ICS 35.240.40
A 11
备案号：

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0025.10—2013
代替JR/T 0025.10—2010

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

China financial integrated circuit card specifications—
Part 10: Debit/credit card personalization guide

2013-02-05 发布　　2013-02-05 实施

中国人民银行 发布

目　　次

前　言

JR/T 0025《中国金融集成电路（IC）卡规范》分为以下部分：

——第1部分：电子钱包/电子存折应用卡片规范（废止）；

——第2部分：电子钱包/电子存折应用规范（废止）；

——第3部分：与应用无关的IC卡与终端接口规范；

——第4部分：借记/贷记应用规范；

——第5部分：借记/贷记应用卡片规范；

——第6部分：借记/贷记应用终端规范；

——第7部分：借记/贷记应用安全规范；

——第8部分：与应用无关的非接触式规范；

——第9部分：电子钱包扩展应用指南（废止）；

——第10部分：借记/贷记应用个人化指南；

——第11部分：非接触式IC卡通讯规范；

——第12部分：非接触式IC卡支付规范；

——第13部分：基于借记/贷记应用的小额支付规范；

——第14部分：非接触式IC卡小额支付扩展应用规范；

——第15部分：电子现金双币支付应用规范；

——第16部分：IC卡互联网终端规范；

——第17部分：借记/贷记应用安全增强规范。

本部分为JR/T 0025的第10部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分对金融借记/贷记卡个人化提供了指导意见。

本部分代替JR/T 0025.10—2010《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》。

本部分与JR/T 0025.10-2010相比主要变化如下：

——修订了标准的前言；

——增加了第6.5节“个人化数据必须遵循的规则”。

——本部分与JR/T 0025.10—2005相比主要变化如下：

——重新起草标准的前言；

——将“规范性引用文件”、“符号和缩略语”在正文中的出现情况做了核对，对于没有出现的直接予以删除，对于出现的进行了修改和完善；另外，将参考到的文件归入参考文献；

——将标准中表述不规范之处进行明确，并参照JR/T 0025的其他部分进行统一。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分主要起草单位：中国人民银行、中国工商银行、中国银行、中国建设银行、中国农业银行、交通银行、中国邮政储蓄银行、中国银联股份有限公司、中国金融电子化公司、银行卡检测中心、中钞信用卡产业发展有限公司、捷德(中国)信息科技有限公司、惠尔丰（中国）信息系统有限公司、福建联迪商用设备有限公司。

本部分主要起草人：王永红、李晓枫、陆书春、潘润红、杜宁、陈则栋、吴晓光、李春欢、刘志刚、张永峰、汤沁莹、李新、张栋、王红剑、李一凡、余沁、周新衡、张步、冯珂、李建峰、向前、涂晓军、齐大鹏、陈震宇、郑元龙、聂舒、丁吉、白雪晶、李子达、沈卓群、刘世英、于海涛、翁秀诚。

本部分所代替标准的历次版本发布情况为：

——JR/T 0025.10—2005；

——JR/T 0025.10—2010。

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

1 范围

JR/T 0025的本部分描述了中国金融集成电路（IC）卡借记/贷记应用特有的个人化指令、特有的数据分组标识（DGI）的定义及个人化时有关安全方面的规定。

本部分适用于由银行发行或接受的中国金融集成电路（IC）卡借记/贷记卡，目的是为数据准备系统提供商和个人化中心定义数据准备阶段的要求提供指导。同时，也可为应用设计者设计默认文件和记录结构提供参考。本部分也可供个人化其它应用时参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0025.5 中国金融集成电路（IC）卡规范 第5部分：借记/贷记应用卡片规范

JR/T 0025.12 中国金融集成电路（IC）卡规范 第12部分：非接触式IC卡支付规范

JR/T 0025.17 中国金融集成电路（IC）卡规范 第17部分：借记/贷记应用安全增强规范

GM/T 0002 SM4分组密码算法

GM/T 0003 SM2椭圆曲线公钥密码算法

GM/T 0004 SM3密码杂凑算法

GM/T AAAA SM2密码算法使用规范

ISO 9807 银行业务和相关金融服务 报文鉴别要求（零售）

3 符号和缩略语

下列符号和缩略语适用于本文件。

ADA	应用缺省行为(Application Default Action)
ATC	应用交易计数器(Application Transaction Counter)
AuthC	授权控制(Authorization Controls)
BIN	银行标识号(Bank Identification Number)
CA	认证中心(Certificate Authority)
CAM	卡片认证方法(Card Authentication Method)
CBC	密文块链接(Cipher Block Chaining)
CDA	复合动态数据认证/应用密文生成(Combined DDA/AC Generation)
CDOL	卡风险管理数据对象列表（Card risk management Data Object List）
CID	密文信息数据(Cryptogram Information Data)
C-MAC	命令—报文鉴别码（Command-Message Authentication Code）
CVM	持卡人验证方法(Cardholder Verification Method)
DDA	动态数据认证(Dynamic Data Authentication)
DDOL	动态数据认证数据对象列表（Dynamic Data authentication data Object List）
DEK/TK	数据加密密钥(Data Encryption Key)

DES	数据加密标准(Data Encryption Standard)
DGI	数据分组标识符(Data Grouping Identifier)
EMV	Europay、MasterCard 和 Visa
ENC MDK	数据加密的主密钥(Master Data encipherment Key)
ENC UDK	独有的数据加密子密钥(Unique Data encipherment Key)
HSM	硬件安全模块(Hardware Secure Module)
IAC	发卡行行为代码(Issuer Action Code)
IC	集成电路(Integrated Circuit)
ICC	集成电路卡(Integrated Circuit(s) Card)
ISO	国际标准化组织(International Organization for Standardization)
ISS	发卡行(ISSuer)
KEK/TK	密钥交换密钥/传输密钥—由数据准备系统和个人化设备共享(Key Exchange Key Transport Key)
KEK_{ISS}	密钥交换密钥—由发行方和数据准备系统共享(Key Exchange Key)
K_{ENC}	卡片独有的密钥，用于产生加密会话密钥
K_{DEK}	卡片独有的密钥，用于产生对称密钥或其他可选保密数据会话密钥
K_{MAC}	卡片独有的密钥，用于产生 C-MAC 会话密钥
KMC	对称主密钥，用于在个人化过程中分散密钥来产生 K_{ENC}，K_{DEK}，K_{MAC}）
KMCID	对称主密钥标识符
MAC	报文鉴别码(Message Authentication Code)
MAC MDK	报文鉴别码主密钥
MAC UDK	报文鉴别码唯一子密钥
MDK	主密钥(Master Key)
PAN	主账号(Primary Account Number)
PEK/TK	PIN 加密密钥—一个专门用于 PIN 传输的传输密钥
PIN	个人识别码(Personal Identification Number)
RSA	Rivest、Sharmir 和 Adleman 提出的一种非对称密钥算法
SAD	已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)
SKU_{ENC}	用于加密的会话密钥，由 K_{ENC} 生成
SKU_{KEK}	用于加密对称密钥或其他可选保密数据的会话密钥，由 K_{DEK} 生成
SKU_{MAC}	用于在命令处理过程中创建 C-MAC，由 K_{MAC} 生成
SUDK ENC	由 MAC ENC 产生的独有数据加密会话密钥
SUDK MAC	由 MAC UDK 产生的报文鉴别码会话密钥
SM2	国家标准 ECC 椭圆曲线算法
SM3	国家标准杂凑算法
SM4	国产对称密码算法
TK	传输密钥
UDK	子密钥（Unique Key）

