，使用应用优先指示器设置其优先级；
  - ✓ 根据采用的密文版本、卡片联机/脱机能力以及发卡行自定义的需求，决定 PDOL 内容。
- 技术

  产生应用选择所需数据，加入个人化输入文件。数据包括：PPSE、应用优先指示器、PDOL 等。

8.3.2.4　应用初始化

为进一步减少交易时间，qPBOC 将以下风险管理特征移到了交易的更早阶段－应用初始化阶段：

1. 卡片风险管理
2. 联机卡片认证
3. 脱机数据认证
4. 交易证书

在联机交易中，仅使用 GET PROCESSING OPTIONS 命令。在脱机交易中，还会使用 READ RECORD 命令读取 SDA 或 fDDA 相关数据，而验证签名（静态或动态）步骤是在卡片离开感应区之后完成。

8.3.2.4.1 卡片风险管理

qPBOC 卡片的风险管理主要是通过卡片附加处理(Tag '9F68')个人化一系列的需求来控制。

表28 卡片附加处理

条件	描述	推荐动作
支持小额检查	该条件表示 qPBOC 卡片只使用 EC 的脱机授权额度(以下简称：EC 额度)进行小额支付的判断。 支持该选项，qPBOC 交易只会使用 EC 额度，不会影响 CTTA 额度。	这种模式不管在标准 PBOC 中设置 CTTA 额度与否，在 qPBOC 交易中只使用 EC 额度；额度控制简单有效，一般建议采用。
支持小额和 CTTA 检查	支持该选项，qPBOC 交易使用 EC 额度，CTTA 额度会发生相应变化。 在这种情况下，EC 额度是 CTTA 额度的一部分（EC 额度<=CTTA 额度）	这种模式两个额度相互关联，同步控制比较复杂，一般不建议采用。
支持小额或 CTTA 检查	支持该选项，qPBOC 首先考虑使用 EC 额度，如 EC 额度不足，转而使用 CTTA 额度。 在这种情况下，EC 额度和 CTTA 额度为两个相互独立的脱机额度。	这种模式实现的复杂程度介于上述两者之间，发卡行应根据卡产品特性、对主系统影响程度等因素综合考虑是否需要采用。
支持新卡检查	如果支持此检查，当判断上次联机 ATC 寄存器为 0 时，卡片请求联机处理。	建议支持。
支持 PIN 尝试次数超限检查	如果支持此检查，当判断 PIN 尝试次数计数器存在并等于 0 时，卡片请求联机处理、或脱机拒绝（如果终端仅脱机）。	建议支持。
允许不匹配货币的脱机交易	设置是否允许不匹配货币的 qPBOC 脱机交易。	发卡行根据卡产品特性、使用范围，决定是否允许。
优先选择接触式 PBOC 联机	在请求联机的情况下，决定是否优先选择接触式 PBOC，按照标准 PBOC 的完整流程进行交易。	发卡行根据卡产品特性、风险策略，决定是否支持。
返回脱机消费可用余额	设置该选项要求联机返回 qPBOC 卡片当前总的脱机授权额度，以便更好地监控资金风险。	发卡行根据卡产品特性、风险策略，决定是否支持。
支持预付	这是针对预付卡的一个检查条件。这种卡在后台没有主账户与电子现金账户之分，不管是联机或脱机完成交易，都需要更新卡内资金余额。	一般正常的借记/贷记产品实现电子现金功能不用考虑这个条件。
不允许不匹配货币的交易	设置是否不允许不匹配货币的 qPBOC	发卡行根据卡产品特性、使用范围，决

	交易。	定是否允许。
如果是新卡且终端仅支持脱机，拒绝交易	如果支持该条件，当判断上次联机 ATC 寄存器为 0 时，卡片脱机拒绝。	发卡行根据卡产品特性、风险策略，决定是否允许。
匹配货币的交易支持联机 PIN	设置对于匹配货币的 qPBOC 交易是否支持 CVM－联机 PIN。	发卡行可以根据（贷记）卡产品特性、风险策略决定对于匹配货币的交易是否支持，也可以根据持卡人的选择来设置。
不匹配货币的交易支持联机 PIN	设置对于不匹配货币的 qPBOC 交易是否支持 CVM－联机 PIN。	发卡行可以根据（贷记）卡产品特性、风险策略决定对于匹配货币的交易是否支持，也可以根据持卡人的选择来设置。
对于不匹配货币交易，卡片要求 CVM	设置对于不匹配货币的 qPBOC 交易是否要求进行持卡人验证。	发卡行根据卡产品特性、风险策略，决定是否允许。
支持签名	设置对于 qPBOC 交易是否支持 CVM－签名。	建议支持。

下表总结了 qPBOC 交易在应用初始化阶段所有的卡片风险管理检查，并标明这些检查的执行条件，同时描述了检查的结果。

表29　qPBOC 卡片风险管理检查

风险管理步骤	检查项	执行条件	结果（如果条件满足）
设置货币匹配标记	货币匹配检查	如果卡片附加处理的“不允许不匹配货币交易”位为 1，此检查生效。	如果卡片内部指示器的“匹配货币”位为 0、并且卡片附加处理的“不允许不匹配货币交易”位为 1，脱机拒绝
终端仅支持脱机	脱机检查	如果卡片附加处理的“如果是新卡且终端仅支持脱机，拒绝交易”位为 1，此检查生效。	如果上次联机 ATC 寄存器为 0、并且卡片附加处理的“如果是新卡且终端仅支持脱机，拒绝交易”位为 1，脱机拒绝
	PIN 尝试限制数超过检查	如果卡片附加处理的“支持 PIN 尝试次数超限检查”位为 1，此检查生效。	如果 PIN 尝试次数计数器存在并等于 0，脱机拒绝 设置 CVR 中指示位
	要求 CVM 检查	如果卡片附加处理的“对于不匹配货币交易，卡片要求 CVM”位为 1，此检查生效。 在检查中用到卡片附加处理的“支持签名”位。	如果卡片和终端都支持签名，继续尝试脱机处理； 如果卡片和终端至少一个不支持签名，中止非接触交易。
终端或卡片要求 CVM	无需 CVM 检查	如果数据元“卡片 CVM 限额”存在；或卡片附加处理的“对于不匹配货币交易，卡片要求 CVM”位为 0，此检查生效。	在终端和卡片都不要求 CVM 的情况下，继续下一步骤“检查联机处理请求”。

