附录七.联网收费 IC 卡安全管理技术要求

目　录

1 总则

本技术要求是交通部公路联网收费技术要求的组成部分，适用于公路联网收费领域内应用的各种集成电路（IC）卡（包括非接触逻辑卡、非接触 CPU 卡、双界面 CPU 卡、PSAM 卡、ISAM 卡等）的选择、发行、管理和使用。

2 引用标准和参考资料

下列标准包含的条文，通过引用构成本规范的条文。凡是不注日期的引用文件，其最新版本适用于本技术要求。

(1) JR/T 0025-2005 《中国金融集成电路（IC）卡规范》
(2) GB/T 16649-1996 《识别卡 带触点的集成的电路卡》(ISO/IEC 7816)
(3) ISO/IEC 14443 《识别卡 — 非接触式集成电路卡 — 近耦合卡》
(4) ISO/IEC 9798-1997《信息技术 — 安全技术》

3 基本安全管理要求

3.1 IC 卡的安全要求

公路联网收费的 IC 卡选型首先要考虑 IC 卡的安全保密性能，其次针对具体应用考虑使用的方便、简单。

公路联网收费的 IC 卡的密钥安全体系以数据加密标准（DES）算法（包括 Triple-DES）为基础，以《中国金融集成电路（IC）卡规范》等要求为依据设计卡的安全体系。卡片中各文件的密钥应设计为一卡一密、一扇区一密，以防止整个应用系统的安全体系被攻破。

(1) 非接触逻辑加密卡因其安全性较低，只能作为通行券、身份卡、公务卡及月票卡等使用；
(2) 非现金支付卡（包括储值卡、记账卡等）应采用高安全性的 CPU 卡，包括非接触式 CPU 卡和双界面 CPU 卡，并符合《中国金融集成电路（IC）卡规范》的有关要求；
(3) IC 卡的各种密钥和密钥的算法应存放在安全存取模块（SAM，指 SAM 卡或 SAM 加密机）（包括 PSAM、ISAM 等）中，密钥和密钥的算法应无法从 SAM 模块中读出。系统的安全性是以 SAM 模块（密钥和算法）的安全为基础的。

3.2 IC 卡读写机具安全要求

IC 卡读写机具的数据存储、处理均应满足安全管理要求。为保证联网收费系统的安全性，IC 卡读写机具应支持一卡一密的各类卡片（非接触逻辑加密卡、CPU 卡等）的读写。所有 IC 卡读写机具中都应有负责安全控制管理的 SAM。SAM 的类型依赖于 IC 卡读写机具的交易类型,如用于支持消费交易的 SAM 称为 PSAM，用于支持充值交易的 SAM 称为 ISAM。SAM 卡应具有一定的通用性。

3.2.1 一般要求

IC 卡读写机具宜用同一 SAM 同时满足多种非接触 IC 卡（包括非接触逻辑加密卡、非接触 CPU 卡、双界面 CPU 卡等）读写控制时的安全需求。在不降低系统安全级别的前提下,基于 SAM 的非接触逻辑加密卡读写机具应能通过简单的软件升级实现对双界面 CPU 卡的读写。

IC 卡读写机具一般存在两种类型的数据：

(1) 通用数据：包括时间、终端识别号等数据，外界可以对这些数据进行访问，但不允许进行无授权的修改；
(2) 敏感数据：包括密钥、应用内部的参数（如 SAM 的标识号，密钥索引等），这类数据的控制需要通过外部认证操作实现，或者通过安全报文的方式实现。

3.2.2 通用数据安全要求

通用数据一般存储在 IC 卡读写机具的存储器中。在更新参数和下载新的应用程序时，IC 卡读写机具必须做到：

(1) 验证更新方的身份，对于应用程序重新下载，只允许 IC 卡读写机具制造厂商、IC 卡读写机具所有者或者有授权的第三方执行；
(2) 校验下载数据的完整性；
(3) 无论在什么情况下，IC 卡读写机具中的数据都不会随意改变和丢失，并保证数据有效。

3.2.3 敏感数据安全要求

所有敏感数据都存储在 SAM 中。

SAM 是一种能够提供必要的安全机制以防止外界对 IC 卡读写机具等设备所储存或处理的数据进行非法攻击的硬件加密模块。SAM 主要负责和处理所有的敏感数据，这些数据包括消费密钥或传输密钥等。

在正常的操作环境下，对 SAM 必须要求：出入模块的以及其内部存放和正在处理的数据不会由于模块自身或其接口造成任何泄露和改变。

3.2.4 安全存取模块的安全要求

SAM 的安全特性必须满足下列要求：

(1) SAM 任何部分的损坏或失效都不会导致敏感数据的泄露；
(2) SAM 应具有一定防窃、查窃机制和足够的防范特性，能够发现数据是否被篡改过；
(3) SAM 应能同时满足同一 IC 卡读写机具读写多种非接触 IC 卡（包括非接触逻辑加密卡、非接触 CPU 卡、双界面 CPU 卡等）时的安全需求。

3.2.5 安全存取模块的逻辑安全要求

SAM 的逻辑设计应保证：调用任何单一功能或组合功能，都不会导致敏感数据的泄露。对于某些敏感数据操作，应有一定的权限限制。

SAM 中可以存放多组不同版本不同索引的主密钥。所有的主密钥通常必须在 IC 卡读写机具使用之前被下装到安全存取模块中。如果在使用过程中，主密钥需要修改，则必须使用安全报文。要实现这一过程通常必须在特殊的授权情况下完成。外部不能存在任何取得密钥的机会。