4 个人化过程概述

4.1 初始化

为了满足通用个人化的要求，在个人化以前，必然存在一个初始化（预个人化）的过程。它主要有以下几个部分组成:

a) 应用及相关文件和数据结构的确定:这是一个发卡系统中多方协调，确认最终应用（可能是多应用）的过程。由于通用个人化的要求，与最终应用相关的文件和数据结构也必须在此定义。与此同时，一些必要的数据准备工作，也在此完成;

b) 初始化设备的处理过程:初始化设备是向 IC 卡发送个人化数据的芯片读写器。对大多数使用这一通用方法的 IC 卡初始化过程来讲，这一设备必须与一个安全模块相连，以便向 IC 卡发送命令时进行数据的加解密和 MAC 校验;

c) IC 卡的初始化处理过程:IC 卡将从初始化设备接受初始化指令和相关数据，并依照初始化指令创建相应的应用、必需的文件结构、写入一定的数据，以便为下一步的个人化做好准备。经过初始化处理后，IC 卡将被部分锁定，从而将只能接受个人化指令和应用指令，不能再次修改文件或应用结构。

对初始化的进一步表述，见第5章和第8章。

4.2 数据准备

数据准备是负责创建存储在IC卡应用数据的程序。一些数据是每张卡都相同的，另一些是每张卡各有所异。一些数据可能在整个个人化过程中均是加密的，如密钥。

对数据准备的进一步表述，见第6章和第8章。

4.3 个人化设备处理

个人化设备是向IC卡发送个人化数据的芯片读写器。对大多数使用通用方法来做个人化的IC卡应用来讲，这设备必须与一个安全模块相连，以便向应用发送命令时进行数据的加解密和MAC校验。

个人化设备应该是独立的，并且与应用无关。

对个人化设备过程的进一步表述，见第7章和第8章。

4.4 借记/贷记应用程序处理过程

IC卡必须能够从个人化设备接收个人化应用数据并存储以供日后使用。

中国金融集成电路（IC）卡借记/贷记应用应被个人化过程之前设定的密钥锁定。

5 初始化

在个人化之前，必须激活IC卡，装入基本中国金融集成电路（IC）卡借记/贷记应用，并建立文件和数据结构。此外，还要把某些数据写入IC卡，在一些情况下，这些数据适用于整个卡（如KMCID：对称会话密钥主密钥标识符），而在另一些情况下，这些数据只适用于某一个应用（如AID：应用标识符）。初始化过程，必须使IC卡满足以下要求：

a) 除非 IC 卡能够动态地建立文件和记录而且能够将它们初始化为‘0’，必须事先为 IC 卡应用分区建立文件并为 JR/T 0025 所描述的数据分配存储空间。此外，这个存储空间必须初始化为二进制‘0’;

b) 必须能够根据 AID 选择每个应用;

c) 如果 IC 卡应用分区的文件控制信息（FCI）不需要个人化，该信息必须在初始化时创建;

d) 以下数据必须在初始化时写入 IC 卡中：

- 应用标示符（AID）必须写入，如果后缀（Suffix）存在，也一起写入;
- 以下数据单元在 RAM 中动态初始化为‘0’：
  - ‘9F27’密文信息数据;
  - 卡片请求脱机拒绝指示位;
  - 卡片请求联机指示位。
- 以下数据被初始化为‘0’，并由卡片操作系统或应用自身管理。当交易过程中卡片与设备间失去联系时，这些数据将被保留。

- 上次交易的数据——用于防拔卡处理：
  ——‘9F36’应用交易计数器（ATC）；
  ——‘9F58’连续脱机交易下限；
  ——‘9F14’连续脱机交易下限；
  ——‘9F59’连续脱机交易上限；
  ——‘9F23’连续脱机交易上限；
  ——PIN。
- 上次交易的数据——可选择保留，用于防拔卡或复位：
  ——连续交易计数器（国际—货币）；
  ——连续交易计数器（国际—国家）；
  ——累计脱机交易金额（双货币）；
  ——累计脱机交易金额；
  ——发卡行脚本命令计数器；
  ——发卡行脚本失败指示位；
  ——发卡行认证失败指示位；
  ——联机授权指示位（上次交易未完成）；
  ——静态数据认证（SDA）失败指示位；
  ——动态数据认证（DDA）失败指示位；
  ——上次联机应用交易计数器（ATC）寄存器；
  ——PIN尝试次数计数器。
- 以下数据被卡片操作系统或应用本身初始化为‘0’（特别表示的除外）：
  ——应用标识符（被初始化为指定应用的应用标识符）；
  ——应用版本号（被初始化为指定应用的应用版本号）；
  ——应用交易计数器（ATC）[注]；
  ——上次联机应用交易计数器（ATC）寄存器[注]；
  ——连续交易计数器（国际—货币）；
  ——连续交易计数器（国际—国家）；
  ——累计脱机交易金额（双货币）；
  ——累计脱机交易金额；
  ——发卡行脚本命令计数器；
  ——发卡行脚本失败指示位；
  ——发卡行认证失败指示位；
  ——联机授权指示位（上次交易未完成）；
  ——静态数据认证（SDA）失败指示位；
  ——动态数据认证（DDA）失败指示位。

注： 可以不通过GET DATA命令来取得。

6 数据准备

6.1 概述

数据准备必须创建用于个人化一个IC卡应用的数据。由数据准备过程中创建的保密数据必须加密，并且应该为传送到个人化设备的数据产生一个MAC，以保证那些数据的完整性。

数据准备过程分为以下五个步骤：

a) 创建个人化数据；

b) 将个人化数据组合为数据分组；

c） 创建个人化指令；

d） 为应用创建用于日志记录的数据；

e） 为个人化设备创建输入文件。

6.2 创建个人化数据

应用个人化过程的设计者必须决定在个人化期间哪些数据将被植入应用中，同时必须确定数据的来源。有些情况下，单一的数据准备过程将创建所有的数据。在其他情况下，数据将来源于多种渠道。数据可分为以下三种类型：

a） 发卡行主密钥及其相关数据；

b） 应用密钥和证书；

c） 应用数据。

6.2.1 发卡行主密钥及其相关数据

个人化过程通常要求创建发卡行主密钥和相关数据。一部分数据可能在个人化期间被植入卡内。主密钥用于生成卡片或应用密钥。

其他过程可能也会使用到一个或多个为个人化过程提供的主密钥。例如，用于数据准备和个人化之间的密钥交换密钥。为保证在过程之间主密钥能安全地被共享，需要一种导入和导出主密钥的方法。

6.2.2 应用密钥和证书

卡片如果支持卡片认证、发卡行认证或发卡行脚本处理，卡片密钥必须按JR/T 0025.5定义的方法，根据PAN和PAN序列号，用发卡行主密钥分散而成。

如果卡片支持脱机数据认证，并且卡片只支持单算法，发卡行需要生成一个SM2公私钥对，并且公钥必须由支付系统认证中心签名，其生成的发卡行公钥证书必须置于卡片中。如果支持DDA作为脱机数据认证方法，每张卡片都必须生成一对公私钥，并且ICC公钥必须由发卡行私钥签名，其生成的ICC公钥证书和相应的私钥也必须包含在卡片中。