	要求 CVM 检查	如果数据元“卡片 CVM 限额”存在；或卡片附加处理的“对于不匹配货币交易，卡片要求 CVM”位为 0，此检查生效。 在检查中用到卡片附加处理的“匹配货币的交易支持联机 PIN”、“不匹配货币的交易支持联机 PIN”、“支持签名”位。	在终端或卡片要求 CVM 的情况下，如果两者均支持联机 PIN，卡片请求联机处理；如果两者均支持签名，继续下一步骤“检查联机处理请求”。
检查联机处理请求	终端请求联机检查	无需卡片数据引发此检查。	卡片也要请求联机处理，跳至“完成联机交易”步骤。
	不匹配货币的脱机交易检查	如果卡片附加处理的“允许不匹配货币的脱机交易”位为 0，此检查生效。	如果货币不匹配，卡片请求联机处理。
	新卡检查	如果卡片附加处理的“支持新卡检查”位为 1，此检查生效。	如果上次联机 ATC 寄存器为 0，卡片请求联机处理。 设置 CVR 中指示位
	PIN 尝试限制数超过检查	如果卡片附加处理的“支持 PIN 尝试次数超限检查”位为 1，此检查生效。	如果PIN尝试次数计数器存在并等于 0，卡片请求联机处理。 设置 CVR 中指示位
脱机货币检查	脱机货币检查	在检查中用到卡片附加处理的“支持小额检查”、“支持小额和 CTTA 检查”、“支持小额或 CTTA 检查”位。	如果货币不匹配，跳至“脱机不匹配货币”步骤； 如果货币匹配，却不支持任何一种脱机消费检查，对于仅脱机终端拒绝交易，对于可联机终端请求联机处理。
小额检查	终端可联机－EC 单笔限额检查	如果数据元“电子现金单笔交易限额”存在，此检查生效。	如果授权金额大于电子现金单笔交易限额，卡片请求联机处理。 设置 CVR 中指示位
	终端可联机－EC 重置阈值检查	如果数据元“电子现金重置阈值”存在，此检查生效。	如果授权金额大于（电子现金余额－电子现金重置阈值），卡片请求联机处理。 设置 CVR 中指示位
	终端仅脱机－小额检查	在检查中用到数据元“电子现金余额”、“电子现金单笔交易限额”（如果存在）。	如果授权金额大于电子现金余额、或大于电子现金单笔交易限额（如果存在），拒绝交易。 设置 CVR 中指示位
小额和 CTTA 检查	终端可联机－EC 单笔限额检查	如果数据元“电子现金单笔交易限额”存在，此检查生效。	如果授权金额大于电子现金单笔交易限额，卡片请求联机处理。 设置 CVR 中指示位
	终端可联机－EC 重置阈值检查	如果数据元“电子现金重置阈值”存在，此检查生效。	如果授权金额大于（电子现金余额－电子现金重置阈值），卡片请求联机处理。 设置 CVR 中指示位

	终端可联机－CTTA 检查	在检查中用到数据元 CTTA、CTTAUL（如果存在，否则使用 CTTAL）。	如果授权金额大于（CTTAUL－CTTA），卡片请求联机处理。 设置 CVR 中指示位
	终端仅脱机－小额和 CTTA 检查	在检查中用到数据元“电子现金余额”、“电子现金单笔交易限额”（如果存在）、CTTA、CTTAUL（如果存在，否则使用 CTTAL）。	如果授权金额大于电子现金余额、或大于电子现金单笔交易限额（如果存在）、或大于（CTTAUL－CTTA），拒绝交易。 设置 CVR 中指示位
小额或 CTTA 检查	终端可联机－单笔限额检查	如果数据元“电子现金单笔交易限额”存在，此检查生效。	如果授权金额大于电子现金单笔交易限额，卡片请求联机处理。 设置 CVR 中指示位
	终端可联机－CTTA 检查	在检查中用到数据元“电子现金余额”、CTTA、CTTAUL（如果存在，否则使用 CTTAL）。	如果授权金额大于电子现金余额、并且大于（CTTAUL-CTTA），卡片请求联机处理。 设置 CVR 中指示位
	终端仅脱机－小额或 CTTA 检查	在检查中用到数据元“电子现金余额”、“电子现金单笔交易限额”（如果存在）、CTTA、CTTAUL（如果存在，否则使用 CTTAL）。	如果授权金额大于电子现金单笔交易限额（如果存在）、或者（授权金额大于电子现金余额、并且大于（CTTAUL-CTTA）），拒绝交易。 设置 CVR 中指示位
脱机下的货币不匹配	国际－货币频度检查	如果连续脱机交易计数器（国际-货币）、连续脱机交易限制数（国际-货币）存在，此检查生效。	如果不超过限制数，卡片脱机批准；如果超过限制数且终端可联机，卡片请求联机；否则，脱机拒绝。 设置 CVR 中指示位。
完成联机交易	优先选择接触式检查	如果卡片附加处理的“支持优先选择接触式 PBOC 联机”位为 1，此检查生效。	如果终端也支持接触式 PBOC，卡片请求中止交易。
	小额和 CTTA 预付检查	如果卡片附加处理的“支持预付”位为 1、“支持小额和 CTTA 检查”为 1，此检查生效。	如果资金不足，卡片拒绝交易； 如果资金足够，卡片请求联机，更新电子现金余额、CTTA。
	小额预付检查	如果卡片附加处理的“支持预付”位为 1、“支持小额检查”为 1，此检查生效。	如果资金不足，卡片拒绝交易； 如果资金足够，卡片请求联机，更新电子现金余额。

注：在整个 qPBOC 卡片风险管理检查过程中，只要卡片请求联机处理，都会用到卡片附加处理的“返回脱机消费可用余额”、“支持小额检查”、“支持小额和 CTTA 检查”、“支持小额或 CTTA 检查”位，判断是否需要计算脱机消费可用余额，以及计算方式。

8.3.2.4.2 执行活动

与 qPBOC 应用初始化相关的活动包括：

- 策略
  - ✓ 决定是否使用脱机消费可用额度、卡片 CVM 限额和卡片交易属性；
    由于这些数据元给予发卡行对 qPBOC 卡片更强的风险控制，银联建议在卡内使用这些数据元。
  - ✓ 决定支持何种脱机数据认证方法。

非接触规范要求 qPBOC 卡片支持 SDA 或 fDDA，银联建议支持 fDDA。

- ✓ 决定需要签名的数据项。
  一般情况下，qPBOC 卡片同时也支持标准（接触式）PBOC，如果 qPBOC 的签名数据与标准 PBOC 不同，就要支持两个 SAD 或两个 IC 卡公钥证书，这将增加实现的复杂度。
  银联建议：如果卡片同时支持 qPBOC 和标准 PBOC，对 qPBOC 使用与标准 PBOC 一样的签名数据。

- 业务
  - ✓ 根据实现功能，与卡片供应商交流需要支持的数据元；
  - ✓ 确定卡片附加处理的各项风险参数值；
  - ✓ 设置卡片 CVM 限额、卡片交易属性相关参数（如果支持）。
- 技术
  产生应用初始化所需数据，加入个人化输入文件。数据包括：卡片附加处理、脱机消费可用额度、卡片 CVM 限额、卡片交易属性等。

8.3.3 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，发卡行如需了解 MSD 的详细信息，请联系银联代表。

9 发卡行主系统改造

本章整体描述了 PBOC 迁移所要求的发卡行主系统改造事项。帮助发卡行决定是以“完全支持”(Full 选项）或“部分支持”（Early 选项）方式实现 PBOC 迁移计划。

9.1 新增数据

本节针对 Early 状态和 Full 状态，集中介绍授权类、金融类以及清算类交易所要求的新增芯片数据。

9.1.1 Early 选项

Early 选项要求的系统改造是最小限度的。发卡行主系统必须对授权类、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。

