ICS 35.030
CCS L 80

GM

# 中华人民共和国密码行业标准

GM/T 0107—2021

# 智能 IC 卡密钥管理系统基本技术要求

**Smart IC card key management system basic technical requirements**

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发 布

# 目　　次

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京江南天安科技有限公司、飞天诚信科技股份有限公司、中金金融认证中心有限公司、北京握奇数据股份有限公司、格尔软件股份有限公司、北京华大智宝电子系统有限公司、成都卫士通信息产业股份有限公司、兴唐通信科技有限公司、北京信安世纪科技股份有限公司、北京数字认证股份有限公司。

本文件主要起草人：朱家雄、王冬冬、朱鹏飞、张利琴、刘雅静、甄世玉、刘淑敏、郭晶莹、刘丽、贺亚、郑强、陈保儒、帅兰兰、张旭、顾蓉、汪宗斌、王春涛。

# 智能IC卡密钥管理系统基本技术要求

## 1 范围

本文件规定了智能IC卡密钥管理系统的应用架构及密钥体系、功能要求、密钥安全机制、系统安全要求等内容。

本文件适用于指导智能IC卡密钥管理系统的设计、开发、检测和使用。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 36322 信息安全技术 密码设备应用接口规范

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GM/T 0044 SM9标识密码算法

GM/T 0045 金融数据密码机技术规范

GM/T 0051 密码设备管理 对称密钥管理技术规范

GM/Z 4001 密码术语

## 3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

**密钥管理系统 key management system**

管理密钥生成、存储、导入、导出、下发、备份、归档、更新、销毁等业务的系统。

3.2

**智能IC卡 smart integrated circuit(s) card**

实现密码运算和密钥管理的含CPU(中央处理器)的智能集成电路卡。

3.3

**发卡机构 issuer**

开展智能IC卡发卡业务的服务机构。

3.4

**密钥分散 key diversify**

对称密钥体制中，根密钥根据分散因子产生子密钥的运算过程。

3.5

**根密钥　root key**

处于层次化对称密钥结构中的顶层，用于智能IC卡级子密钥及下级机构子密钥的产生或保护。

注：参考GM/Z 4001中对主密钥的定义："处于对称密码系统层次化密钥结构中的顶层，用于下层密钥的产生或保护"（定义2.152）。

3.6

**业务密钥　application key**

密码应用系统中与具体应用相关的密钥。

[GM/T 0051—2016，定义3.4]

## 4　符号和缩略语

### 4.1　符号

下列符号适用于本文件。

$K_{ENC}$　加密会话密钥

$K_{DEK}$　对称密钥或其他可选保密数据会话密钥

$K_{MAC}$　MAC会话密钥

### 4.2　缩略语

下列缩略语适用于本文件。

| | | |
|---|---|---|
| ATM | 自动取款机 | (Automatic Teller Machine) |
| IC | 集成电路 | (Integrated Circuit) |
| KEK | 密钥加密密钥 | (Key Encrypted Key) |
| MAC | 消息鉴别码 | (Message Authentication Code) |
| PAN | 主账号 | (Primary Account Number) |
| PIN | 个人识别码 | (Personal Identification Number) |
| POS | 销售终端 | (Point Of Sale) |
| PSAM | 销售点终端安全存取模块 | (Purchase Secure Access Module) |
| SAM | 安全存取模块 | (Secure Access Module) |
| SK | 子密钥 | (Sub key) |
| TAC | 交易验证码 | (Transaction Authorization Crypogram) |
| TK | 传输保护密钥 | (Transport Key) |

## 5　应用架构及密钥体系

### 5.1　应用架构

智能IC卡密钥管理系统是一套针对智能IC卡应用所需的密钥生命周期统一管理系统，为使用密钥的智能IC卡相关业务系统提供密钥服务功能。其功能主要包括：对智能IC卡受理终端、智能IC卡卡管系统、智能IC卡清结算系统、数据准备系统、用户卡发卡系统、SAM卡发卡系统等提供密钥生成、密钥存储备份、密钥申请、密钥分发、密钥使用等操作进行统一管理，并对密钥使用情况进行监控和审计。