为避免伪操作，存放在 SAM 中的不同类型的主密钥必须与不同特定的应用操作相结合。

SAM 应能实现对称密钥算法（DEA）和符合本规范定义的主密钥到子密钥的分散算法。

本技术要求中定义的 SAM 宜采用 CPU 卡或加密机的方式来实现。

3.3 安全存取模块的安全管理要求

3.3.1 安全存取模块的安全应用基本原则

(1) SAM 的选型

SAM 的选型首先要考虑其安全保密性能，且应同时能支持多种 IC 卡（非接触逻辑加密卡、CPU 卡等）的需求；其次针对具体应用考虑使用的方便、简单。

(2) 安全原则

SAM 的密钥安全体系以 DES 算法为基础，并符合《中国金融集成电路（IC）卡规范》的有关要求。

与应用有关的密钥和数据存放在 SAM 中，密钥和密钥的算法应无法从 SAM 中被读出。系统的安全性是以 SAM 模块（密钥和算法）的安全为基础的。

3.3.2 基于 DES 的 SAM 应用安全算法描述

(1) DES 加密算法

DES 算法应遵循有关国际标准。IC 卡应支持 Single DES、Triple DES 密码算法，密钥长度分别是 8 和 16 个字节。DES 属于对称加密算法，加密和解密密钥相同。

① Single DES 算法

Single DES 算法是指使用单长度（8 字节）密钥 K 对 8 字节块的输入数据 X_1，X_2，X_3…加密，得到 8 字节块的输出数据 Y_1，Y_2，Y_3…。

其中，

$Y_I = DES(K)[X_I]$

解密方式如下：

$X_I = DES^{-1}(K)[Y_I]$

② 3DES 算法（Triple DES 算法）

3DES 算法是指使用双长度（16 字节）密钥 K＝（$K_L||K_R$）将 8 字节明文数据块加密成密文数据块，如下所示：

$Y = DES(K_L)[DES^{-1}(K_R)[DES(K_L[X])]]$

解密的方式如下：

$X = DES^{-1}(K_L)[DES(K_R)[DES^{-1}(K_L[Y])]]$

(2) 密钥分散算法

为了使应用系统在使用对称加密算法时获得最大的安全性，应当使每张卡片密钥在系统中具有唯一性，即卡片密钥 ＝ 主密钥对特定数据（分散代码）进行分散的结果。

对于 Single DES 主密钥，分散方法参见图 1。

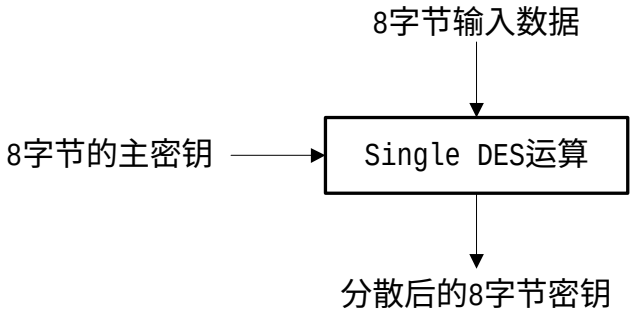

图 1：Single DES 密钥分散

对于 Triple DES 主密钥，分散方法参见图 2。

左边的 8 字节输入数据 ＝ 特定数据；

右边的 8 字节输入数据 ＝ 特定数据按位求反；

图 2：Triple DES 密钥分散

此时，终端必须知道此主密钥。

(3) 过程密钥生成算法

过程密钥是由指定密钥对可变数据加密产生的单倍长密钥。过程密钥产生后只能在某一（消费、取现等）过程中有效。图 3 描述了产生过程密钥的机制，其中输入数据是 8 字节。

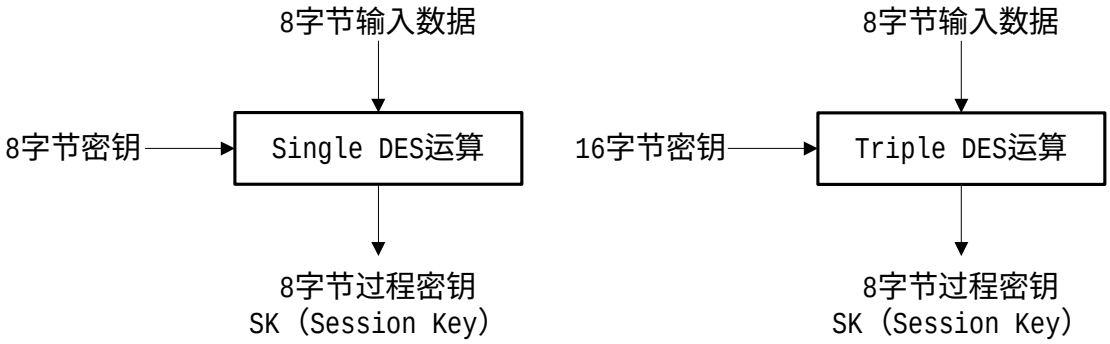

图 3：过程密钥的产生

(4) MAC 的计算

MAC 是使用命令的所有元素（包括命令头）产生的。一条命令的完整性，包括命令数据域（如果存在的话）中的数据元，通过安全报文传送得以保证。

MAC 总是命令或命令响应数据域中最后一个数据元素。在公路联网收费应用中规定 MAC 的长度总是 4 个字节。

应按照如下的方法使用三重或单重 DES 加密方式产生 MAC。

第一步：收费终端向用户 CPU 卡发出取随机数指令，从用户 IC 卡中取得 4 字节的随机数。然后在该随机数的后面补 4 字节 16 进制的“00”，所得到的 8 字节结果作为 MAC 计算初始值。