实现 Early 选项，发卡行主系统改造所要求的活动如下：

技术

技术人员应该评估实现 Early 选项对主系统会造成怎样的影响，以及技术支持模式：由内部开发、或由主系统厂商负责改造、或依靠第三方处理商。最终决定是由发卡行自己进行改造、还是与主系统厂商或第三方处理商合作进行改造。

由于涉及的改动很小，银联不要求实现 Early 选项的发卡行进行主机认证。发卡行在开发完成后应该测试系统，以确保能够正确处理 PBOC 交易。

9.1.2 Full 选项

Full 选项涉及的系统改造范围要比 Early 选项广泛的多，但它能够带来更深远的影响、更大的价值，包括：防止伪造数据、简化争议处理等。

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。

发卡行还需要对后台系统进行改造，例如：持卡人对账单、报表等。更多信息请参见“发卡行后台系统改造”。

Early 选项要求的全部数据也是实现 Full 选项同时要求的。其它要求的新增数据在下表进行描述：

表30　新增 PBOC 数据元

域名	描述	转接系统（域/Tag）	文件系统（段/位移）
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 功能处理结果的一组指示位。例如：脱机数据认证结果。	55－95	段 2，30-39
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
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）。

实现 Full 选项，进行发卡行主系统改造所要求的活动如下：

技术

技术人员应该评估实现 Full 选项对主系统会造成怎样的影响，以及技术实现模式：由内部开发、或由主系统厂商负责改造、或依靠第三方处理商。

- 内部开发

  因为发卡行实现 Full 选项涉及的改造范围更加广泛，有必要启动一个正式的项目。发卡行应该首先组建一个跨部门的团队，集合每个技术领域的骨干，指派一个项目经理负责协调、管理这个项目计划。和所有正式项目一样，项目计划、定期会议、会议纪要、发布清单等作为成果是必须的；商务需求、技术需求和设计文档，还有测试与质量控制过程也是需要的。
- 主系统供应商

  大多数发卡行选择主系统供应商客户化其软件，以满足独特的要求。银联建议：发卡行应该在客户化完成后彻底地进行系统测试。
- 第三方处理商

  发卡行使用第三方处理商的系统，也需要测试其整体实现功能。

发卡行应该在开发完成之后测试其系统，以确保交易的正确处理。

不管采用哪种模式，实现 Full 选项的发卡行都必须执行银联要求的集成测试和联机测试。

9.1.3 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 卡片，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。

9.1.4 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。

9.2 联机卡片认证

本节描述了对于发卡行实现联机卡片认证，主系统需要进行的改造。

9.2.1 概要

当卡片和终端共同决定一笔交易上送联机，芯片会生成一个授权请求密文(ARQC)。芯片将相关卡片、终端和交易数据按特定算法组合起来，然后使用应用密文过程密钥(AC SESK) 、对称密钥算法生成 ARQC。这个密文对每个交易是唯一的。

注：AC SESK 是由存放在卡片安全区内的应用密文子密钥(AC UDK)生成的。

芯片卡将 ARQC 及相关数据传给终端，终端将 ARQC 以及生成这个密文所用到的原始数据传给收单行，这些数据包括脱机风险管理（处理限制、脱机 PIN、脱机数据认证）的结果。收单行将 ARQC 按格式放入请求报文、通过联机网络转发给发卡行；发卡行使用 HSM 验证这个密文，将验证结果用于授权决定。发卡行也可以选择 CUPS 代为验证。

本节描述发卡行在自己的系统内实现联机卡片认证，需要执行的活动。如果发卡行希望 CUPS 代为验证 ARQC，请参见“CUPS 卡片认证服务”。

9.2.2 先决条件

联机卡片认证的先决条件包括：

- 发卡行必须设置卡片支持联机卡片认证。
- 发卡行系统必须升级，以支持 Full 选项。
- 受理此类交易的收单行必须支持 Full 选项。如果收单行处于 Early 状态，其请求报文不会提供联机卡片认证所要求的数据；因而发卡行或银联都不能执行联机卡片认证。

为了支持联机卡片认证而准备系统环境，必须：

- 将应用密文主密钥(AC MDK)和对应的分散密钥索引(DKI)装载到发卡行主系统中。
- 支持双倍长密钥。
- 升级发卡行主系统，支持 ARQC 验证。

注：ZCMK 和 MDK 必须是双倍长的。

9.2.3 执行活动

下表列示了有关实现联机卡片认证的技术活动：

表31 联机卡片认证执行活动

步骤	责任方	活动
1	技术	收到一个交易请求报文时，发卡行应该将验证 ARQC 所要求数据发给 HSM，这些数据包括： • ARQC；

		• 生成 ARQC 要求数据； • 用于定位合适的 MDK 和派生 UDK 的信息（DKI、PAN、卡片序列号）。
2	技术	HSM 使用 DKI 定位 MDK。
3	技术	找到 MDK，HSM 使用 MDK 结合 PAN 和卡片序列号分散得到 UDK。
4	技术	HSM 使用 UDK 结合应用交易序号分散得到 SESK。
5	技术	HSM 结合 SESK 和生成 ARQC 要求数据，使用对称密钥算法生成一个 ARQC。
6	技术	HSM 将其生成的 ARQC 与卡片生成的 ARQC 进行比较，如果两者匹配，表示联机卡片认证成功；反之，则表示联机卡片认证失败。
7	技术	主系统记录联机卡片认证的结果。
8	技术	主系统将联机卡片认证结果用于联机授权决定。

9.3 联机发卡行认证

本节描述了对于发卡行实现联机发卡行认证，主系统需要进行的改造。

9.3.1 概要

为了保护发卡行授权响应，确保这个响应是来自于真实的发卡行，发卡行可以发送一个“联机发卡行认证”的密文给卡片，这个密文称为授权响应密文(ARPC)。用于生成 ARQC 的数据包括：ARQC 和发卡行授权响应。

发卡行在响应报文中包含 ARPC，终端将其转发给卡片，卡片使用存放在卡内的 UDK 验证 ARPC。ARPC 的验证结果将影响最后的交易部署，例如：如果 ARPC 验证失败，卡片可以推翻发卡行（或代理）的批准授权响应，拒绝交易。则可以防止在授权处理中，由未经授权方批准交易。

卡片会设置、保存联机发卡行认证结果，发卡行能够在清分交易或下次联机授权请求中读取这个指示器。

本节描述发卡行在自己的系统内实现联机发卡行认证，需要执行的活动。如果发卡行希望 CUPS 代为生成 ARPC，请参见“CUPS 发卡行认证服务”。

9.3.2 先决条件

联机发卡行认证的先决条件包括：

- 发卡行必须设置卡片支持联机发卡行认证。
- 发卡行系统必须升级，以支持 Full 选项。
- 受理此类交易的收单行必须支持 Full 选项。如果收单行处于 Early 状态，其授权报文不会提供联机发卡行认证所要求的数据；因而发卡行或银联都不能执行联机发卡行认证。