如果卡片支持脱机数据认证，并且卡片支持双算法，发卡行需要同时生成一个SM2公私钥对和一个RSA公私钥对，并且SM2公钥和RSA公钥都必须由支付系统认证中心签名，其生成的发卡行SM2公钥证书和RSA公钥证书都必须置于卡片中。如果支持DDA作为脱机数据认证方法，每张卡片都必须生成一对SM2公私钥对和一对RSA公私钥，并且ICC SM2公钥和ICC RSA公钥都必须由发卡行私钥签名，其生成的ICC SM2公钥证书相应的私钥和ICC RSA公钥证书相应的私钥也都必须包含在卡片中。

6.2.3 应用数据

有些应用数据可能对于某个发卡行的所有IC卡都通用，例如，对在单一国家内发行卡的发卡行来说，发卡行国家代码总是一样的。有些应用数据对IC卡是唯一的，例如，PAN或参考PIN。

6.3 记录格式

将IC卡应用数据传送到个人化设备的格式见《EMV卡个人化规范：2003》的2.6。

MAC—中国金融集成电路（IC）卡规范推荐安全等级设定是在EXTERNAL AUTHENTICATE命令中使P1=‘01’。EXTERNAL AUTHENTICATE后的所有被IC卡应用接收的命令包含一个C-MAC。

结束个人化处理

个人化设备应将最后一个STORE DATA命令的P1参数的b8设置为‘1’，以便表明应用个人化的完成。随着最后一个STORE DATA命令的结束，应用完成个人化，并且STORE DATA命令会被应用屏蔽掉。

中国金融集成电路（IC）卡借记/贷记应用并不要求使用数据分组‘7FFF’在最后一个STORE DATA命令中提出数据请求。

6.4 中国金融集成电路（IC）卡的数据分组

在中国金融集成电路（IC）卡借记/贷记应用的个人化数据被创建之后，它必须放入正确的分组。这些数据分组随后按照记录格式（见《EMV卡个人化规范：2003》的表7）被植入数据元‘ICC数据’。

数据分组的设计在个人化过程中承担着重要的作用。数据分组标识符（DGI）是两字节十六进制数。数据分组标识的第一个字节等于‘01’到‘1E’，表明数据存储的SFI。第二个字节表明SFI记录的记录

编号。其他那些第一个字节在此范围之外的所有数据分组标识都用于索引并不存储于SFI的数据，它们在JR/T 0025中定义，为JR/T 0025、支付系统和发卡行所用。

中国金融集成电路（IC）卡借记/贷记应用对于该约定的例外情况包括数据分组标识的‘0D01’和‘0E01’。这些数据分组标识中的数据，使用READ RECORD或UPDATE RECORD命令是无法访问的。根据具体实现的不同，卡片可能把数据元存储于这些数据分组标识中作为记录，也可能不存储。

中国金融集成电路（IC）卡借记/贷记应用由用于支持必要功能的基本最小数据集，和支持可选功能（对应用而言可能激活也可能没有）的附加数据集组成。用于支持基本支付服务所需的数据元包含于所有中国金融集成电路（IC）卡借记/贷记应用中。其它数据元根据发卡行对那些数据元支持功能的需求可能提供也可能没有。这些功能包括：

——授权控制（AuthC）；

——动态数据认证（标准 DDA 或 CDA）；

——静态数据认证（SDA）；

——脱机 PIN ；

——卡片联机/发卡行认证（CAM/Isuth）；

——发卡行脚本，用于发布后更新。

中国金融集成电路（IC）卡借记/贷记应用建议的数据分组见表1。

表1　中国金融集成电路（IC）卡借记/贷记应用的数据分组标识符

数据分组标识	数据内容	特性	加密	外部访问
0101	2 磁道等价数据—表 2	最小数据	否	读及更新记录
0102	2 磁道等价数据（无持卡人姓名）—表 3	最小数据	否	读及更新记录
0103	持卡人证件数据—表 4	最小数据	否	读记录
0201	数据认证数据—表 5	SDA，DDA	否	读记录
0202	数据认证数据—表 6	SDA，DDA	否	读记录
0203	签名静态应用数据—表 7	SDA	否	读记录
0204	ICC 动态认证数据—表 8	DDA/PIN 编码	否	读记录
0205	ICC 动态认证数据—表 9	DDA/PIN 编码	否	读记录
02nn*[a]	重复的签名静态应用数据—表 10，表 11	SDA	否	读记录
02nn	重复的数据认证数据—表 12	DDA	否	读记录
0301	卡片风险管理数据—表 13	最小数据，CVM	否	读记录
0302	卡片风险管理数据—表 14	最小数据，SDA，CAM	否	读记录
0303	持卡人验证方式列表—表 15	CVM	否	读及更新记录
03nn*	重复的卡片风险管理数据—表 16	最小数据，CVM	否	读记录
0401	终端频度检查卡片数据—表 17		否	读及更新记录
0D01	卡片内部风险管理数据—表 18	AuthC	否	输入数据输出数据

0E01	卡片私有风险管理数据—表 19	AuthC	否	无
0E02	需锁定的应用—表 20	发行人脚本	否	无
0Enn	重复的私有风险管理数据—表 21	AuthC	否	无
9200	GENERATE AC 命令响应数据—表 22	CAM	否	产生 AC
注：阴影表示的那些数据分组的数据分组建议包含在签名静态应用数据（SAD）中。如果有任何数据元不包含在签名中，它们应该被置于数据分组标识0302或数据分组标识0303。这些数据分组标识不含SAD（非阴影区域）中的数据元。如果发卡行计划使用发卡行脚本处理更新CVM列表，数据分组标识0303必须包含CVM列表。				
[a] nn*表明存储在文件最后一条记录中，因为它是一个重复的数据元。				

在下面每一数据分组标识的数据元表（表2-表22）中，标题为‘要求’的列给出了对每一数据元的要求：

——M（必备）表明该数据元必须具备，可以通过使用 READ RECORD 命令访问，它们被提供给终端以便交易过程的继续进行；

——R（要求）表明该数据元必须具备，但如果没有接受到数据，终端设备不应该终止交易；

——C（条件）表明该数据元在某些条件下必须具备。关于这些条件的信息可以在中国金融集成电路（IC）卡借记贷记卡片规范中找到；

——O（可选）表明该数据元是可选择的。

表2　数据分组标识‘0101’的数据内容

要求	标签	数据元	长度	加密
M	57	2 磁道等价数据[a]	直到 19	不适用
R	5F20	持卡人姓名	2-26	不适用
R	9F1F	1 磁道自定义数据	可变	不适用
[a]这个域可能在末尾加上一个十六进制字符‘F’以保证整个字节。				

表3　数据分组标识‘0102’的数据内容

要求	标签	数据元	长度	加密
M	57	2 磁道等价数据[a]	直到 19	不适用
R	9F1F	1 磁道自定义数据	可变	不适用
[a]这个域可能在末尾加上一个十六进制字符‘F’以保证整个字节。				