第二步：按照顺序将以下数据连接在一起形成数据块：

① 命令报文：CLA，INS，P1，P2，Lc＋4，DATA

② 必须置 CLA 的后半字节为‘4’

③ 在命令的数据域中（如果存在）包含明文或加密的数据

第三步：将该数据块分成 8 字节为单位的数据块，标号为 D1，D2，D3，D4 等，最后的数据块有可能是 1-8 个字节。

第四步：如果最后的数据块长度是 8 字节的话，则在其后加上 16 进制数字‘ 80 00 00 00 00 00 00 00 ’，转到第五步。

如果最后的数据块长度不足 8 字节的话，则在其后加上 16 进制数字‘ 80 ’，如果达到 8 字节长度，则转入第五步；否则在其后加入 16 进制数字‘ 0 ’直到长度达到 8 字节。

第五步：对这些数据块使用相应的密钥进行加密。（有关密钥由中国金融 PSAM 卡专用密令所制定）

① 如果该密钥长度为 8 字节，则依照图 4 的方式来产生 MAC（根据在第三步中产生的数据块的长度不同，又可能在计算中会多于或少于三步）。

② 如果该密钥长度为 16 字节，则依照图 5 的方式来产生 MAC（根据在第三步中产生的数据块的长度不同，又可能在计算中会多于或少于三步）。

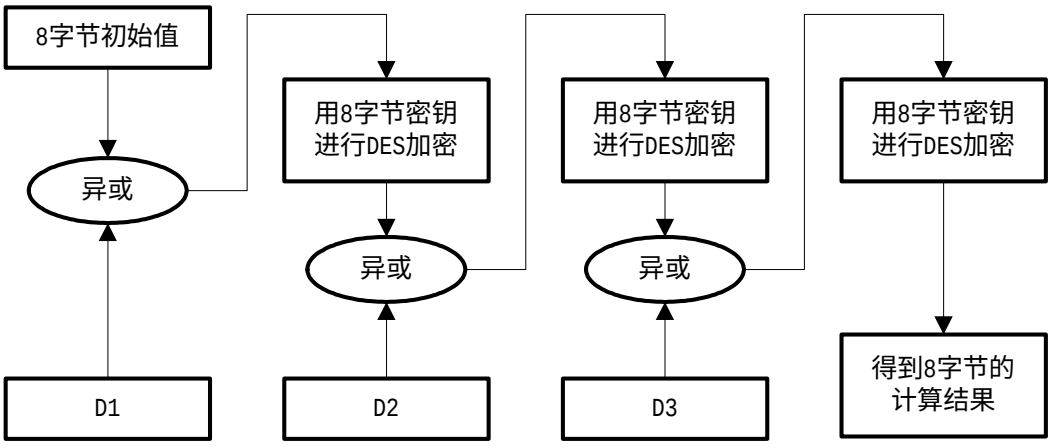

图 4：用 Single DES 密钥产生 MAC 的算法

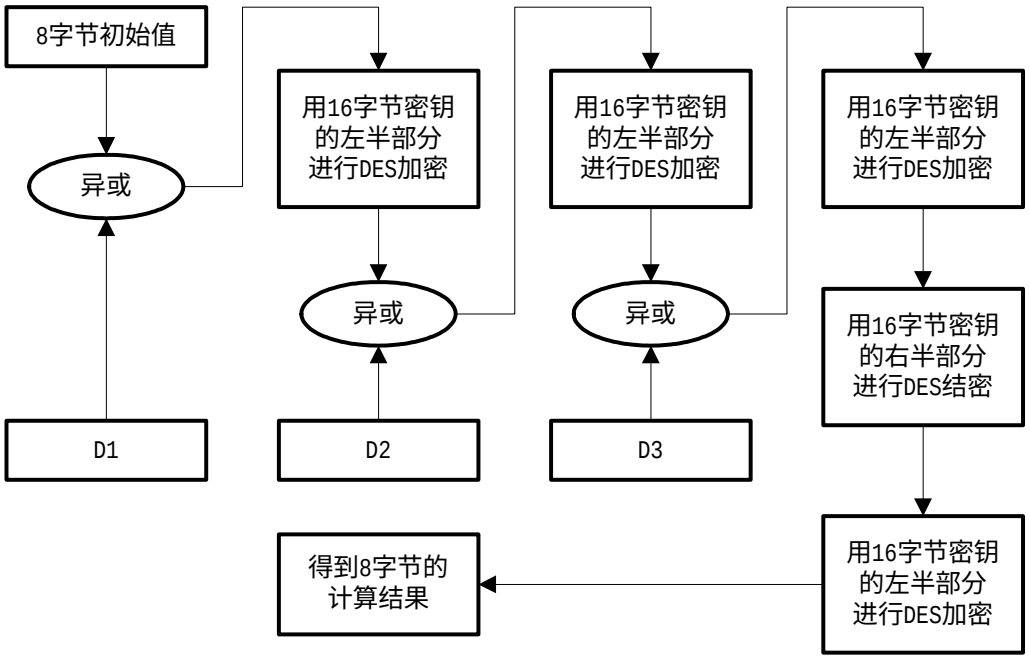

图 5：用 Triple DES 密钥产生 MAC 的算法

第六步：最终得到的是从计算结果左侧取得的 4 字节长度的 MAC。

(5) TAC 的计算

交易认证码（TAC）可用于鉴别交易记录的合法性。

TAC 由内部密钥（DTK）左右 8 位字节异或运算的结果对表 1 中的数据按照 MAC 计算方法生成。

MAC 计算的初始值为 8 个字节的十六进制数字“ 0 ”，方法参见上一节。

TAC 码计算数据域　　表 1

数据	长度
交易金额	4
交易类型标识	1
终端机编号	6
终端机交易序号	4
终端交易日期	4
终端交易时间	3

3.3.3 PSAM 卡应用要求

PSAM 卡用于收费车道的 IC 读写操作。基于电子钱包的储值卡消费交易应遵循《中国金融集成电路（IC）卡规范》中所规定的电子钱包脱机消费交易流程。

PSAM 卡应用文件结构应当符合 ISO/IEC 7816-4 的要求，但不符合本规范的其他应用也可以出现在本支付应用系统（PSA）上。如果系统增加其他应用，相应在 PSAM 卡上增加其他应用 ADF 即可，新应用所需要的数据和密钥均存放在新 DF 中，新增加的 DF 不得与原来的 DF 存在冲突。

PSAM 卡支持多级发卡的机制，各级发卡方在卡片主控密钥和应用主控密钥的控制下创建文件和装载密钥。PSAM 卡中 PSA 的路径可以通过明确选择支付系统环境（PSE）来激活。

PSAM 卡文件结构参见本技术要求正文第四章。