智能IC卡密钥管理系统在整个智能IC卡应用的架构见图1。

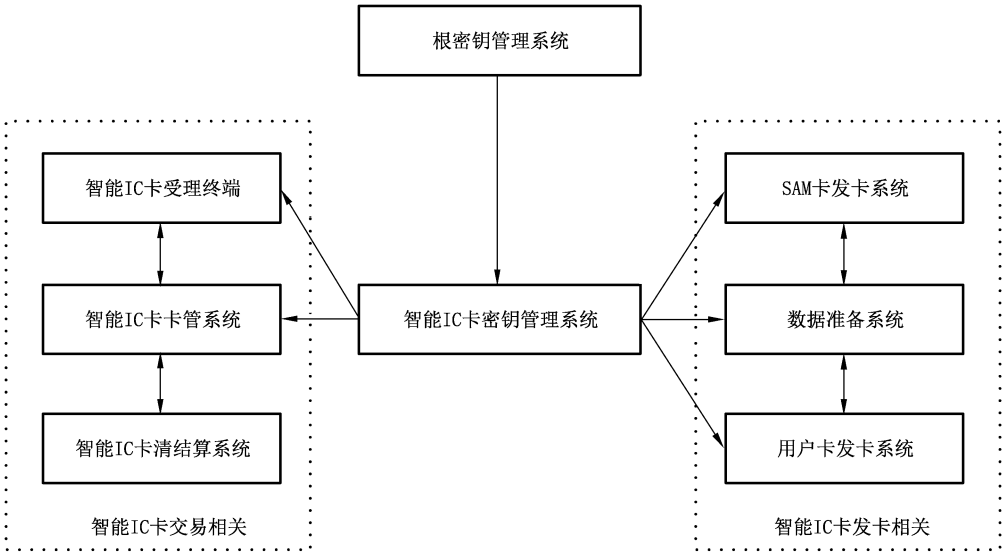


**图1　智能IC卡密钥管理系统应用架构图**

智能IC卡应用通常支持多级架构，分为上级机构侧的根密钥管理系统和发卡机构侧的智能IC卡密钥管理系统，各模块的功能和密钥的分布说明如下：

——上级机构侧的根密钥管理系统：负责生成和管理智能IC卡业务根密钥和根公钥证书，并签发下级机构证书或者分散生成下级机构业务密钥；

——发卡机构侧的智能IC卡密钥管理系统：负责从上级机构导入证书和密钥，生成和管理本级机构的智能IC卡业务密钥和机构证书，并为智能IC卡发卡和交易提供密钥服务；

——智能IC卡受理终端：处理智能IC卡交易的终端（包括POS、ATM、闸机、车载终端等），受理终端侧导入智能IC卡业务根公钥证书或者是包含智能IC卡消费密钥根密钥的PSAM卡，通过这些证书或者公钥完成与智能IC卡的脱机认证；

——智能IC卡卡管系统：管理智能IC卡业务数据及为智能IC卡发卡和交易提供服务的系统，智能IC卡卡管系统部署智能IC卡交易类密钥（电子钱包类密钥或者电子现金密钥），通过这些密钥完成与智能IC卡的联机认证；

——智能IC卡清结算系统：处理智能IC卡交易的清算、结算业务的系统，智能IC卡清结算系统部署智能IC卡结算类密钥，通过这些密钥完成智能IC卡清结算时的交易认证；

——数据准备系统：处理智能IC卡发卡所需的业务数据和安全数据并形成最终的制卡文件，数据准备系统包含智能IC卡卡片证书、智能IC卡密钥等信息；

——SAM卡发卡系统：执行SAM卡的发卡过程，经过安全认证安全加载相关密钥和文件到SAM卡中，SAM卡发卡系统中部署智能IC卡消费根密钥、SAM卡管理类密钥等；

——用户卡发卡系统：执行用户卡的发卡过程，经过安全认证后安全加载相关密钥和文件到用户卡中，用户卡发卡系统中部署用户卡的业务密钥等。

## 5.2　密钥体系

### 5.2.1　概述

智能IC卡密钥管理系统涉及的密钥按照密钥用途或者密钥来源可分为智能IC卡业务密钥和系统

保护密钥两种。

智能IC卡业务密钥属于智能IC卡应用规范所定义，智能IC卡业务密钥通过智能IC卡密钥管理系统进行管理维护，用于保证智能IC卡发卡和交易处理过程中的安全。智能IC卡业务密钥可分为对称密钥和非对称密钥，对称密钥按照用途又可以划分为管理类密钥和交易类密钥两种类型，智能IC卡业务密钥分类情况见表1。