表4　数据分组标识‘0103’的数据内容

要求	标签	数据元	长度	加密
M	9F61	持卡人证件号	直到 40	不适用
M	9F62	持卡人证件类型	1	不适用

表5　数据分组标识‘0201’的数据内容

要求	标签	数据元	长度	加密
C	90	发卡行公钥（IPK）证书	可变	不适用

表6　数据分组标识‘0202’的数据内容

要求	标签	数据元	长度	加密
C	9F32	IPK 指数(使用 RSA 时)	1 或 3	不适用
C	92	IPK 余项(使用 RSA 时)	可变	不适用

C	8F	认证中心公钥索引	1	不适用

表7　数据分组标识‘0203’的数据内容

要求	标签	数据元	长度	加密
C	93	签名静态应用数据	可变	不适用

表8　数据分组标识‘0204’的数据内容

要求	标签	数据元	长度	加密
C	9F46	ICC 公钥证书	可变	不适用

表9　数据分组标识‘0205’的数据内容

要求	标签	数据元	长度	加密
C	9F47	ICC 公钥指数(使用RSA 时)	1 或 3	不适用
C	9F48	ICC 公钥余项(使用RSA 时)	可变	不适用
C	9F49	DDOL	可变	不适用

表10　数据分组标识‘02nn’的数据内容（重复 SAD）

要求	标签	数据元	长度	加密
C	‘93’	签名静态应用数据（SAD）	可变	不适用

表11　数据分组标识‘02nn’的数据内容（重复数据认证数据）

要求	标签	数据元	长度	加密
C	‘90’	发卡行公钥（IPK）证书	可变	不适用
C	‘8F’	认证中心公钥索引	1	不适用

表12　数据分组标识‘02nn’的数据内容（重复数据认证数据）

要求	标签	数据元	长度	加密
C	‘9F32’	IPK 指数(使用RSA 时)	1 或 3	不适用
C	‘92’	IPK 余项(使用RSA 时)	可变	不适用

表13　数据分组标识‘0301’的数据内容

要求	标签	数据元	长度	加密
M	5A	应用主账号（PAN）	可变	不适用
O	5F34	应用 PAN 序列号	1	不适用
R	8E	持卡人验证方法（CVM）列表	可变	不适用
M	9F0D	IAC—缺省	5	不适用
M	9F0E	IAC—拒绝	5	不适用
M	9F0F	IAC—联机	5	不适用
M	5F24	应用失效日期	3	不适用
C	5F28	发卡行国家代码	2	不适用
O	9F07	应用使用控制	2	不适用
O	5F25	应用生效日期	3	不适用
C	9F4A	SDA 标签列表	可变	不适用
M	8C	卡片风险管理数据对	可变	不适用

		象列表 1（CDOL1）		
M	8D	CDOL2	可变	不适用

注： 这一分组中的数据元包含在签名应用数据（SAD）中。如果发卡行使用脚本处理更新持卡人验证方法（CVM）列表，或使用多CVM列表和一单独的SAD，则CVM列表应该包含在数据分组标识0303而不是在数据分组标识0301中。

表14 数据分组标识‘0302’的数据内容

要求	标签	数据元	长度	加密
C	97	TDOL	可变	不适用
O	9F05	应用自定义数据	可变	不适用
O	9F0B	持卡人姓名扩展（27-45）	可变	不适用
C	9F44	应用货币指数	1	不适用
C	9F42	应用货币代码	2	不适用
O	5F30	服务码	2	不适用
M	9F08	应用版本号	2	不适用

表15 数据分组标识‘0303’

要求	标签	数据元	长度	加密
C	8E	持卡人验证方法（CVM）列表	可变	不适用

表16 数据分组标识‘03nn’的数据内容

要求	标签	数据元	长度	加密
C	5A	应用主账号（PAN）	可变	不适用
C	5F34	应用 PAN 序列号	1	不适用
R	8E	持卡人验证方法（CVM）列表	可变	不适用
C	9F0D	IAC—缺省	5	不适用
C	9F0E	IAC—拒绝	5	不适用
C	9F0F	IAC—联机	5	不适用
C	5F24	应用失效日期	3	不适用
C	5F28	发卡行国家代码	2	不适用
C	9F07	应用使用控制	2	不适用
C	5F25	应用生效日期	3	不适用

注： 如果要求多于一个SAD，则本分组中的数据元必须包含在签名应用数据（SAD）中。

表17 数据分组标识‘0401’的数据内容

要求	标签	数据元	长度	加密
O	9F14	连续脱机交易下限（终端频度检查）	1	不适用
O	9F23	连续脱机交易上限（终端频度检查）	1	不适用

表18 数据分组标识‘0D01’的数据内容

要求	标签	数据元	长度	加密
C	9F58	连续脱机交易下限	1	不适用

		（终端频度检查）		
C	9F59	连续脱机交易上限（终端频度检查）	1	不适用
C	9F53	连续脱机交易限制，国际	1	不适用
C	9F72	连续脱机交易限制，国际（国家）	1	不适用
C	9F54	累计脱机交易金额限制	6	不适用
C	9F75	累计脱机交易金额限制（双重货币）	6	不适用
C	9F73	货币兑换因子	4	不适用
C	9F5C	累计脱机交易金额上限	6	不适用
C	9F4F	日志格式	可变	不适用

表19　数据分组标识‘0E01’的数据内容

要求	标签	数据元	长度	加密
C	9F51	应用货币代码	2	不适用
C	9F52	应用默认行为（ADA）	2	不适用
C	9F56	发卡行认证指示位	1	不适用
C	9F57	发卡行国家代码	2	不适用
C	9F76	第二应用货币代码	2	不适用

表20　数据分组标识‘0E02’的数据内容

要求	标签	数据元	长度	加密
C	不适用	AID FFF_1 AID FFF_2…AID FFF_nn	可变	不适用

表21　数据分组标识‘0Enn’的数据内容

要求	标签	数据元	长度	加密
C	9F52	应用默认行为（ADA）	2	不适用

表22　数据分组标识‘9200’的数据内容

要求	标签	数据元	长度	加密
M	9F10	发卡行应用数据	可变	不适用

6.5　个人化数据必须遵循的规则

如果发卡机构期望启用qPBOC功能，则卡片附加处理（9F68）必须被个人化至卡中。

如果CVM列表中存在脱机PIN的入口,则脱机PIN的值以及PIN尝试限制数应当被个人化至卡中,且PIN尝试计数器（9F17）的值应当能被GetData命令取回。

依据JR/T 0025.12，电子现金余额（9F79）的取得方式为GetData命令，故电子现金余额（9F79）不应当被写入可供终端用Read Record命令读出的记录中。

发卡机构应当发行支持DDA和/或CDA的卡片，不应发行仅支持SDA的卡片。

CDOL1和CDOL2应被放置在AFL中指明的参与脱机数据验证的记录中。

如果卡片上存在磁条，那么芯片中数据应当遵循下列规则：

——磁条 2 等效数据（57）中的主账号应当与磁条第 2 磁道数据中的主账号保持一致；
——磁条 2 等效数据（57）中的失效日期应当与磁条第 2 磁道数据中的失效日期保持一致；
——磁条 2 等效数据（57）中的服务代码应当与磁条第 2 磁道数据中的服务代码保持一致；
——应用主账号（5A）应当与磁条第 2 磁道数据中的主账号保持一致；
——应用失效日期（5F24）的年月值应当与磁条第 2 磁道数据中的失效日期保持一致；
——服务码（5F30）应当与磁条第 2 磁道数据中的服务代码保持一致。