为了防止因为 PSAM 卡意外流失而造成对电子收费系统的不良影响，如利用其进行如非现金支付卡的入口信息改写等，建议采用“ 登录签到 ”的方式对 PSAM 卡的使用进行限制管理。亦即在 PSAM 卡加电后开始使用之前需要进行在线 “ 登录签到 ”，以获取必要的使用权限。

3.3.4 ISAM 应用要求

ISAM 用于储值卡（电子钱包）的充值交易，交易遵循《中国金融集成电路（IC）卡规范》中描述的电子钱包的圈存交易过程。

金融应用中，圈存交易的进行必须在金融终端上联机进行，并要求提交个人密码（PIN）；圈存主密钥通常放在系统主机上，由主机来控制整个交易的进行。

在公路联网收费系统中，充值操作可以参照《中国金融集成电路（IC）卡规范》中描述的电子存折／电子钱包的圈存交易过程，使用 ISAM 卡来实现，将充值主密钥存放在 ISAM 卡上，将 ISAM 卡放置在脱机终端内，在 ISAM 卡的控制下完成充值交易，然后集中处理交易记录。实际情况中可以根据系统工作环境和实现的方便程度来选择使用充值方式。

ISAM 卡在充值终端上的安装和使用需要有一定的安全保障。终端和 ISAM 卡之间的是以安全方式进行通信的。ISAM 卡上应用主工作密钥数据元的使用需要有一定的权限控制。

ISAM 卡的结构参见上节对 PSAM 卡结构的描述。

3.3.5 SAM 卡文件结构说明

3.3.5.1 MF 区域说明

在 PSAM 卡的 MF 区域中，文件创建和密钥装载是在卡片主控密钥的控制下进行。

(1) 目录数据文件

DIR 目录数据文件的说明参考《中国金融集成电路（IC）卡规范》，但 DIR 目录数据文件的入口地址必须包括全国密钥管理总中心应用 ADF。

(2) 卡片主控密钥

卡片主控密钥是卡片的控制密钥，由卡片生产商写入，由发卡方替换为发卡方的卡片主控密钥。卡片主控密钥的更新在自身的控制下进行。发卡方必须在卡片主控密钥的控制下，

① 创建卡片 MF 区域的文件；
② 装载卡片维护密钥、应用主控密钥；
③ 更新卡片主控密钥、卡片维护密钥。

卡片主控密钥的控制可通过外部认证操作实现，也可通过安全报文的方式实现。

(3) 卡片维护密钥

卡片维护密钥用于卡片 MF 区域的应用维护，在卡片主控密钥的控制下装载和更新。卡片的管理者可在卡片维护密钥的控制下，

① 安全更新记录文件；
② 安全更新二进制文件。

卡片维护密钥的控制通过安全报文的形式实现。

(4) 卡片公共信息文件

卡片公共信息文件存放卡片的公共信息，在卡片主控密钥的控制下创建，可自由读，可在卡片维护密钥的控制下改写。

(5) 终端信息文件

终端信息文件存放终端的信息，在卡片主控密钥的控制下创建，可自由读，可在卡片维护密钥的控制下改写。

3.3.5.2 ADF 区域说明

在 PSAM 卡的 ADF（Application Data File）区域中，文件创建和密钥装载是在应用主控密钥的控制下进行。ADF 下的文件结构可由应用发行者自行确定。全国密钥管理中心应用 ADF 的文件结构必须包括应用主控密钥、应用维护密钥、应用主工作密钥数据元、应用公共数据文件和终端应用交易序号数据元。