**表1　智能IC卡业务密钥归纳表**

| 按计算方式分类 | 按用途分类分类 | 密钥类型 | 用途 |
|---|---|---|---|
| 对称密钥 | 交易类密钥 | 应用密文主密钥 | 用于产生智能IC卡应用密文子密钥，用于应用密文的产生和验证 |
| | | 安全报文认证(MAC)主密钥 | 用于产生智能IC卡MAC子密钥，用于安全报文鉴别码的产生和验证 |
| | | 安全报文加密主密钥 | 用于产生智能IC卡加密子密钥，用于加密解密安全报文 |
| | | 消费主密钥 | 用于产生智能IC卡消费子密钥，用于消费/取现交易中的报文鉴别码的产生和验证 |
| | | 圈存主密钥 | 用于产生智能IC卡圈存子密钥，用于圈存交易中的报文鉴别码的产生和验证 |
| | | 圈提主密钥 | 用于产生智能IC卡圈提子密钥，用于电子存折应用圈提交易中的报文鉴别码的产生和验证 |
| | | TAC主密钥 | 用于产生智能IC卡TAC子密钥，用于消费/取现交易中产生TAC |
| | | PIN解锁主密钥 | 用于产生智能IC卡PIN解锁子密钥，用于解锁PIN |
| | | PIN重装主密钥 | 用于产生智能IC卡PIN重装子密钥，用于重装PIN |
| | 管理类密钥 | 修改透支额度主密钥 | 用于产生智能IC卡修改透支额度子密钥，用于修改电子存折应用透支额度中的报文鉴别码的产生和验证 |
| | | 发卡机构主密钥 | 用于产生智能IC卡卡片级密钥($K_{ENC}$、$K_{MAC}$、$K_{DEK}$)、用于保护智能IC卡发卡过程的安全 |
| | | 卡片主控主密钥 | 用于产生智能IC卡卡片主控密钥，用于发卡过程中的卡片认证 |
| | | 卡片维护主密钥 | 用于产生智能IC卡卡片维护密钥，用于发卡过程中的卡片文件的保护写入和更新维护 |
| | | 应用主控主密钥 | 用于产生智能IC卡应用主控密钥，用于发卡过程中卡片中应用的认证 |
| | | 应用维护主密钥 | 用于产生智能IC卡应用维护密钥，用于发卡过程中卡片中应用文件的保护写入和更新维护 |
| | | 应用开通主密钥 | 用于产生智能IC卡应用开通密钥，用于与扩展应用相关的安全应用开通密钥报文鉴别码的产生和验证 |

表 1　智能 IC 卡业务密钥归纳表（续）

| 按计算方式分类 | 按用途分类分类 | 密钥类型 | 用途 |
|---|---|---|---|
| 非对称密钥 | | 根公私钥对 | 用于脱机数据认证，根私钥用于自签根公钥证书，并为发卡机构签发发卡机构公钥证书，根公钥用于验证自签根公钥证书和发卡机构公钥证书 |
| | | 发卡机构公私钥对 | 用于脱机数据认证，发卡机构私钥用于签发智能 IC 卡公钥证书，发卡机构公钥用于验证智能 IC 卡公钥证书 |
| | | 智能 IC 卡公私钥对 | 用于脱机数据认证，基于智能 IC 卡公私钥对完成交易数据的签名和认证 |

系统保护密钥又可分为系统传输保护密钥和系统存储保护密钥，系统传输保护用于保证智能 IC 卡密钥管理系统和其关联系统之间业务密钥及敏感数据传输的机密性和完整性，系统存储保护密钥用于保障智能 IC 卡密钥管理系统自身对业务密钥及敏感数据存储的机密性和完整性。

系统传输保护密钥一般指系统间的传输保护密钥（TK）或者密钥加密密钥（KEK），系统传输保护密钥并不是智能 IC 卡密钥管理系统进行管理维护的密钥，一般是多个系统间协商或者共同约定。