在任何情况下，AFL与数据分组的设计，必须同时遵循下列规则：
——同一笔交易，同一条记录同一个数据元应只出现一次；
——同一笔交易，不同的记录中同一个数据元应只出现一次；
——同一笔交易，GPO 响应中已经返回的数据不应在读记录时再次返回。（特别注意的是，包括但不仅限于 qPBOC 脱机批准交易时的 5F34）。

7 中国金融集成电路（IC）卡借记贷记应用需求

如要保证对中国金融集成电路（IC）卡借记/贷记应用进行个人化时能使用此通用个人化方法，以下要求必须满足：

a) 中国金融集成电路（IC）卡借记/贷记应用必须满足在《EMV 卡个人化规范：2003》中规定的所有要求；
b) 中国金融集成电路（IC）卡借记/贷记应用必须满足 JR/T 0025.5 中规定的所有要求；
c) 中国金融集成电路（IC）卡借记/贷记应用必须将 JR/T 0025.5 中强制规定的所有数据个人化。

8 安全规范

8.1 安全综述

在中国金融集成电路（IC）卡个人化的过程中，每一个步骤都有其特定的安全要求。现就各方面的要求，制定出以下的规范。

关于加密方式，根据JR/T 0025.7或JR/T 0025.17所提出的方式来对数据进行加密。

8.2 初始化安全

密钥数据（KEYDATA）必须按表23设置，该数据由KMCID和芯片序号（CSN）组成。KMCID是个人化主密钥标识符，应由发卡行或个人化厂商提供。KMCID的长度为6个字节。CSN是IC卡片物理标识符最右边的4个字节。

表23 KEYDATA 的初始存储内容

字段	长度	格式
KMC（例如 IIN/BIN，左对齐，用 1111b/半字节填充）标识	6	BCD
芯片序列号（CSN）	4	二进制数

KEYDATA（密钥数据）是每个IC卡应用分区都可以访问的一个数据单元，KMCID是INITIALIZE UPDATE命令响应数据的一部分，并给定位IC卡发行商的KMC提供了方便。

在IC卡上必须存在‘个人化主密钥（KMC）’的版本号，这个主密钥用来为每个应用生成初始的个人化密钥（K_{ENC}、K_{MAC}和K_{DEK}）。

必须为每张IC卡生成一个加密分散密钥（K_{ENC}），并把它写入相应的应用中。这个密钥用来生成IC卡密文和验证主机密文。如果密文的安全等级要求STORE DATA命令的数据字段是加密的，这个分散密钥还用来在CBC模式下对该命令的数据字段进行解密。

如果使用双长度DES密钥，K_{ENC}是一个16字节（112比特加奇偶校验位）的DES密钥。

K_{ENC}密钥用以下方法推算：

K_{ENC} ：= DES3（KMC）[KEYDATA的6个最低有效字节||‘F0’||‘01’]||DES3（KMC）[KEYDATA的6个最低有效字节||‘0F’||‘01’]。

必须为每张IC卡生成一个校验码分散密钥（K_{MAC}）并写入相应的IC卡。这个密钥用来校验EXTERNAL AUTHENTICATE命令使用的C-MAC。同时当STORE DATA命令的密文安全级要求命令中的数据采用MAC时，这个密钥也用来校验STORE DATA命令使用的C-MAC。

K_{MAC}是一个16字节（112比特加奇偶校验位）的DES密钥。

K_{MAC}应采用以下方法导出：

K_{MAC}：=DES3（KMC）[KEYDATA的6个最低有效字节||‘F0’||‘02’]||DES3（KMC）[KEYDATA的6个最低有效字节||‘0F’||‘02’]。

必须为每张IC卡生成一个密钥加密分散密钥（K_{DEK}）并将它写入相应的IC卡。这个密钥用来在ECB模式下对STORE DATA命令收到的机密数据进行解密。

K_{DEK}是一个16字节（112比特加奇偶校验位）的DES密钥。

K_{DEK}应采用以下方法导出：

K_{DEK}：=DES3（KMC）[KEYDATA的6个最低有效字节||‘F0’||‘03’]||DES3（KMC）[KEYDATA的6个最低有效字节||‘0F’||‘03’]。

如果使用SM4算法，K_{ENC}是一个16字节的SM4密钥。

K_{ENC}密钥用以下方法推算：

K_{ENC} ：= SM4（KMC）[KEYDATA的6个最低有效字节||‘F0’||‘01’]||SM4（KMC）[KEYDATA的6个最低有效字节||‘0F’||‘01’]。

必须为每张IC卡生成一个校验码分散密钥（K_{MAC}）并写入相应的IC卡。这个密钥用来校验EXTERNAL AUTHENTICATE命令使用的C-MAC。同时当STORE DATA命令的密文安全级要求命令中的数据采用MAC时，这个密钥也用来校验STORE DATA命令使用的C-MAC。

K_{MAC}是一个16字节的SM4密钥。

K_{MAC}应采用以下方法导出：

K_{MAC}：=SM4（KMC）[KEYDATA的6个最低有效字节||‘F0’||‘02’]||SM4（KMC）[KEYDATA的6个最低有效字节||‘0F’||‘02’]。

必须为每张IC卡生成一个密钥加密分散密钥（K_{DEK}）并将它写入相应的IC卡。这个密钥用来在ECB模式下对STORE DATA命令收到的机密数据进行解密。

K_{DEK}是一个16字节的SM4密钥。

K_{DEK}应采用以下方法导出：

K_{DEK}：=SM4（KMC）[KEYDATA的6个最低有效字节||‘F0’||‘03’]||SM4（KMC）[KEYDATA的6个最低有效字节||‘0F’||‘03’]。

必须把IC卡响应INITIALIZE UPDATE命令时返回来的序列计数器初始化为‘0001’。

8.3 密钥定义

8.3.1 个人化密钥描述

个人化密钥见表24所示。

表24 个人化密钥描述

密钥名称	密钥共享	用途	主密钥	卡密钥	对话密钥
发卡行主密钥	发卡行、IC卡厂商和个人化设备	IC卡厂商使用这个KMC生成卡片级密钥（K_{ENC}、K_{MAC}、K_{DEK}），并将它们写到卡上。	KMC		
		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_{ENC}	SKU_{ENC}

		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_{MAC}	SKU_{MAC}
		用来创建一个对话密钥，利用该对话密钥可在 ECB 模式下加密对称密钥或灵活的加密其它机密数据。		K_{DEK} 数据加密密钥	SKU_{DEK}
发卡行密钥交换密钥	发卡行和数据准备设备	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。	KEK_{ISS}		
数据加密密钥/传输密钥	数据准备设备和个人化设备	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，用于保护对称密钥。	DEK/TK		
MAC 密钥（校验码密钥）	在个人化数据文件中，由数据准备设备向个人化设备提供	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。	MAC 密钥	不适用	不适用