为了支持联机发卡行认证而准备系统环境，必须：

- 将应用密文主密钥(AC MDK)和对应的分散密钥索引(DKI)装载到发卡行主系统中。
- 支持双倍长密钥。
- 升级发卡行主系统，支持 ARPC 验证。

9.4 CUPS 代校验服务

使用 CUPS 代校验服务，发卡行只需设置卡片支持联机卡片认证和发卡行认证而不用相应改造主系统，就可以获得这些安全认证所提供的防止欺诈、数据复制等益处。

如果需要银联提供 CUPS 代校验服务，发卡行必须与银联签订相关协议、并将其 MDK 共享给 CUPS。

9.4.1 CUPS 卡片认证服务

在代校验过程中，CUPS 从 Full 状态收单行的请求报文中获得新增数据，对 ARQC 进行验证，并将校验结果传递给发卡行、或使用这个结果进行代授权。

如果发卡行签订了此项服务，将在交易请求报文中收到“ARQC 认证结果值”。至于该笔交易是批准还是拒绝由发卡行做最终决定，CUPS 不对交易结果做判断。

9.4.2 CUPS 发卡行认证服务

在代校验过程中，CUPS 代替发卡行计算生成一个 ARPC，通过响应报文传递给卡片。卡片使用这

个密文来验证与之通讯的发卡行是否真实有效（在这种情况下，是发卡行的代理－银联）。

9.4.3 执行活动

CUPS 代校验服务涉及的活动包括：

- 策略

  发卡行决定是否使用 CUPS 代校验服务。代校验服务对于 Full 状态发卡行是可选的，对于 Early 状态发卡行是必须的。

  Full 状态发卡行应该考虑为由银联代授权的交易签订代校验服务；如果发卡行系统不支持认证服务，应该为所有交易签订代校验服务。

- 业务

  为了实施 CUPS 代校验服务，银联需要知道发卡行的 MDK。有两种实现方法：

  ✓ 发卡行将它的 MDK 通过地区控制主密钥(ZCMK)加密后传送给 CUPS。

  ✓ 由 CUPS 为发卡行生成 MDK，通过 ZCMK 加密后传送给发卡行。

- 技术

  发卡行参加这项服务，需要改造主系统，以使用 CUPS 代校验服务提供的相关信息。

9.5 未来密文支持

随着市场发展的需要，有可能会定义新的密文版本，包含不同的数据元以适应特定需求。银联建议：发卡行主系统应该具备足够的灵活性以适应新的密文版本。可以在主系统中将“密文版本号”设置为一个处理参数，这样当一个新的密文版本号被导入时，系统架构就很容易适应这个变化。

未来密文支持所要求的活动如下：

技术

通过使用“密文版本号”作为处理联机卡片认证和发卡行认证的逻辑参数，设置系统架构能够方便地适应新密文的导入。

9.6 数据记录/存档

CUPS 在联机报文和清算文件中提供了许多新增数据。发卡行应该根据其客户服务、风险管理、服务评估以及交易分析的需要，决定将认为最重要的数据进行存档。本节建议发卡行考虑的活动如下：

- 策略

  决定想要存档的数据。发卡行应该继续保存当前系统需要存档的数据；除此之外，发卡行应该存档与联机卡片认证相关的数据，记录：

  ✓ 联机卡片认证通过与否；

  ✓ DKI 是否存在于报文中；

  ✓ MDK 在 HSM 中是否找到；

  ✓ 密文版本 01 要求数据元是否都存在；

  ✓ 是否出现 HSM 奇偶校验错。

  发卡行也应该存档其它有助于交易分析的芯片数据：

  ✓ 脱机 PIN 结果（在 CVR 中）；

  ✓ 脱机认证结果（在 TVR 中）；

  ✓ 应用交易计数器的值。

- 技术

  改造系统以记录新增数据。

9.7 发卡行脚本处理

本节描述了：对于发卡行实现发卡行脚本处理，主系统需要进行的改造。

9.7.1 概要

发卡行脚本处理允许发卡行在发卡后修改账户相关信息，或锁定卡内所有应用。发卡行将脚本命令放在交易应答报文中传送给终端，终端将命令转发给卡片。当满足安全要求以后，卡片执行命令。

安全报文机制用到了两种 DES 密钥：

- 报文认证码(MAC)密钥
  这个密钥用于保护发卡行脚本处理的安全，对于任何发卡行脚本命令都必须使用。用于确认数据没有被篡改过（完整性），同时可以确认命令发出的发卡行是否是合法（发卡行认证）；MAC 主密钥(MAC MDK)存放在发卡行主系统 HSM，由其分散得到 MAC 子密钥（MAC UDK）存放在卡内。
- 数据加密(ENC)密钥
  这个密钥用来加密脚本中的敏感数据，如脱机 PIN 等。ENC 主密钥(ENC MDK)存放在发卡行主系统 HSM，由其分散得到 ENC 子密钥（ENC UDK）存放在卡内。

发卡行脚本处理支持的命令包括：

- 应用锁定
- 应用解锁
- 卡片锁定
- PIN 修改/解锁
- 设置数据
- 修改记录

每个命令的细节，请参见 “表 18－发卡行脚本处理命令”。

9.7.2 先决条件

发卡行脚本处理的先决条件包括：

- 发卡行系统必须升级，以支持 Full 选项。
- 受理此类交易的收单行必须支持 Full 选项。或者在发卡行自己的处理网络中，受理环境能够支持 Full 选项，那么发卡行内部交易可以发送脚本处理命令。
- 配置卡片支持接收、处理发卡行脚本命令和数据。发卡行在采购卡片之前，先获得卡片供应商对此的确认。
- 在交易应答报文中返回的发卡行脚本长度不能超过 128 字节。某些网络可能不支持这个长度，因此银联建议：发卡行应该尽量避免使用最大长度发送脚本。从发卡行专用设备也可以发送发卡行脚本命令，如：ATM、柜台终端；依照 EMV 规定，这些命令可以长至 261 字节（如果发卡行网络支持）。

发卡行脚本处理必须应遵守《中国金融集成电路（IC）卡规范》以及相关的操作规则。

- 发卡行脚本处理不应对 POS 交易或 ATM 交易造成不良影响。
- 仅发卡行拥有二次发卡更新权限。
- 只可通过交易应答报文发送发卡行脚本。

为了支持发卡行脚本处理而准备系统环境，必须：

- 将 MAC MDK 和 ENC MDK 装载到发卡行主系统中。
- 支持双倍长密钥。
- 升级发卡行主系统，支持发卡行脚本处理。

9.7.3 执行活动

下表列示了有关实现发卡行脚本处理的技术活动：

表32 发卡行脚本处理执行活动

步骤	责任方	活动
1	技术	为了确保只有发卡行能够发送脚本处理命令、以及脚本中任何敏感数据的安全，发卡行主系统必须执行以下密钥管理操作： • 将 MAC MDK 导入 HSM，这个密钥用于保护发卡行脚本处理的安全； • 将 ENC MDK 导入 HSM，这个密钥用来加密脚本中的敏感数据，例如：如果想要使用