系统存储保护密钥一般指密码机的本地主密钥，系统存储保护密钥并不是智能 IC 卡密钥管理系统进行管理维护的密钥。

### 5.2.2　对称密钥体系

智能 IC 卡业务密钥的对称密钥主要涉及管理类密钥和交易类密钥，主要作用是保证发卡过程和交易过程的安全，具体的密钥类型和用途由对应的智能 IC 卡业务规范所定义，本标准不做具体约束。

智能 IC 卡业务密钥的对称密钥体系一般都是多级分散结构的，根密钥管理系统产生和管理部分业务根密钥，并分散产生发卡机构业务根密钥，发卡机构智能 IC 卡密钥管理系统导入上级机构产生的部分业务根密钥，并产生部分自己独立管理和维护的业务根密钥，再经过一级或者多级分散产生具体的卡片密钥。

对称密钥体系见图 2。

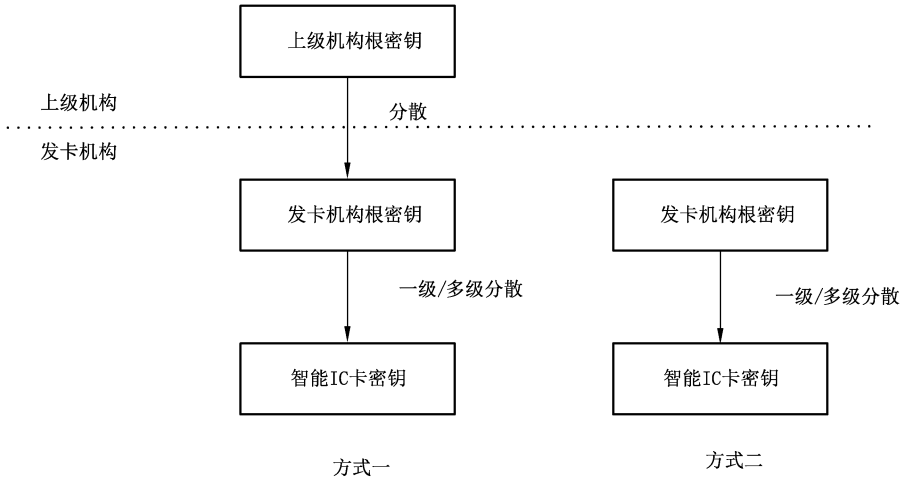


图 2　智能 IC 卡业务密钥的对称密钥体系图

方式一：某些应用场景下，部分智能 IC 卡业务密钥由上级机构的密钥管理系统产生和管理（JT/T 978 规范中的交通 IC 卡的消费根密钥）。

方式二：某些应用场景下，部分智能 IC 卡业务密钥由发卡机构的密钥管理系统产生和管理（JR/T 0025 规范中的联机交易类密钥）。

发卡机构的智能 IC 卡密钥管理系统再根据一级/多级分散产生具体的智能 IC 卡密钥，具体的分散机制见 7.1.3。

发卡机构的智能 IC 卡密钥管理系统具备的对称密钥管理功能见 6.3，对称密钥管理所需要的安全机制见 7.1。

#### 5.2.3 非对称密钥体系

智能 IC 卡业务密钥的非对称密钥体系主要是基于自定义智能 IC 卡体系证书的非对称密钥，用于实现交易过程中根密钥管理系统对发卡机构的认证，发卡机构对智能 IC 卡的认证。