8.3.2 中国金融集成电路（IC）卡借记/贷记应用密钥描述

借记/贷记应用密钥见表25所示。

表25 中国金融集成电路（IC）卡借记/贷记应用密钥描述

密钥名称	密钥共享	用途	主密钥	卡密钥	对话密钥
借记/贷记应用联机验证密钥	发卡行和卡	主密钥用来生成唯一的卡片密钥，用于卡片和发卡行进行联机验证。	MDK	UDK	SUDK（用于通用密文）
借记/贷记应用信息认证密钥	发卡行和卡	主密钥用来生成唯一的卡片密钥，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 MDK	MAC UDK	SUDK MAC
借记/贷记应用数据加密密钥	发卡行和卡	主密钥用来生成唯一的卡片密钥，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 MDK	ENC UDK	SUDK ENC
ICC 私钥	发卡行和卡	由发卡行生成并安全地存储在卡上。在脱机数据验证（DDA）处理过程中，用这个私钥对动态数据进行数据签名。个人化完成以后，发卡行通常不持有该密钥。			

密钥用途如图 1 所示。

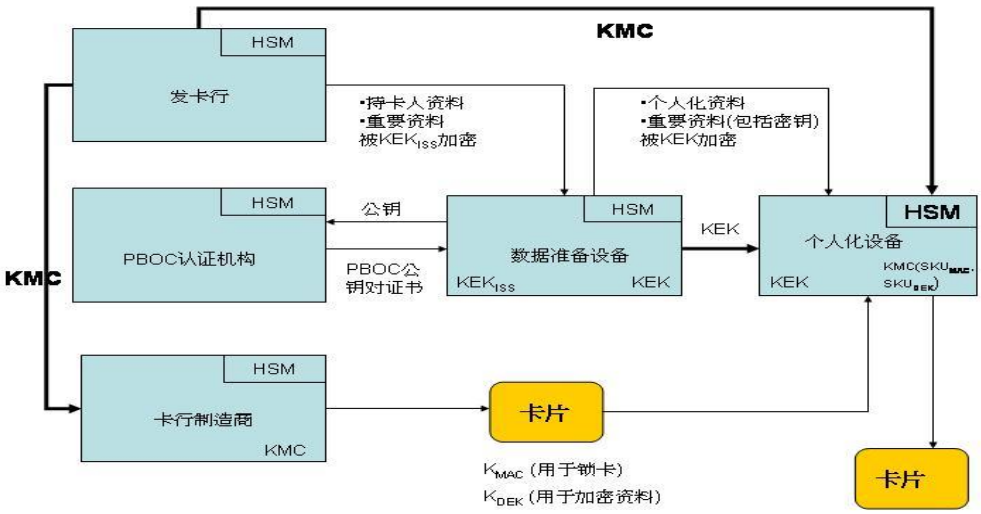

图1　密钥用途

8.4　管理要求

8.4.1　环境

8.4.1.1　创建安全数据的环境要求

见各支付组织的相关个人化安全和质量管理要求。

8.4.1.2　安全数据的产生

开始进行个人化之前，必须创建相应的加密密钥，这些密钥可以由发卡行创建，也可以由个人化厂商创建。如果由个人化厂商创建，必须按本部分的规定进行。

至少应生成以下的密钥：

a) 发卡行主密钥（KMC）：用来派生 K_{MAC}、K_{ENC} 和 K_{DEK} 三个密钥。

- K_{MAC}——用来锁闭中国金融集成电路（IC）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。

b) 主密钥（MDK）——用来导出：UDK——用于联机的卡认证和发卡行认证。

就每个BIN（银行标识码）而言，MDK通常是唯一的，而UDK对每张卡都必须是唯一的。

c) 发卡行公私钥对——通常由发卡行生成，公钥应传输给中国金融集成电路（IC）卡认证机构，供其创建发卡行公钥证书。私钥被保存在发卡行的 HSM（主机加密模块）内。

d) 密钥交换密钥（KEK）——用来对发卡行个人化输入文件中的机密数据进行加密，每个发卡行的 KEK 必须是唯一的。

e) 传输密钥（TK）——用来对数据准备系统向个人化系统传送的发卡行个人化输入文件中的机密数据进行加密。

作为选择，也可以用发卡行公私钥对生成这些密钥。

f) ICC 公私钥对——IC 卡利用这一对密钥执行 DDA 和 CDA/AC 密文生成算法。其中，公钥须经过发卡行私钥的签名，才能获得发卡行公钥证书。

每张卡的ICC公私钥对必须是独一无二的。

g) MDK ENC——用来导出：UDK ENC——用来加密发卡行的脚本机密信息。

h) MDK MAC——用来校验发卡行的脚本信息。

MDK EC和MDK MAC至少对于每个BIN是独一无二的，而UDK ENC 和 UDK MAC必须对每张卡都是唯一的。

如果发卡行生成自己的密钥，就必须创建ZMK，以便联机传输这些密钥。

在IC卡之外执行的一切加密和解密操作必须在HSM上进行。

密钥区

一般说来，个人化过程有三个密钥区：在发卡行和数据准备系统之间有一个密钥区，在数据准备系统和个人化设备之间有一个密钥区，在个人化设备和卡片之间还有一个密钥区，如图2所示。