		PIN 修改/解锁命令更改持卡人 PIN，发卡行必须使用这个密钥对新 PIN 进行加密； • 将这些 MDK 安全传递至个人化系统，用于派生 UDK 并导入卡内。
2	技术	分析发卡行脚本命令，决定准备实现的命令集。 一个简单的方法是：在项目初期，仅支持应用锁定命令；随着管理发卡行脚本处理的经验积累，逐步支持其它命令。如果发卡行支持脱机 PIN，应该支持 PIN 修改/解锁命令。
3	技术	发卡行主系统增加支持的命令文件。
4	技术	创建后台处理流程：允许客户服务、风险管理平台在主文件中，对特定卡品牌、卡类型或卡段设置要求发卡行脚本处理的标志。以下描述了几个命令的例子： • 应用锁定－卡片没收处理，在主文件中进行标记仍使用现有流程，还需要在返回拒绝响应的同时，增加允许发卡行发送应用锁定命令的处理逻辑； • 设置数据－通过对持卡人历史数据分析，发卡行可以设置对某些卡或某个范围的卡要求更改频度计数器。 银联建议：对多应用卡不要返回“没收卡”的响应，代之以使用卡片锁定或应用锁定命令。
5	技术	在联机交易处理过程中，查询主文件信息，如果主文件指出需要发起一个发卡行脚本处理，定位其发卡行脚本命令。这个命令已经在步骤 4 中准备好。
6	技术	依据这个命令，添加命令所要求的特定数据，如：新的持卡人脱机 PIN、频度限制的更新值。
7	技术	如果在脚本中有敏感数据，执行以下操作加密敏感数据；否则，跳至步骤 9。 • 在 HSM 中定位 ENC MDK； • 使用 ENC MDK 分散得到 ENC UDK； • 使用 ENC UDK 结合 ATC 分散得到 ENC 过程密钥(ENC SESK)； • 使用 ENC SESK 加密敏感数据。
8	技术	生成一个 MAC 值，附于发卡行脚本末尾： • 在 HSM 中定位 MAC MDK； • 使用 MAC MDK 分散得到 MAC UDK； • 使用 MAC UDK 结合 ATC 分散得到 MAC 过程密钥(MAC SESK)； • 使用 MAC SESK，针对二次发卡数据的全部内容生成一个 MAC 值。 注：确保卡片支持这个 MAC 长度（目前 PBOC 规定 MAC 长度为 4）。
9	技术	将发卡行脚本加入交易应答报文中（55 域，Tag－72）。
10	技术	发卡行从清算文件或后续请求报文中获得发卡行脚本处理结果后，修改主文件相关数据。

9.8 授权决定处理

发卡行在芯片和磁条交易中都可以使用新增芯片相关数据进行授权决定处理。本节提供使用这些数据的建议。

9.8.1 芯片发起交易

发卡行应该延续使用授权决定处理的现有标准，如：确保账户有良好的信誉、充足的资金。同时，分析所有新增芯片数据，特别是卡片验证结果(CVR)和终端验证结果(TVR)，决定哪些信息是对发卡行特别重要的。银联建议：发卡行应结合下表所列数据进行授权决定处理。

表33 参与授权决定处理的数据元

新增数据	作用
联机卡片认证结果	防止伪卡，提供数据完整性。 有卡交易的证据。 脱机处理结果的有效性证明。
脱机 PIN 验证结果	防止失窃卡。

	持卡人在交易现场的证据。
脱机数据认证结果 [1]	防止数据篡改（SDA）、数据篡改以及伪造卡（DDA）。
新卡标志 [1]	卡片首次使用的证据。
商户强制交易联机标志 [1]	商户认为交易（或持卡人）可疑，强制要求联机的证据。
PIN 尝试次数超限标志 [1]	卡片被偷或持卡人忘记 PIN 的证据。
应用交易计数器(ATC)	因为这个计数器为每笔交易提供一个连续的参考号，如果出现一个重复的或跨度很大的 ATC 值，可能预示着伪卡或其它欺诈嫌疑。

1－如果发卡行对这些条件设置卡片动作为脱机拒绝，发卡行授权系统将无法获得这些事件的证据。

使用 PBOC 数据参与发卡行授权决定处理所要求的活动包括：

- 策略

  决定发卡行产生授权决定标准。建议在当前使用标准的基础上，结合银联推荐的数据予以增强。
- 技术

  改造主系统，使用新增芯片数据参与授权决定处理。

9.8.2 降级使用交易

降级使用交易(Fallback)是指芯片卡在具有芯片能力的终端上执行非芯片交易（磁条交易）。在发卡行主系统，可以通过以下数据域的组合识别这种情况：

- “服务点输入方式码（PAN 输入方式）”不是 05 或 95（22 域），表明是一个非芯片卡读取方式。
- “终端读取能力”是 5（60.2.2 域），表明是可读取芯片卡的终端。
- “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），表明卡片上有芯片存在。

发卡行应该改造主系统，检查磁条交易的这些值以确定是否为一笔 Fallback 交易。发卡行应该决定是否将 Fallback 交易与其它交易区别对待，需要在客户服务和风险控制之间权衡后做出决策。

处理 Fallback 交易要求的活动包括：

- 策略

  发卡行基于市场条件，决定如何对待 Fallback 交易。如果所处市场向芯片迁移已经比较成熟，发卡行应该倾向于视 Fallback 交易为高欺诈和信用风险的交易。发卡行需要决定何时是认可或拒绝 Fallback 交易合适的时间点。

  发卡行可以决定：在产品投放市场之初、或判断市场上的新型芯片技术已经稳定之前，不拒绝 Fallback 交易。当感觉到所处市场已经足够成熟，应该考虑对 Fallback 交易进行更严格的处理。

  需要注意的是：导致 Fallback 交易的因素是多种多样的；例如：欺诈、与商户勾结、糟糕的商户受理手续、芯片不可操作、终端读取芯片设备出现故障等，都可能导致 Fallback 交易。

  银联强烈建议：发卡行应对 Fallback 交易执行趋势分析。这个分析能够帮助发卡行判断 Fallback 交易发生的原因，银联和发卡行、涉及的其它会员行可以一起使用这些信息来追踪 Fallback 的真实情形。
- 技术

  改造主系统以识别 Fallback 交易，对 Fallback 交易的处理动作，开发 Fallback 交易趋势分析报表。

10 发卡行后台系统改造

本章主要描述：为了支持 PBOC 应用，后台功能模块所要求的技术改造。包括以下方面：

- 电子现金
- 对账单
- 客户服务

- 卡管理系统
- 卡片置换
- 争议处理
- 清算与对账
- 报表
- 内部员工培训

10.1 电子现金

10.1.1 账户设置

虽然小额支付规范对于发卡行主机端的账户设置、额度使用方式定义的相对灵活，但是应考虑避免账户管理过于复杂、避免让持卡人产生混淆，建议按以下原则管理账户：

- 从主账户余额划出电子现金额度，也可以对持卡人的授信额度按一定比例新增一个电子现金额度。
- 将电子现金额度标识为与主账户关联的一个映射账户，将金额从当前账户移至映射账户，称之为电子现金账户。
- 所有联机交易均针对持卡人主账户进行授权和清算，既不影响电子现金账户金额，也不影响卡片电子现金余额。
- 通过卡片电子现金余额脱机授权完成的消费交易，后续针对电子现金账户进行清算。
- 电子现金账户不挂失、不计息、不能取现（销卡时可以圈提）。