智能 IC 卡业务密钥的非对称密钥体系一般都是三级证书体系，见图 3。

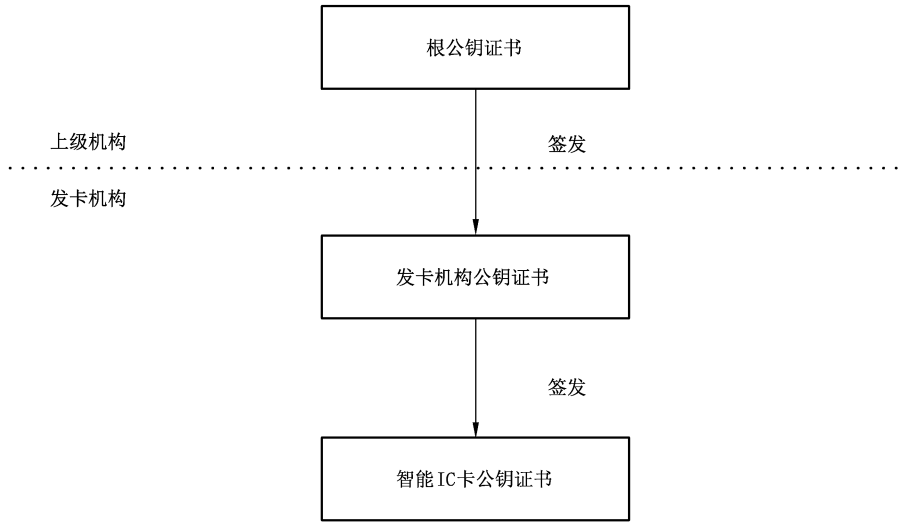


**图 3 智能 IC 卡应用的非对称密钥体系**

根密钥管理系统负责生成和管理根公钥和根私钥，并自签根公钥证书，同时为发卡机构签发发卡机构公钥证书。

发卡机构密钥管理系统生成发卡机构的公私钥对，并提交相应的公钥请求文件由根密钥管理系统签发发卡机构公钥证书；发卡机构密钥管理系统负责生成和管理具体的智能 IC 卡公私钥对，并签发智能 IC 卡公钥证书，系统应支持的非对称密钥和证书管理功能见 6.4，非对称密钥管理应支持的安全机制见 7.2。

## 6 功能要求

### 6.1 概述

智能 IC 卡密钥管理系统主要生成和管理智能 IC 卡业务根密钥及相应证书，并为其他的智能 IC 卡相关系统提供密钥服务功能，应至少包含系统管理、对称密钥管理、非对称密钥管理、审计管理、接口服务等功能。

### 6.2 系统管理功能

系统管理功能应负责用户角色权限管理、操作员管理、系统配置管理以及设备管理功能 。

a) 角色权限管理：应包括权限资源管理、用户管理，用于对角色进行增、删、改、查、设置权限等操作为对应的角色分配恰当的权限。

b) 操作员管理：应根据角色划分不同权限的用户，同时应为操作员分配不同的角色。用于对系统操作员进行增、删、改、查的操作，并在创建操作员时，为操作员分配相应角色。

c) 系统配置管理：应实现对管理智能 IC 卡密钥管理系统的各种系统配置，应包括各种基础信息及业务信息配置。

d) 设备管理：应实现智能 IC 卡密钥管理系统的加密机管理，应包括对加密机资源信息的维护、加密机资源的合理分组管理及对加密机的监控管理功能。应支持加密机的添加、修改、查看、删除等操作，完成加密机的配置管理。

### 6.3 对称密钥管理功能

对称密钥管理功能应支持各种对称类型密钥的产生、存储、使用、销毁功能处理，包括对于存储在加密机中的密钥和存储在数据库中的密钥的安全管理，可支持对称密钥的密钥属性和密钥状态的管理。

a) 生成/注入密钥：应实现增加密钥的功能。增加的对称密钥的信息，宜包括但不限于密钥名称、到期期限、密钥类型、密钥索引、密钥版本号、存储方式等。如果使用密文方式增加密钥，则应增加解密密钥、解密算法、密钥值等相关信息。

b) 密钥分散：密钥在使用过程中，会进行不同级别的分散。在密钥添加过程中，同时应定义使用何种级别的分散，不同级别的分散因子组成。密钥的分散机制见 7.1.3。

c) 更新密钥：应查询出已经添加的密钥信息，并对其进行修改保存。

d) 导出密钥：应查询出已经添加的密钥信息，可对其相关信息进行导出备份操作，导出的密钥可使用密码信封或者密钥传输卡等方式保护。

e) 密钥销毁：应按照条件查询出对称密钥的信息，对过期或者已经泄露或者其他原因不再使用的对称密钥进行删除操作。

f) 到期密钥管理：应对于已经或者即将到期的密钥，进行密钥有效期的修改。

### 6.4 非对称密钥管理功能

非对称密钥管理功能应支持各种非对称类型密钥的产生、存储、使用、销毁功能处理，包括对于存储在加密机中的密钥和存储在数据库中的密钥的安全管理，可支持非对称密钥的密钥属性和密钥状态的管理。同时应支持与之相关的证书的管理，应负责证书的签发和验证。主要包括但不限于生成证书请求、导入/导出证书、销毁证书等功能。