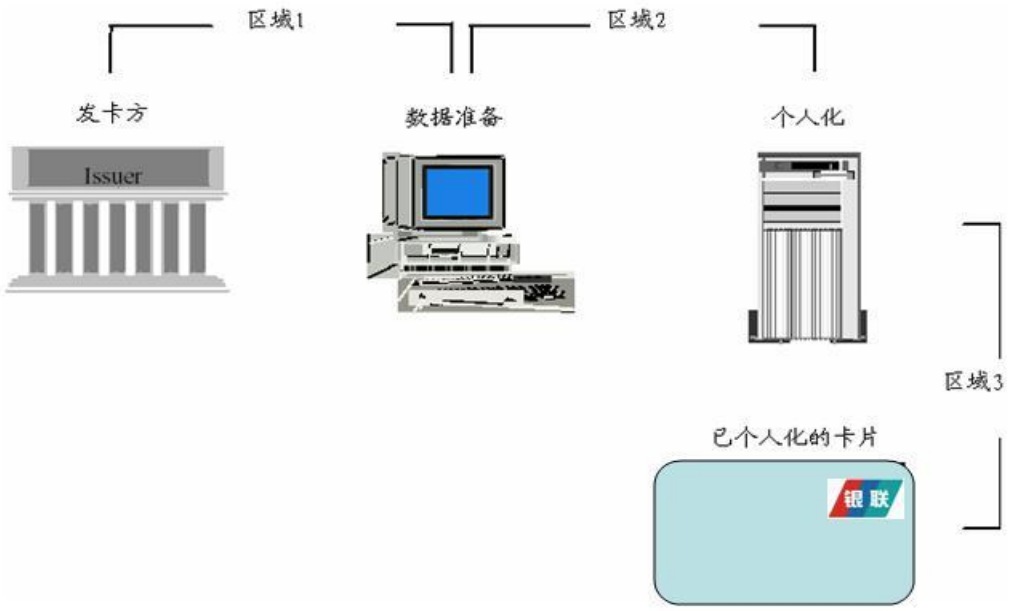

图2　密钥区

在发卡行和数据准备系统之间的密钥区里，建有一个通称为KEK（密钥交换密钥）的加密密钥，采用该密钥对中国金融集成电路（IC）卡的安全信息进行加密。

该密钥可以由发卡行生成，也可以由个人化设备生成，但必须遵循本部分的要求。除了这些要求以外：

——KEK 对每个发卡行必须是独一无二的；

——KEK 至少必须逐年进行更改。

接收来自发卡行的机密数据时，必须把KEK密钥置换成TK（传输密钥），以便在数据准备过程和个人化设备之间对机密数据进行加密。

该密钥必须独特于其它所有密钥，并且只承担加密机密数据的任务。

个人化设备接收这些机密数据时，机密数据必须从TK变换成IC卡的K_{DEK}，然后通过个人化过程被传送给IC卡，再由IC卡对它们进行解密和存储。

8.4.1.3　银行客户资料到个人化数据的安全流程

接收来自发卡行的个人化文件时，文件信息必须：

——始终得到安全的存储，访问这些信息的权利必须严格地局限于业务需求者；

——在成功完成个人化之后，将生产系统内的数据清除干净。

另外，机密信息必须：在HSM上从KEK解译成TK，以便将机密信息向前传输给个人化设备。

此外，数据准备系统至少必须：位于一个能够控制数据存取的中间安全区，并将数据访问权局限于业务需求者。

8.4.1.4 数据组的安全要求

加密过程的安全要求应适合于给定的数据组及IC卡用途，而且无论是在数据准备过程中，还是在个人化设备相关的本机处理过程中，都必须与相应的加密过程协调一致。

8.4.1.5 个人化过程中的安全要求

在个人化阶段，个人化设备必须：

——在 HSM 上执行本部分定义的 K_{DEK} 推算过程；

——将个人化文件中的机密信息从传输密钥 TK 解译成 K_{DEK}，以便将其传送给卡片。这一解译过程必须在 HSM 上执行。

另外，个人化设备必须安装在工厂的高安全区并符合各支付组织的相关生产安全标准规定的一切安全要求和程序要求。

8.4.2 操作

8.4.2.1 密钥的形成与分发

不同类型的加密算法支持《EMV卡个人化规范：2003》中的不同功能。然而，当加密算法没有得到正确实施时，加密算法的预定作用将受到负面的影响。一种安全的实施将取决于规范所需的不同密钥被签发者管理的好坏程度。以下材料的目的是提供不同算法类型所扮演的加密角色的一个概述，以及提出安全地管理密钥所必需的基本要求。

a） 非对称（SM2/RSA）密钥管理

IC卡的安全性取决于私钥（签名）的保护。不能保证用来对静态或动态数据元签名的私钥的安全性将使IC卡面临被伪造的风险。私钥面临的主要风险包括：

——成功地解决 ECDLP 问题，以及成功地分解 RSA 模数；

——私钥自身的泄漏。

为了限制这些风险所代表的潜在的泄露问题，我们推荐使用以下发卡行要求。

私钥（签名）的安全性取决于许多因素，包括：

——SM2/RSA 密钥模数位的长度，例如：256 或者 1024 和 1152；

——组成公钥/私钥模数的主要数字的质量；

——用来从物理上保障（保护）私钥（签名）不受未经授权的访问和暴露/危害的影响的方法，特别是当 IC 卡或其它安全加密设备（SCD）使用它们时为密钥提供的保护。

SM2/RSA密钥生成

当生成SM2/RSA公私钥对时，推荐在一台物理安全的设备的受保护内存中完成这个过程。这种设备必须包含一个随机或伪随机数字生成器，执行原始校验例程，并支持篡改响应机制。

——SM2/RSA 私钥（签名）可能对物理安全设备而言是暂时性的；

——密钥生成将利用一个随机或伪随机过程，以使得不可能预测出任何密钥或者确定密钥空间中的某些密钥比其它任意密钥可能性更大；

——个人计算机或其它类似的不安全设备，即不被信任的设备，将永远不能用来生成 SM2/RAS 公私钥对。

密钥传输和存储

为了保护公私钥对的完整性，对发卡行而言，确保这种密钥数据使用以下步骤非常重要：

——公钥应能被确保安全以及用一种能够保证它们完整性的方式来传输。推荐公钥始终在诸如一个证书之类的数据结构中传输，或者可以跟一个报文鉴别码（MAC）来保证完整性，这个报文鉴别码是由一个仅用于该用途的密钥按照 ISO 9807 定义的算法应用于公钥和相关数据而得。也推荐使用双重控制技巧来确保公钥的接收方有办法验证它的发送方和完整性，即通过公钥上的一个校验值的单独和独立的传输来实现这一点；

——私钥必须用一种能够保证它们的完整性和私密的方式来保障安全和传输。传输机制可能包括：

- 一台安全加密设备；
- 利用至少与加密相等力量的对称算法来对被保护密钥的私钥进行解密；
- 作为几个部分（在 IC 卡上保障安全），并使用一个对称算法来进行解密。

b） 对称密钥管理

JR/T 0025中的对称密钥用于特殊的事务功能。对称密钥是在个人化期间从一个主导出密钥（Master Derivation Key）中导出的。最终的卡片级密钥是唯一的。

发卡行主密钥包括：

——发卡行主导出密钥（IDKAC）：用来导出卡片密钥，该密钥用于生成称为应用密文（AC）的 MAC；

——发卡行安全报文主密钥（IMKSMC IMKSMI）：用来导出卡片密钥，这些卡片密钥用在卡片和验证系统之间的安全报文中，即卡片锁定、应用锁定/解锁、更新卡片特定数据和修改 PIN。

密钥生成

发卡行将使用以下原则来使密钥数据在创建期间泄漏的机会最小化：

——在生成密钥时，它们必须要么在一台由篡改响应机制保护的物理安全的设备中生成，要么必须由授权的工作人员以一部分一部分的形式生成（见下文）。设备必须包含一个随机或伪随机的数字生成器；

——任何时候一个未被保护的密钥都不能存在于一台物理安全的设备的被保护内存之外。任何时候物理安全的设备都不能输出纯文本的密钥，除非作为密码或者以两个或更多部分的形式输出；

——当密钥由授权工作人员通过一个将各部分组合的过程来生成时，必须要求每一方生成一个和要生成的密钥一样长的部分。密钥组合过程在一个物理安全的设备内部进行。此外，组合各部分的方法应当是，知道了各部分的任何一个子集也无法知道密钥值。分开的密钥由一个管理机构掌握，至少应有一个部分持有人是发卡行的一名员工；

——应当为实际密钥的全部计算校验位；

——个人电脑或类似的不安全设备永远不能用来生成密钥资料；

——如果发现任何密钥存在于一个物理安全的设备之外，或者密钥的各个部分被人所知，或者有被单个人掌握的嫌疑，那么该密钥将被认为已被泄漏，并且必须用一个新的密钥来替换它。

密钥传输和存储

对称密钥可能需要被传输和存储。例如包括将对称密钥从发卡行的站点传输给一个第三方的处理商或卡片个性化供应商。当对称密钥正被传输或存储时，以下措施将限制数据泄漏的潜在危险：