10.1.2 脱机授权额度设置

PBOC 用于脱机授权的额度有两个：CTTA 额度和 EC 额度。对于这两种额度的区别可以这样理解：CTTA 额度缺省对应主账户，使用 CTTA 额度进行脱机消费有可能发生透支；而 EC 额度对应电子现金账户，使用 EC 额度进行脱机消费不可能发生透支。

标准 PBOC 脱机授权使用的是 CTTA 额度，而标准 PBOC 下的电子现金功能使用的是 EC 额度，这时它完全独立于 CTTA 额度。qPBOC 则提供了三种脱机授权选项：

- 小额－只使用 EC 额度；
- 小额和 CTTA－使用 EC 额度，同步更新 CTTA 额度；
- 小额或 CTTA－首先考虑使用 EC 额度，如 EC 额度不足，转而使用 CTTA 额度。

发卡行如何使用这两种额度需要考虑多方面的因素，但是在受理环境普遍支持电子现金交易（或 qPBOC 交易）的情况下，建议只使用 EC 额度、而不设置 CTTA 额度。

10.2 对账单

实现 PBOC 应用，可能会对两类账单造成影响：

- 银联给发卡行的对账单可能变化；
- 客户对账单可能发生变化。

10.2.1 银联对账单

发卡行应该联系银联代表，确定是否会发生针对 PBOC 的账单变化。例如：根 CA 处理可能要求新的收费。

10.2.2 客户对账单

当现有磁条卡替换为芯片卡、但产品服务不变时，通常不会改变定价。发行芯片卡的成本通常由发卡行自己承担；使用芯片卡能够显著降低欺诈损失，有助于抵销部分成本。

但是，如果发卡行发布的产品导入了新的增值服务，这是一个重新定价的机会。价格调整可以采用配套账户定价或总体交易收费的形式。在定价改变之前，发卡行应该完成相应的对账单要素改造，例如：

- 新的客户关系类型及费用；
- 新的服务类型及费用；
- 应用交易计数器；

- 在账户声明栏说明新增服务及收费情况。

任何定价的变化，应该在发卡行法律部门评估、并向客户公示之后再实施。

注：银联不会推荐详细的定价安排，产品定价基于成员行自己的判断。

10.3 客户服务

发卡行实施借/贷记产品芯片化，提供优秀的客户服务是一个关键的成功要素。对客户询问予以快速而精确的处理，将有助于促进 PBOC 应用的普及。要达到这种支持标准，肯定需要对客户服务系统做出修改；增加芯片卡功能和交易的相关信息，并且修改客户服务手册。

客服代表需要在其操作屏幕上区分芯片卡与磁条卡，查阅卡片脱机参数等。在客服屏幕上应该显示的信息包括：

- 芯片卡标志；
- 发卡行脚本处理命令携带的芯片个人化信息；
- 按 PBOC 标准或磁条处理的交易数据；
- 卡内存放的应用列表、对应卡号（账号）；
- 卡管理系统提供的数据。

银联建议：使用一个芯片标志、而不是卡号范围来指示 PBOC 卡。

修改客户服务手册，帮助客服代表解答客户与芯片相关问题。例如，与一笔被拒绝的 PBOC 交易相关问题包括：

- 卡是使用芯片还是磁条处理而被拒绝的？
- 卡是因为输入错误的 PIN 而被拒绝的吗？
- 尝试了多少次交易？交易金额是多少？
- 交易被拒绝之前，完成了什么？

10.4 卡管理系统

升级卡管理系统以反映芯片卡的新增数据和风险参数。卡管理系统增加这些参数，可以跟踪卡片这些芯片数据的使用情况，可以根据这些记录在卡片失窃时重新发卡、或到期换卡。根据卡片支持功能的不同，银联推荐发卡行包含以下数据：

- 卡片序列号（当一个卡号关联着多个持卡人时）；
- 授权控制参数，特别是按卡片类型或卡号范围区分的频度检查参数；
- 持卡人验证方法(CVM)列表设置；
- 持卡人脱机 PIN 和 PIN 尝试限制数；
- DKI（指示联机卡片认证、发卡行认证以及发卡行脚本处理使用的 MDK）。

另外，在卡片生命周期中所做的任何发卡行脚本更新，都应该同步修改卡管理系统的相关信息，这样可以保证使用正确的配置重新发卡。

10.5 卡片置换

在 PBOC 迁移过程中，发卡行应该考虑如何管理卡片置换活动，特别是对多应用卡。决定卡片置换流程，需要考虑以下方面：

- 如果芯片卡交货时间太长，是否使用磁条卡作为过渡；
- 芯片卡在哪里进行个人化，相关信息怎样传递给个人化厂商；
- 卡管理系统如何修改，以标识卡片置换、跟踪卡片置换整个周期；
- 在卡片置换过程中，客服代表怎样调阅卡片信息；
- 怎样将所有应用完整置换到多应用卡上，包括非支付应用，如：积分应用。

10.6 争议处理

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主系统和客户服务系统的潜在影响。差错处理允许发卡行通过退单将交易退回收单行。

发卡行需要决定在系统中如获取、处理、记录及备份影响争议处理的芯片数据，并进行相应改造。

银联建议：保留这类数据足够长的时间 ，以应对可能发生的争议处理；如：180 天以上。

对于一笔交易，其请求报文中的某些芯片数据提供了卡片和终端执行风险检查的证据，交易应答报文提供了发卡行执行处理的证据。

10.7 清算与对账

实施 PBOC 迁移应该不会对清算与对账处理造成影响。为了便于跟踪、分析，应该对 PBOC 交易有单独的报表统计；对于自动对账系统，芯片交易也应包含在输入文件中。

脱机授权交易在系统中只有一笔清算交易，不会有一笔授权交易与之关联。

10.8 报表

本节协助发卡行改造内部报表系统。

10.8.1 芯片交易统计

应该有单独的芯片交易报表、区分芯片和磁条交易的报表，交易笔数和交易金额都是需要关注的。这些统计数据在清算与对账、欺诈、客户服务、服务费用等一系列报表中都会有所体现，帮助发卡行监控 PBOC 应用的增长率、风险控制成效。

发卡行可以通过以下数据域识别芯片发起交易：

- “服务点输入方式码（PAN 输入方式）”为 05 或 95，表明是一笔芯片发起交易；
- “终端读取能力”为 5，表明终端具备读取芯片能力。

10.8.2 Fallback 交易

降级使用交易(Fallback)是指芯片卡在具有芯片能力的终端上执行非芯片交易（磁条交易）。银联建议：发卡行跟踪、报告所有 Fallback 交易，以确定其发生原因。如果 Fallback 交易频繁发生，说明卡片或受理环境出现异常。

发卡行可以通过以下数据域的组合识别 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。
- “IC 卡条件代码”为 1 或 2，指示磁条上的“服务代码”是 2xx 或 6xx，表明卡片上有芯片存在。