a) 生成非对称密钥对：可支持生成密钥对功能，应考虑非对称密钥对的参数不同，在生成密钥对时，使用不同的参数进行生成密钥对指引。

b) 导入非对称密钥对：应支持可将已经生成的密钥对导入到智能 IC 卡密钥管理系统中使用。

c) 导出非对称密钥对：应支持将已经生成的密钥对导出智能 IC 卡密钥管理系统，私钥为加密状态，公钥为明文状态。

d) 密钥销毁：应按照条件查询出非对称密钥的信息，对过期或者已经泄露或者其他原因不再使用的非对称密钥进行删除操作。

e) 生成发卡机构证书请求：选择或输入证书请求文件的信息，应包括但不限于密钥信息、识别码信息、证书有效期信息，应根据选择的内容生成证书请求文件，并向根密钥管理系统提出证书申请，证书请求文件可查看，可导出到指定目录存储。

f) 导入发卡机构证书：应验证证书有效性并导入对应的证书文件，验证证书并进行导入及管理，对已导入的证书文件，也可导出到指定目录进行存储。

g) 生成智能 IC 卡公钥证书：应支持响应智能 IC 卡公钥证书申请，生成智能 IC 卡公钥证书申请数据并签发智能 IC 卡公钥证书，并支持在线或离线的智能 IC 证书签发的功能，同时也应支持签发智能 IC 卡静态应用数据的功能。

### 6.5 审计管理功能

审计管理功能应提供对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计的功能。审计数据应归档且不能被篡改和删除。应包括实时监控管理、统计管理和操作日志管理模块功能。

a) 实时监控管理：应对加密机以及各种类型密钥的使用，以及对于密钥管理系统访问接口调用情况进行实时监控，出现异常情况进行及时反馈和报警。

b) 统计管理：应实现对于系统的加密机、密钥及相关对位接口的使用进行统计功能。应支持按照多维度进行查询和统计，可导出统计报表。如按照日、月、年使用情况生成报表。

c) 操作日志管理：应记录日志事件发生的时间、事件的操作者、操作类型及操作结果等信息。应按时间、操作者、操作类型等对日志进行分类或综合查询，应使用数字签名等方法，保证日志不被篡改。

### 6.6 接口服务功能

接口服务应实现密钥管理系统对外的密钥服务功能，接口服务支持离线文件和在线网络服务等多种形式。

接口服务应包括但不限于加解密、密钥分散、密钥导入、密钥导出、智能 IC 卡证书签发、发卡机构证书下发、智能 IC 卡密钥下发等服务，接口的传输协议应提供数据机密性和完整性保证。

具体接口参数和接口协议可遵循相应的智能 IC 卡应用规范的要求，本文件不做具体的规定。

## 7 密钥安全机制

### 7.1 对称密钥安全机制

#### 7.1.1 概述

智能 IC 卡密钥管理系统主要对智能 IC 卡业务根密钥进行生命周期管理，包括密钥生成、密钥分散、密钥下发、密钥传输、密钥存储、密钥备份、密钥归档，密钥销毁等。在生命周期管理过程中应具备完善的密钥安全机制。

#### 7.1.2 密钥生成

智能 IC 卡业务根密钥的生成应在密码模块中随机生成，密码模块的安全要求见 8.2；或通过安全介质由外部系统导入，安全介质可以采用智能 IC 卡或者智能密码钥匙等介质，具体格式不做要求，但需保障密钥导入的完整性和机密性。