——对称密钥可以被安全地转移到一块安全令牌或智能卡的保护之下，以进行传输和存储；

——对称密钥只能以以下方式在安全令牌或智能卡的受保护内存之内进行传输或存储：

利用双重控制和分持机密的原则，以两个或更多部分的形式作为密码，密码是用一个由各方安全地建立的传输或存储密钥来创建的。

8.4.2.2 根密钥明文数据的保存

根密钥明文数据的保存要求如下：

a） 一旦接收到密钥资料，负责的密钥管理人员必须立即检查邮包是否篡改，并且必须验证内容；

b） 如果接收的管理人员对密钥数据的完整性有任何不确定的地方，必须立即通知发送方。发送方与接收方商议决定密钥数据将来的状况。关于继续使用密钥资料的任何决定的基础必须记录在案并由双方保留；

c） 如果硬拷贝数据要保留任意一段时间，那么各个硬拷贝组成部分、安全令牌或智能卡必须保存在一个序列化的保密信封中；

d) 这个序列化的保密信封必须持续保存在一个物理安全的容器中，这个容器仅能由指定的密钥管理人员或预备人员访问。每次对密钥数据的访问都必须记入日志，包括时间、日期、信封序列号、目的和签名。这些日志将可以向任何相应的请求机构提供；

e) 密钥资料永远不能在超过任务所需的访问必需的时间之后保留在保密信封和它们的物理安全的环境之外。

8.4.2.3 其他密钥数据的保存

下面给出了关于密钥存储问题的一些一般的指导，它适用于非对称和对称密钥存储：

a) PC板的使用

一块向主机提供加密服务的 PC 板可以看作是 HSM 的一种形式和类似的期望保护级别。

注： 使用加密安全设备的主要原因是保护密钥。如果使用HSM主机的系统自身是不安全的，那么攻击者将更容易危害系统的软件功能，而忽略HSM。

b) 访问控制

所有在卡外和HSM外保存的密钥都应当保持在至少双重的控制之下。

c) HSM 和 IC 安全内存

一般而言，HSM将包含单独的存储和处理设备，而密钥资料将跨内部硬件总线传送。由于这个原因，当检测到了危害时，HSM清除（或归零）它的内存是很重要的。此外，HSM的硬件设计解决电磁辐射的问题也很重要。HSM一般设计位于一个安全的环境之中。

8.4.2.4 操作流程

发卡行在发卡之前必须执行以下几个步骤，这些步骤有时还需要在使用支付系统的过程中得以执行：

a) 生成发卡行密钥对

发卡行必须安全地生成并保存一对或几对公钥和私钥。私钥将被用来签署IC卡静态数据或IC卡公钥证书（这取决于IC卡各自执行的数据认证是静态的还是动态的）。在支付模式允许的情况下，建议发卡行为每个银行标识码（BIN）或首标分配不同的密钥对，这样，一旦发卡行的私钥被泄密，就可以把相应的BIN锁闭起来。

b) 生成发卡行密钥

发卡行必须根据IC卡密钥的推算需要而安全地生成并保存一个或几个密钥。

c) 接收“CA 公钥（PBOC Public Key）”

发卡行必须接收并安全地保存一个或几个CA公钥。这些公钥必须以一定的方式进行传输，使发卡行能够对它们的完整性和数据源进行核实。CA公钥将用来验证发卡行公钥证书。

d) 请求并接收发卡行公钥证书

就发卡行公钥而言，发卡行必须获得相应的发卡行公钥证书。为此，须将每个发卡行公钥传输给CA认证机构（PBOC CA），继而发卡行会收到发卡行的公钥证书。发卡行公钥必须以一定的方式传输给CA认证机构，使之能够对公钥的完整性和数据源进行核实。接收CA认证机构发来的公钥证书时，发卡行可以采用CA公钥对证书进行验证。

e) 传输“发卡行加密密钥”

如果发卡行希望授权给第三方生成和验证IC卡密码，发卡行必须将推算IC卡密钥所使用的发卡行加密密钥安全地传输给第三方。

8.4.3 管理规范

8.4.3.1 人员管理

负责管理加密密钥和密钥要素及其它密钥数据设备的人员必须由不同的参与方（即发卡行、第三方处理商和/或IC卡个人化厂商）指派。

指派专人负责监控密钥数据时，必须落实足够的保密控制措施，以保证任何个人或未经认可的个人没有任何机会读取密钥的数据成分。

密钥保管人必须是正式受托的职员，决不可以是临时佣工或顾问。

另外，为了确保服务的连续性，可以把候补人员当作主要密钥管理人的“备份”。选择“备份”管理人的标准应该和选择主要密钥管理人的标准相同。

密钥管理人的责任重大，而且是发卡行安全协议的一个基本组成部分，他们所要管理的密钥数据是发卡行发卡程序中最重要的加密操作码。每个发卡行应对内部密钥管理程序和下列业务的有关人员的作用进行核查：

a） 密钥管理人员的职责包括密码资料的控制、验证和安全存储；

b） 密钥管理人或其“备份”的责任是：

- 接收和安全存储密钥元；
- 对读取和使用密钥数据的记录或日志进行管理，包括读取次数、日期、目的和重新安全存储情况；
- 对传输给发卡行控制权限以外的其它所有指定人员的密钥数据进行验证；
- 对过期密钥元的销毁进行签名作证；
- 时常根据需要将密钥数据输入安全加密模块；
- 依据数据所有人的通知，指导和监视过期密码资料的销毁。

c） 密钥数据最初生成时的密钥管理人，应负责保护该数据，并将其转发给接收单位的指定密钥管理人，这个责任还包括对数据收讫进行验证。

8.4.3.2 操作管理

参见各支付组织的相关个人化安全和质量管理要求。

8.4.3.3 文档管理

a） 数据传输安全管理

参见各支付组织的相关个人化安全和质量管理要求。

b） 数据存储介质的管理

参见各支付组织的相关个人化安全和质量管理要求。

c） 数据信息使用的控制

参见各支付组织的相关个人化安全和质量管理要求。

8.5 安全模块

防止篡改的要求：篡改的防止可以分为物理和逻辑两个安全领域。

8.5.1 物理安全属性

物理安全包括以下属性：

——对侵入的保护，包括擦除敏感数据；

——对将导致敏感信息暴露的未授权修改的保护；

——防止对设备运转带来的电磁辐射的监控的保护。

8.5.2 逻辑安全属性

逻辑安全特性包括以下属性：

——真实性的验证；

——设备功能集的设计确保没有单个或设备功能的组合将导致敏感信息的泄露；

——存在的、用来确保密钥分割的机制；

——敏感状态操作需要双重控制；

——包含的用来验证软件下载的技巧。

8.5.3 功能需求

一个HSM的最小的需求应围绕着对以下内容的支持：

——密钥值生成；

——密钥值交换；

——密钥配置文件分离（逻辑分割密钥属性）；

——密钥值输出和输入；

——密钥值的安全存储。

8.5.4 安全模块等级

HSM须符合国家制订的法规。

8.6 风险审计

在每个IC卡应用的个人化过程的最后，必须创建这个应用的个人化过程的记录。在整个个人化过程的最后，必须创建包含所有的IC卡应用的个人化过程纪录的审计文档。对每一张IC卡的审计文档的格式，见《EMV卡个人化规范：2003》表21。

这些记录可保证对个人化过程的可审计性和可跟踪性。

参考文献

[1] “银联”标识卡个人化企业安全和质量管理指南
[2] EMV卡个人化规范：2003