(1) 应用主控密钥

应用主控密钥是应用的控制密钥，在卡片主控密钥控制下写入。发卡方必须在应用主控密钥的控制下，

① 装载应用维护密钥、应用主工作密钥；
② 更新应用主控密钥、应用维护密钥。

应用主控密钥的控制可通过外部认证操作实现，也可通过安全报文的方式实现。

(2) 应用维护密钥

应用维护密钥用于卡片 ADF 区域的应用维护，在应用主控密钥的控制下装载和更新。卡片的管理者可在应用维护密钥的控制下，

① 安全更新记录文件；
② 安全更新二进制文件；
③ 进行应用解锁。

卡片维护密钥的控制通过安全报文的形式实现。

(3) 应用主工作密钥

应用主工作密钥用于卡片的交易，在应用主控密钥的控制下装载。

(4) 应用公共信息文件

应用公共信息文件存放应用的公共信息，在应用主控密钥的控制下创建，可自由读，可在卡片维护密钥的控制下改写。

(5) 终端应用交易序号数据元

终端应用交易序号长度 4 字节，用于终端的脱机交易，在消费交易 MAC2 验证通过的情况下由卡片操作系统改写。

终端应用交易序号只对本应用有效。

4 联网收费系统 IC 卡密钥管理体系

公路联网收费系统的密钥管理体系可分为两大类，包括：非接触逻辑加密卡密钥管理体系以及非现金支付 CPU 卡的密钥管理体系。

人工现金收费系统中非接触逻辑加密卡（用于通行券、身份卡、公务卡等）的密钥由各收费路网结算中心自行统一管理。

考虑到未来跨区域非现金方式的通行费支付与结算，人工半自动收费系统中的非现金支付卡（CPU 卡，包括记账卡、储值卡等）以及组合式电子收费系统中使用的双界面 CPU 卡等的密钥须由全国公路联网电子收费密钥管理中心实行统一管理。密钥的装载、更新和下发应符合中国人民银行 PSAM 卡标准。

各区域联网收费系统所使用的密钥为全国公路联网电子收费密钥管理中心从根密钥分散后得到的二级密钥。

4.1 密钥管理系统体系

4.1.1 密钥管理系统体系介绍

公路联网电子收费非现金支付密钥管理系统采用 3DES 加密算法，采用由全国公路联网电子收费密钥管理中心、区域（省、市）联网收费结算中心组成的二级管理体制，可在全国范围内实现公共主密钥的安全共享、跨区域收费交易。

系统在充分保证密钥安全性的基础上，支持 IC 卡密钥的生成、注入、导出、

备份、恢复、更新、服务等功能，实现密钥的安全管理。密钥受到严格的权限控制，不同机构或人员对不同密钥的读、写、更新、使用等操作具有不同的权限。密钥存储及服务根据应用目的不同一般以密钥卡或硬件加密机的形式提供，而密钥备份可以采用密钥卡的形式。

4.1.2 密钥管理系统体系结构

全国公路联网电子收费密钥管理中心负责系统的根密钥、总控密钥卡、业务代码卡、业务主密钥母卡及传输卡、主密钥分散卡、PSAM 卡、用户卡母卡、电子标签密钥母卡等的生成与管理。各区域联网收费结算中心负责本区域内的非现金支付卡（储值卡、记账卡）、PSAM 卡、ISAM 卡及管理用卡的生成与管理。密钥的装载、更新和下发符合《中国人民银行 PSAM 卡规范》。密钥管理体系结构参见图 6。