#### 7.1.3 密钥分散

智能 IC 卡业务根密钥应分散生成智能 IC 卡级子密钥或下级机构子密钥，分散方式应支持一级分散和多级分散，分散因子的选择及分散过程参见附录 A。

#### 7.1.4 密钥分发

智能 IC 卡业务根密钥或者机构子密钥应采用安全介质保护的方式进行，安全介质可以采用智能

IC卡或者智能密码钥匙，下发过程需保障密钥下发的完整性和机密性。附录B中定义了一种采用密钥母卡和认证卡进行密钥下发的方式。

#### 7.1.5 密钥存储

智能IC卡业务根密钥应保存在密码模块中，密码模块的安全要求见8.2；或者使用系统存储保护密钥加密后保存在系统数据库中。

#### 7.1.6 密钥备份

智能IC卡业务根密钥应采用备份密钥库、备份根密钥合成因子到安全介质、备份根密钥分量到安全介质等多种方式。

#### 7.1.7 密钥归档

密钥超过使用期限或不再使用时，根据密钥管理策略可被归档。

密钥可采用下述形式归档：

a) 以至少两个分离的密钥分量形式分别存储于密码模块中；

b) 使用密钥加密密钥加密归档密钥。

已归档密钥使用要求：

a) 只能用于证明在归档前进行的交易的合法性；

b) 不应返回到操作使用中；

c) 不能影响在用的密钥的安全。

#### 7.1.8 密钥销毁

应支持对过期、已经泄露或者其他原因不再使用智能IC卡业务的根密钥进行销毁操作。

### 7.2 非对称密钥安全机制

#### 7.2.1 概述

智能IC卡密钥管理系统还应对发卡机构公私钥对和智能IC卡公私钥对进行整个生命周期的管理，包括密钥生成、密钥分发、密钥存储、密钥备份、密钥归档、密钥销毁。

#### 7.2.2 密钥生成

发卡机构公私钥对和智能IC卡公私钥对应在密码模块中生成，智能IC卡密钥管理系统应支持预生成智能IC卡公私钥对，密码模块的安全要求见8.2。

#### 7.2.3 密钥分发

发卡机构私钥仅存储在智能IC卡密钥管理系统中，无需进行分发；智能IC卡私钥应分发到数据准备系统及智能IC卡发卡系统中，分发过程应采用系统传输保护密钥加密后分发；发卡机构公钥证书和智能IC卡公钥证书可直接分发到数据准备系统及智能IC卡发卡系统中。

发卡机构智能IC卡密钥管理系统导入发卡机构证书时，应验证其有效性，包括验证有效期、验证数字签名。导入根证书时，应验证根证书签发机构的可信和根证书的有效性，包括验证证书有效期、验证数字签名等。