如果一个特定卡号或卡号范围的卡频繁发生 Fallback 交易，有可能是卡片存在某种错误，如：不正确的个人化数据、或无法使用的芯片。对于这种情况，银联建议：发卡行联系持卡人面谈此事；如有可能，应该请求持卡人将卡片带到银行或寄送过来，以便进一步研究。

发卡行如果发现某个商户或收单行发生 Fallback 交易的比率过高，应该及时联系银联代表，由银联代表协调发卡行、收单行共同解决这个 Fallback 问题。

10.8.3 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。在发卡行实现 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功能。可以考虑增强以下报表：

- 欺诈类报表，突出磁条和芯片卡的差异；
- 基于卡片参数设置来鉴别可疑活动的报表；
- 脱机交易和联机交易的比较统计报表；
- 联机卡片认证、脱机数据认证、脱机 PIN 验证结果信息报表；
- 芯片卡发行量、交易量统计报表。

10.8.4 交易研究工具

实现 Full 选项的发卡行，可以考虑开发一个分析 PBOC 交易的工具。例如：可以实时或在交易完成后立即采集 PBOC 授权信息传递给一个后台数据仓库。通过查询这个数据库，可以确定脱机数据认证、脱机 PIN 验证、联机卡片认证和发卡行认证等处理的正确性。这个数据库对负责客服、争议处理、清算与对账的员工也会很有帮助。

10.9 内部员工培训

PBOC 与其说是一个新产品，不如说是现有卡产品的重新构造。它影响当前事务的所有方面，包括：市场推广人员、客服员工、业务支持员工、后台处理员工、系统开发团队、法律顾问以及风险管理人员。

发卡行制定培训计划，应考虑为不同岗位员工定制有针对性的专业知识培训。整个培训应细分为多个特定单元。与持卡人直接交互的单元需要进行更广泛的培训，因为芯片处理流程十分复杂，与磁条处理有很大差异。银联建议：将培训计划办成一个持续的活动，因为多数员工可能需要几次培训才能理解、掌握这么多技术事项。发卡行也应将 PBOC 应用培训安排到新员工培训计划中。

发卡行可以在培训计划启动的初期，开通一个内部热线或 E-MAIL 来解答员工提出的问题。银联建议：设立一个内部网站收藏相关文档，方便员工查阅。

培训计划应该包含以下任务：

- 确定整个机构涉及 PBOC 迁移的部门；
- 制定对不同岗位员工的培训目标；
- 决定对不同岗位员工的培训要求；
- 设计培训课程；
- 编制培训材料、操作手册、用户指南；
- 根据各部门要求，调整培训计划；
- 制定培训时间表；
- 按计划开展培训。

一个完善的培训计划有助于 PBOC 迁移活动的平稳实施，有效避免在项目临近上线时问题丛生。

10.10 执行活动

本节针对发卡行后台系统的对账单、卡片置换、争议处理、报表及员工培训诸方面要求执行的活动做一汇总：

- 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
  - ✓ 评估价格变动的影响，确定合适的交换费率；
  - ✓ 通知持卡人新的价格结构（如果适用）；
  - ✓ 制定、实施卡片置换流程；
  - ✓ 评估 PBOC 对争议处理业务规则的影响；
  - ✓ 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，应涵盖所有涉及员工。
- 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，以及实现卡片置换所需要的改造。

11 发卡行主机认证

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

本文未涉及 PBOC 迁移的其它测试事项，如：内部系统、后台处理。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发卡行测试计划中。

银联提供测试工具协助发卡行进行主机认证。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 程序改造的内部测试，发卡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。

联系银联代表获取认证脚本以及其它认证材料。

银联建议：发卡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 选项的发卡行主机认证过程。发卡行必须按照认证测试脚本执行一系列交易，以证明发卡行主机系统能够发送和接收每个报文的新增数据域。

下表总结了发卡行主机认证的重要步骤：

表34 发卡行主机认证

步骤	责任方	活动
1	技术	提交发卡行主机认证申请表。包括：机构信息表、卡片信息表等。 联系银联代表获取这些表格。
2	银联	审批发卡行主机认证申请。
3	银联	银联提供获取测试工具（5 个工作日）。包括：测试案例库、相关文档。
4	银联	银联为发卡行安排测试培训。
5	技术	执行脱机测试－发卡方模式。
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	发卡行提前向银联提供测试卡。
10	技术	如果认证通过，发卡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，发卡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/贷记发卡机构入网测试还包括“卡片认证”，发卡行每发行一种PBOC卡产品、或同一种卡产品的个人化数据设置变化可能影响到联网通用，都需要进行卡片认证。有关卡片认证的详细信息，请咨询银联代表。

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发卡行的具体要求，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、以及如何促进发卡行的商业需求，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、持卡人、产品厂商、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。

本附录用于帮助发卡行规划 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：如果发卡行的一个主要目标是发行包含积分功能的多应用卡，就需要确保所选卡片结构、存储容量以及参数设置能够支持这个功能；对与之无关的其它可选功能就不需要投入太多关注了。

发卡行可以依据项目范围来决定实现此计划的方法。发卡行应根据设备、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：

- 卡产品经理

  卡产品经理从业务角度把握迁移计划的格局，决定准备实现的功能及其业务策略。卡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 迁移计划涉及到与供应商签订新合同、或修订原有合同，与持卡人的用户条款也需要修改，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。
- 客户服务

  客户服务处理持卡人查询、账户维护、持卡人争议等业务流程需要改造以适应 PBOC 应用。
- 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”可以帮助发卡行制定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	发卡行完全迁移
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	密钥管理系统建设
4.2.1	对称密钥系统建设
4.2.2	非对称密钥系统建设
4.3	芯片卡选择与个人化
4.3.1	卡片选择
4.3.1.1	确定对卡片功能、安全要求
4.3.1.2	确定对多应用平台的要求
4.3.1.3	评估卡片安全性能
4.3.1.4	分析卡片规格是否满足各项要求
4.3.1.5	卡片供应商提供卡片质量管理服务
4.3.1.6	确认卡片供应商通过银行卡检测中心认证
4.3.2	卡片设计、制造
4.3.2.1	卡面设计
4.3.2.2	确定卡片安全传输机制
4.3.2.3	生成卡片传输密钥
4.3.2.4	将传输密钥送至卡片生产厂商
4.3.2.5	卡片封装、印刷
4.3.2.6	获得用于个人化的卡片
4.3.3	发卡行证书的生成和下载
4.3.3.1	生成发卡行公私钥对
4.3.3.2	创建发卡行公钥文件
4.3.3.3	获得根 CA 申请表
4.3.3.4	将表格和公钥文件提交给银联
4.3.3.5	接收发卡行公钥证书
4.3.4	数据准备系统安装调试
4.3.5	卡片个人化
4.3.5.1	根据数据准备系统的输出产生个人化脚本
4.3.5.2	连接密钥管理系统，获得卡片密钥
4.3.6	选择个人化数据模板
4.3.6.1	正确选择 PBOC 个人化数据
4.3.6.2	针对数据模板设置个人化系统
4.3.7	验证卡片数据的正确性
4.3.7.1	采用 PBOC IC 卡测试工具对卡片进行验证
4.3.7.2	将卡片送至银联由银联对卡片数据进行验证
4.3.7.3	银联反馈测试报告
4.3.8	生产样卡
4.4	主机系统改造
4.4.1	交易处理系统改造
4.4.2	业务处理系统改造