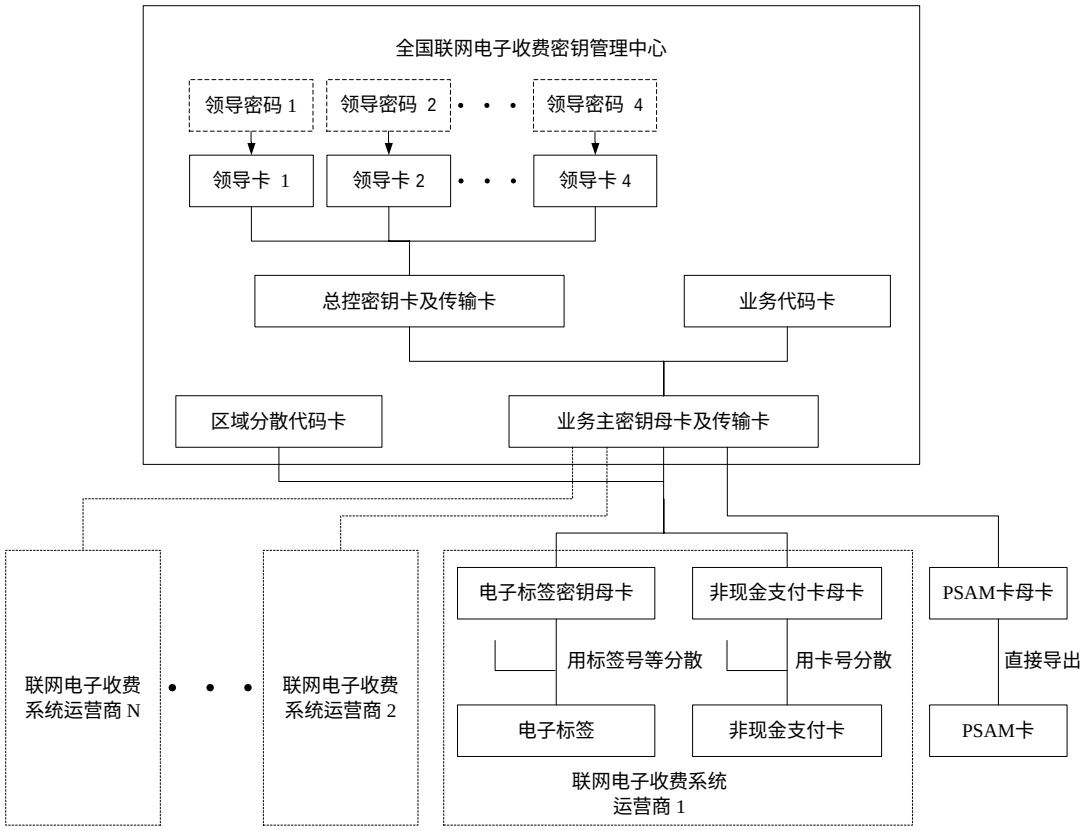

图 6：IC 卡密钥管理体系结构

总控密钥卡存放系统的总控密钥，总控密钥是全国公路联网收费 IC 卡非现金支付系统的根密钥。

业务代码总控卡存放有区别不同业务的分散代码，路如区别充值、消费、外部认证等业务的分散代码。

总控密钥卡的根密钥经过业务代码总控卡的分散代码分散后导出各类应用主密钥，并存放在业务主密钥卡里。各类应用密钥包括外部认证密钥、消费密钥、内部密钥、电子标签密钥等。

业务主密钥分散卡中存放标识各区域联网收费系统的区域分散代码。

业务主密钥卡中的应用主密钥经过业务主密钥分散卡的分散代码分散导出生成存放于非现金支付卡母卡及电子标签密钥卡母卡中的消费密钥、外部认证密钥、内部密钥等。PSAM 卡中存放的消费密钥、外部认证密钥、内部密钥则由业务主密钥卡中的相应应用密钥直接导出。其中，非现金支付卡母卡存放有所属区域内非现金支付卡的部分主密钥 ;电子标签密钥卡母卡存放有电子标签的各种主密钥。由各区域联网收费系统利用非现金支付卡母卡通过分散非现金支付卡卡号生成最终用户使用的非现金支付卡 ;利用电子标签密钥卡母卡通过分散电子标签序列号等生成最终存储在电子标签中的相应子密钥。

PSAM 卡母卡由各区域联网收费系统向全国公路联网电子收费密钥管理中心申领。PSAM 卡存放有非现金支付卡的消费认证密钥等，同时还可以在其他应用目录内存放各区域通行卡、身份卡、公务卡等的密钥。

通过上述分级扩展机制可以实现用户非现金支付卡的跨区域使用。

4.2.3 密钥的生成与保存流程

(1) 总控密钥的生成

总控密钥应在可以认为是绝对安全的环境下产生，并存放在总控密钥卡中。该密钥应具有在可以认为是绝对安全的环境下可重新生成的能力。

总控密钥由全国公路联网电子收费密钥管理中心负责生成。在管理人员辅助并保证环境安全的情况下，由四位领导依次输入 8 位数字的十六进制密码，系统根据一定的算法产生总控密钥，制作出总控密钥卡及其传输卡。生成过程如图 7 所示。

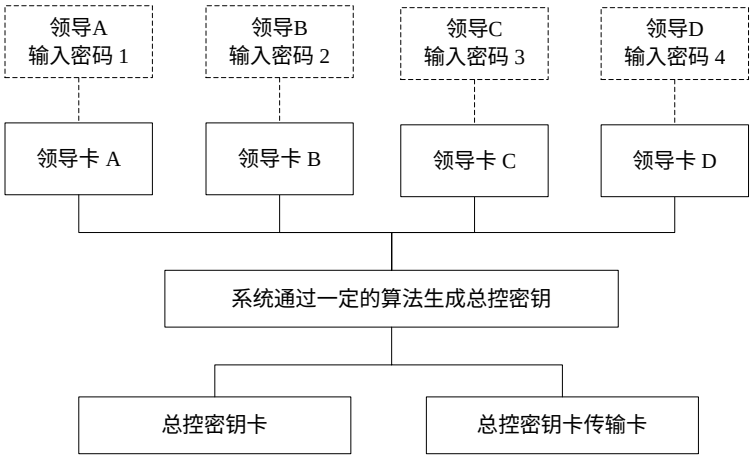

图 7：总控密钥生成过程

(2) 业务分散代码的生成

业务分散代码由密钥管理中心负责生成，可由管理人员手工输入或者由加密机随机生成，并存储在业务代码卡中。在保证环境安全情况下，根据业务分散代码和保护密码，制作出业务代码卡。生成过程如图 8：

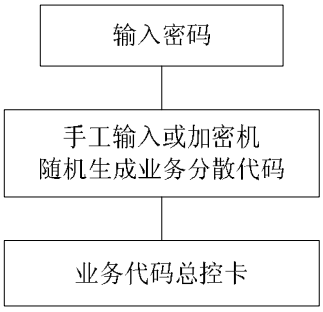

图 8：业务分散代码的生成

(3) 业务主密钥的生成

业务主密钥由密钥管理中心负责生成。系统在总控密钥卡传输卡的保护下，使用业务分散代码对总控密钥进行分散产生业务主密钥，制作出业务主密钥卡及其传输卡，其过程如图 9：

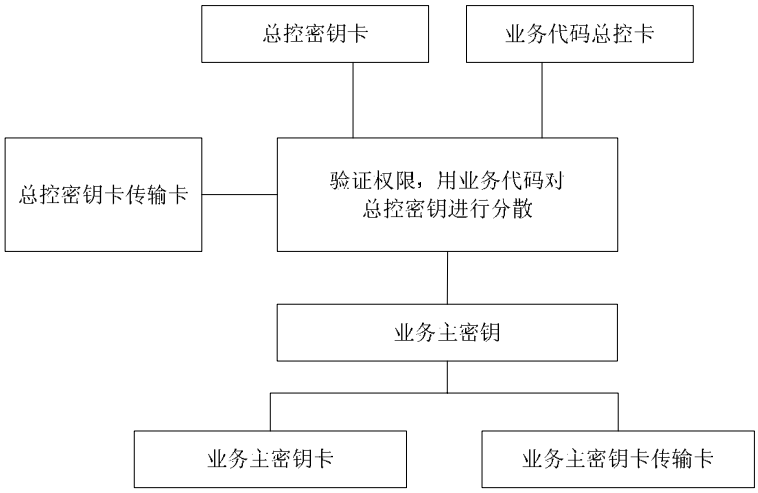

图 9：业务主密钥的生成

(4) 区域分散代码的生成

区域分散代码由密钥管理中心负责生成。在保证环境安全情况下，可由管理人员手工输入或者由加密机随机生成，制作出业务主密钥分散卡。生成过程如图 10：

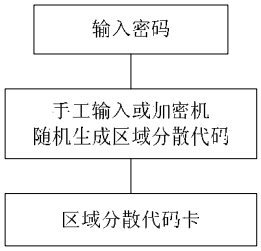

图 10：区域分散代码的生成过程

(5) 非现金支付卡母卡、电子标签密钥卡母卡密钥的生成

非现金支付卡母卡、电子标签密钥卡母卡中的密钥由全国公路联网电子收费密钥管理中心负责生成。系统在业务主密钥分散卡保护密码，使用业务主密钥分散代码对业务主密钥进行分散产生各类密钥，并制作出母卡及其传输卡。制作过程如图 11：

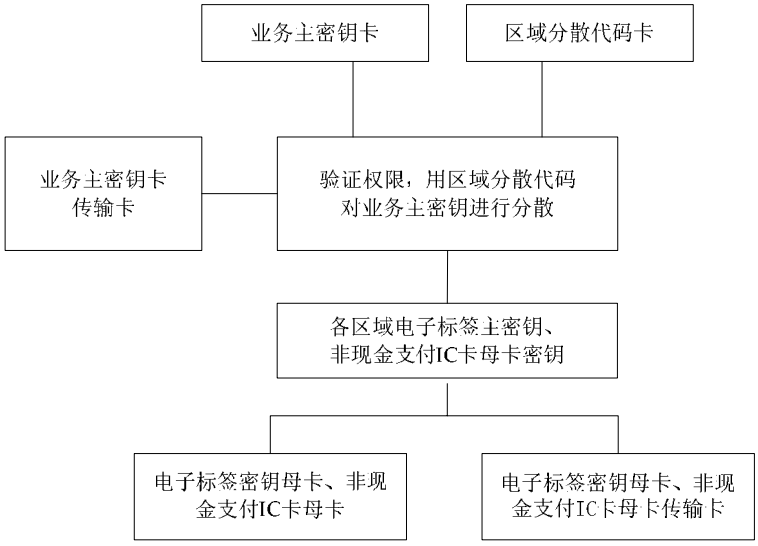

图 11：非现金支付卡母卡、电子标签密钥卡母卡密钥的生成过程

(6) PSAM 卡密钥的生成

PSAM 卡由全国公路联网电子收费密钥管理中心负责生成。PSAM 卡中的各种业务密钥由业务主密钥卡中相应密钥直接导出。

各区域联网收费结算中心可以在 PSAM 卡内导入本区域内逻辑加密卡（通行卡、身份卡等）的密钥，并单独存放在一个目录内。

各区域制作发行的逻辑加密卡（通行卡、身份卡等）只能在本区域内使用。

4.2 密钥管理技术要求

4.2.1 密钥生成

(1) 密钥生成的基本安全要求

密钥生成是密钥整个生命周期内最核心的任务。为保证密钥的安全和防止密钥的泄露，应从以下几个方面采取措施。

① 密钥生成采用多人生成或硬件加密的方式；
② 密钥生成环境的安全管理，应可视为相对安全；
③ 参加密钥生成的特殊人员的安全管理规定；
④ 密钥生成过程应按照严格的操作规程进行。

(2) 密钥生成方式

密钥生成一般采用集中方式产生,即由项目最高管理机构生成相应的各种主密钥组，其它密钥由该组密钥分散产生。密钥产生的两种基本方法：

① 不重复的密钥产生 :随机过程,产生不可恢复的密钥,每次的数值不相同；
② 可重复的密钥产生：密钥变换、密钥衍生；而且密钥的产生是可以重复的，在需要的情况下能够重新得到与原来相同的密钥值。

(3) 密钥安全生成的安全技术

不需重复生成的密钥采用随机产生的办法生成，由系统随机产生这些密钥，写入卡中保存，不需人工干预，安全性能更高。

可重复产生的密钥采用密钥种子交换或衍生的办法生成,确保密钥变换或衍生的过程绝对安全，这样就可以保证系统的安全及使用方便。

4.2.2 密钥发行

(1) 密钥发行方式

密钥的发行采用梯级生成、下发的方式。即由上一级生成下一级所需的各种子密钥，并保存在密钥母卡中传递给下一级。

(2) 密钥发行的安全技术

使用传输密钥控制业务主密钥的加密装载、直接加密导出、分散加密导出。

4.2.3 密钥更新

(1) 密钥更新的基本安全要求

当密钥的生命周期结束或系统密钥泄露后，需要进行密钥更新。密钥更新的基本原则是保护持卡人的利益不受损害，不影响持卡人的正常交易；密钥更新的全过程应保证系统的安全性能不受影响。