4.5	系统入网测试认证
4.5.1	脱机测试部分
4.5.1.1	使用银联仿真器测试
4.5.1.2	提交测试日志
4.5.1.3	银联对日志进行评审
4.5.2	联机测试部分
4.5.2.1	进行联机测试认证
4.5.2.2	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	产品发布
6.1	确定产品发布策略
6.2	制定产品发布计划
6.3	制定设备交付计划
6.4	准备技术环境
6.4.1	网络连通
6.4.2	环境测试
6.4.3	系统安装
6.5	投产准备
6.5.1	规划并实施投产预演
6.5.2	导入投产数据
6.5.3	操作培训
6.5.4	测试灾备系统
6.6	投产
6.6.1	制定投产方案、预期结果
6.6.2	准备验证数据
6.6.3	执行投产计划
6.6.4	验证 PBOC 应用的正确性
6.6.5	通过业务部门验收
6.6.6	移交给日常运维部门

附 录 B
（资料性附录）
密钥快速参考表

本附录提供了 PBOC 应用涉及密钥的快速参考，包含以下类型的密钥。

B.1 个人化密钥

用于保护个人化过程。

表35 个人化密钥

缩写	名称	生成级别	说明
KMC	发卡行主密钥	每个卡片供应商	IC 卡厂商使用这个 KMC 生成卡片级密钥（KENC、KMAC、 KDEK），并将它们写到卡上。
K_{ENC}	数据加密密钥（卡片级）	每个应用	用来创建一个对话密钥，利用该对话密钥可创建密文和以 CBC 模式加密机密数据。
K_{MAC}	MAC 密钥（卡片级）	每个应用	用来创建一个对话密钥，利用该对话密钥可创建命令处理过程中所使用的 C-MAC。
K_{DEK}	数据加密密钥（卡片级）	每个应用	用来创建一个对话密钥，利用该对话密钥可在 ECB 模式下加密 DES 密钥或灵活的加密其它机密数据。
KEK_{ISS}	发卡行密钥交换密钥	每个发卡行	对发卡行与数据准备设备之间的脱机 PIN 及其它机密数据进行保护。
DEK/TK	数据加密密钥/传输密钥	每个个人化设备	对数据准备设备与个人化设备之间的脱机 PIN 及其它机密数据进行保护。 下列特殊类型的数据传输密钥可能会被使用： PEK/TK - PIN 加密密钥，用于保护 PIN 数据。 KEK/TK - 密钥交换密钥，用于保护 DES 密钥。
MACkey		每个个人化设备	用于保证在个人化数据文件中，提供给个人化设备的应用数据的完整性。

B.2 联机卡片和发卡行认证密钥

用于联机卡片认证和发卡行认证。

表36 联机卡片和发卡行认证密钥

缩写	名称	生成级别	说明
AC MDK	应用密文主密钥	每个 BIN	生成唯一的卡片密钥，用于卡片和发卡行进行联机验证。
AC UDK	应用密文子密钥	每个应用	生成唯一的对话密钥－SUDK AC，用于应用密文的产生和验证。
DKI	分散密钥索引	每个 MDK	用来明确使用哪个主密钥分散得到卡片中的子密钥。

B.3 公钥

用于 SDA、DDA、脱机密文 PIN。

表37 公钥

名称	用途	生成级别	说明
认证中心公私钥对	SDA、DDA、脱机密文 PIN	PBOC 根 CA 生成	根 CA 负责认证中心公钥对的生成、管理。
发卡行公私钥对	SDA、DDA、脱机密文 PIN	每个 BIN	由发卡行生成，公钥应传输给 PBOC 根 CA，供其创建发卡行公钥证书。私钥被保存在发卡行的 HSM 内。
IC 卡公私钥对	DDA、脱机密文 PIN	每个应用	支持 DDA 要求发卡行为每张 IC 卡产生 IC 卡公私钥对，IC 卡私钥存放在 IC 卡中的安全存贮区域，IC 卡公钥由发卡行私钥签名，产生 IC 卡公钥证书并存放在卡片中。
签名的静态应用数据(SAD)	SDA、DDA	每个应用	用来验证卡片应用数据的签名。对于 SDA,使用发卡行私钥签名的 SAD 单独存放在卡内；对于 DDA，SAD 包含在 IC 卡公钥证书中。
发卡行公钥证书	SDA、DDA、脱机密文 PIN	每个 BIN	证书中包括了使用根 CA 私钥签名的发卡行公钥
IC 卡公钥证书	DDA、脱机密文 PIN	每个应用	包含发卡行私钥签名的 IC 卡公钥，在卡片个人化时放入卡中。证书中有使用发卡行私钥作签名加密的静态应用数据。

B.4 发卡行脚本处理密钥

用于保护发卡行脚本处理数据。

表38 发卡行脚本处理密钥

缩写	名称	生成级别	说明
MAC MDK	安全报文认证(MAC)主密钥	每个 BIN	生成唯一的卡片密钥－MAC UDK，这个卡片密钥用于生成进行发卡后的数据更新所需要的消息认证对话密钥。
MAC UDK	安全报文认证(MAC)子密钥	每个应用	生成唯一的对话密钥－SUDK MAC，用于安全报文认证码的产生和验证
ENC MDK	安全报文加密主密钥	每个 BIN	生成唯一的卡片密钥－ENC UDK，这个卡片密钥用于生成对发卡后更新机密数据（脱机 PIN）进行加密的对话密钥。
ENC UDK	安全报文加密子密钥	每个应用	生成唯一的对话密钥－SUDK ENC，用于加密解密安全报文

B.5 传送密钥

用于发卡行与银联、第三方供应商之间传递密钥。

表39 传送密钥

缩写	名称	生成级别	说明
ZCMK	地区控制主密钥	每个实体关系 如：发卡行与银联	由发卡行或银联生成，存储于各个实体的 HSM 中。

附 录 C
（规范性附录）
中国银联 IC 卡发卡入网工作流程

入网发卡机构要开通 IC 卡功能，其流程与磁条卡发卡类似，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

发卡行的 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

在完成入网测试后，发卡行进入 IC 卡入网开通申请流程，具体如下：

1. IC 卡入网机构提出发卡入网申请
   入网机构填写业务管理部提供的相关发卡申请表格，完成后统一交至业务管理部进行审定。
2. 中国银联对申请进行审核
   业务管理部对入网机构的申请进行审核，包括以下内容：
   - ✓ IC 卡新 BIN 号的分配
   - ✓ 卡样的审查
   - ✓ 样卡磁道信息的检查，以及芯片信息与磁道信息一致性的检查,可以委托检测中心进行（如果仅发行芯片卡的话，则仅对芯片的主帐户信息和磁道镜像信息检查）
   - ✓ 其它相关的检查（如：CVN 检查、三磁依赖检查等）
3. 以上步骤完成后即可等待业务开通

C.3 特别说明

对于银联IC卡发卡入网工作流程，有几点需要明确：

1. 入网机构的脱机测试包括：卡片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。