(2) 密钥的版本更新

每组密钥必须有有效期，有效期后系统须重新生成新的密钥组,并用于发行

新卡。

(3) 密钥的索引更新

同一功能的密钥（如消费密钥），若使用频度高，应使用多个索引，在卡片生命周期的不同时期或当前使用的密钥泄露的紧急情况下，起用不同索引的密钥。

(4) 正常密钥更新

正常密钥更新的两种方法：

① 密钥替换
② 更换密钥组

(5) 紧急密钥更新

一旦密钥泄露，必须立即进行紧急密钥更新。紧急密钥更新的主要方法有：

① 安装多组紧急密钥备份组
② 停止现有系统的使用，重新构造密钥体系

4.2.4 密钥装载

密钥装载采用安全报文的方式，利用 WRITE KEY 命令来进行。安全报文产生的方式参见命令的说明。

密钥装载的控制过程如下：

① 卡片主控密钥在卡片主控密钥的控制下更新
② 卡片维护密钥在卡片主控密钥的控制下装载和更新
③ 应用主控密钥在卡片主控密钥的控制下装载
④ 应用主控密钥在应用主控密钥的控制下更新
⑤ 应用维护密钥在应用主控密钥的控制下装载和更新
⑥ 应用主工作密钥在应用主控密钥的控制下装载和更新。

4.2.5 密钥访问

① 密钥不允许直接读

② 密钥必须在主控密钥的控制下更新

③ 密钥必须不能被外界直接访问，只能接受内部操作系统发来的进行 MAC 计算的指令，按照指定的流程计算出 MAC

④ 计算临时密钥产生的结果只保留在卡片内部，不能被外界直接访问。

4.2.6 密钥属性

密钥的使用都有一定的限制，必须满足密钥属性的要求。密钥属性应包括以下几项

(1) 密钥用途

密钥用途长度为 1 字节，低 5 位为密钥类型，高 3 位为密钥分散级数，密钥类型约定如下：

① 0 — 主控密钥
② 1 — 维护密钥
③ 2 — 消费密钥
④ 3 — PIN 解锁密钥
⑤ 4 — 重装 PIN 密钥
⑥ 5 — 用户卡应用维护密钥
⑦ 6 — MAC 密钥
⑧ 7 — 加密密钥
⑨ 8 — MAC、加密密钥
⑩ 9-31 — 保留

(2) 密钥算法标识

密钥算法标识指定了密钥所支持加密算法，长度 1 字节，密钥算法标识约定如下：

① 0，3DES
② DES
③ 2-255，保留

(3) 密钥版本

密钥版本制定某种类型密钥的标识长度 1 字节，对消费密钥来说，密钥版本是用于消费交易密钥选择过程中的密钥版本号，而对于其他密钥来说，密钥版本

是密钥标识。

4.3 全国公路联网电子收费密钥管理中心洗卡流程

全国通用的消费／取现主密钥（GMPK）是系统的根密钥，如果一旦被盗取或被非法使用，公路联网收费系统发行的所有非现金支付 IC 卡将不得不停止使用，从而带来政治、经济上的重大损失。所以，从安全的角度来说，全国所有的 PSAM 卡必须在全国公路联网电子收费密钥管理中心统一安全装载 GMPK。任何个人和组织都无法得到 GMPK 的明文，也无法通过 PSAM 卡来利用 GMPK 进行非法的密钥运算。区域联网收费结算中心行可以向全国公路联网电子收费密钥管理中心申报所需 PSAM 卡的数量，由全国公路联网电子收费密钥管理中心按需求量统一下发。

全国公路联网电子收费密钥管理中心从生产商处得到一批 PSAM 卡，卡片已经过预个人化处理，卡片 MF 区域和全国公路联网电子收费密钥管理中心 ADF 区域下的文件已由厂商建好，生产商密钥（卡片主控密钥）也已装载。在 IC 卡生产商将这一批 IC 卡交给全国公路联网电子收费密钥管理中心的同时，存放生产商密钥的生产商母卡也要交给全国公路联网电子收费密钥管理中心。

全国公路联网电子收费密钥管理中心在接到这批卡之后，用生产商母卡中的生产商密钥 kMprd 来鉴别每一张 IC 卡。鉴别通过后，全国公路联网电子收费密钥管理中心将用自己产生的密钥 kIctlR，来替换卡上的生产商密钥 kMprd，成为卡上的卡片主控密钥。

kIctlR 是全国公路联网电子收费密钥管理中心随机产生或采用其他方法产生的，被加密导入后作为这一批 PSAM 卡的主控密钥，控制 MF 区域下文件创建和密钥更新。

全国公路联网电子收费密钥管理中心必须在卡片主控密钥的控制下装载和更新密钥。具体的过程如下：

① 在生产商密钥（卡片主控密钥）的控制下，更新卡片主控密钥
② 在卡片主控密钥的控制下，装载卡片维护密钥
③ 在卡片维护密钥的控制，安全更新卡片 MF 区域的文件
④ 在卡片主控密钥的控制下，装载应用主控密钥
⑤ 在应用主控密钥的控制下，装载应用维护密钥
⑥ 在应用主控密钥的控制下，装载应用主工作密钥
⑦ 在应用维护密钥的控制下，安全更新卡片 ADF 区域的文件