#### 7.2.4 密钥存储

发卡机构公私钥对应保存在密码模块中，密码模块的安全要求见8.2。预生成的智能IC卡公私钥

对应使用系统存储保护密钥加密，以密文形式存储在系统数据库中。

#### 7.2.5 密钥备份

发卡机构私钥应采用密码模块本身的密钥备份机制进行备份。

智能IC卡私钥应采用备份密钥库方式进行备份。

#### 7.2.6 密钥归档

发卡机构公私钥对不再使用后应进行密钥归档。

已经签发了智能IC卡证书的智能IC卡公私钥对应进行密钥归档。

#### 7.2.7 密钥销毁

应支持对过期、已经泄露或者其他原因不再使用的非对称密钥进行销毁操作。

## 8 系统安全要求

### 8.1 建设原则

建设原则要求包括：

——系统应遵循标准化、模块化的建设原则；

——系统应设置相对独立的功能模块，实现各项功能；

——各模块产生的审计日志文件应采用统一的格式传递和存储；

——系统应具备访问控制机制；

——系统在实现密钥安全管理功能的同时，应充分考虑系统本身的安全性；

——系统的安全建设建议按照各行业主管部门的建设要求，结合建设方实际情况，参考信息系统等级保护具体的安全要求对系统进行定级，并遵循相应的等级进行安全建设。

### 8.2 密码应用要求

#### 8.2.1 概述

智能IC卡密钥管理系统的密码应用要求整体应遵循GB/T 39786。

#### 8.2.2 密码算法

密码算法要求包括：智能IC卡应用中使用的密码算法，应采用国家密码管理主管部门批准的密码算法，具体的密码算法包括但不限于以下密码算法：

——签名算法应使用SM2，应遵循GB/T 32918；应使用SM9，应遵循GM/T 0044；

——杂凑算法应采用SM3算法，应遵循GB/T 32905；

——数据加解密应采用SM4分组密码算法，应遵循GB/T 32907。

#### 8.2.3 密码模块

密码模块包括下列要求。

a） 整体要求；

系统使用的密码模块，应是依法接受检测认证，经商用密码认证机构认证合格的密码模块，并在使用过程中保证私钥和对称密钥不以明文形态出现在密码模块外。

b） 密码功能要求：

1） 产生随机数：生成指定长度的随机序列，产生的随机数应符合 GB/T 32915 要求；

2） 密钥生成：生成指定算法类型和长度的密钥，分散产生子密钥；

3） 非对称密码运算：加密、解密、签名、验签、密钥协商；

4） 对称密码运算：数据加密、解密；

5） 密码杂凑运算：密码杂凑生成、验证；

6） 消息鉴别码运算：消息鉴别码生成、验证；

7） 分散产生子密钥并被传输密钥加密、生成公私钥对并传输密钥加密私钥分量等。

c） 接口要求。

密码模块服务接口应遵循 GB/T 36322 或 GM/T 0045。

# 附 录 A
（资料性）
## 分散因子及分散过程描述

利用16字节的主密钥(MK)分散得到子密钥(SK)的过程及选择的分散因子描述如下。

a) 由根密钥管理系统管理的业务根密钥分散得到发卡机构级别的业务根密钥时，分散因子宜采用发卡机构编码；发卡机构如果有多级，则每级分散因子采用各自的机构编码；由发卡机构密钥管理系统管理的业务根密钥分散得到卡片密钥时，分散因子宜采用主账号(PAN)和主账号序列号组成，记为X。

b) 若X的长度小于16个数字，X右对齐，在最左端填充十六进制的'00'以获得8字节的Y。若X的长度至少有16个数字，则Y由X的最右边的16个数字组成。

c) 计算Z:=SM4(MK)[Y||(Y('FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'))]，16字节的子密钥SK就等于Z。

子密钥分散流程见图A.1。

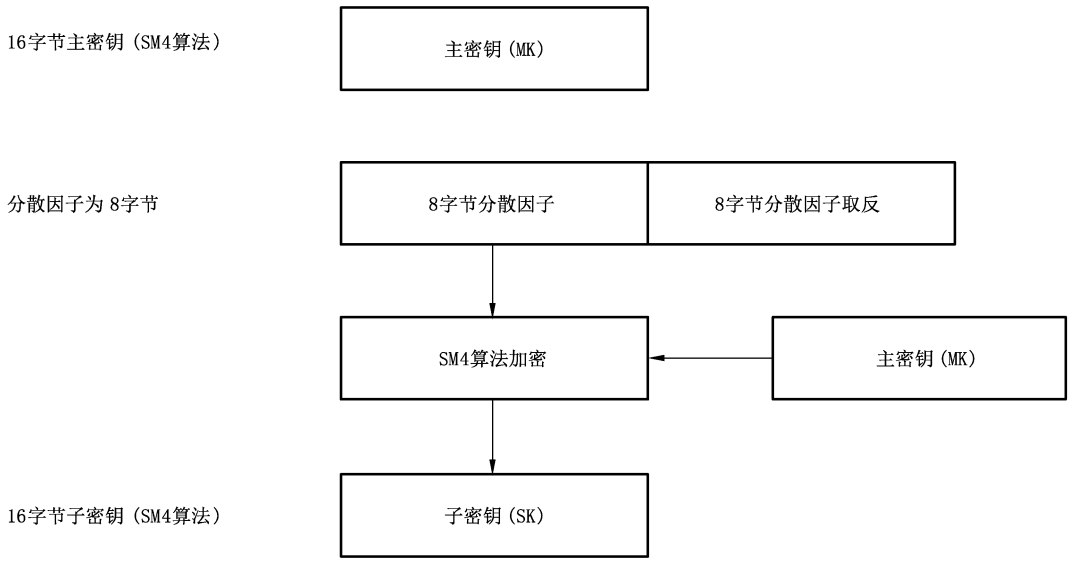


图 A.1 子密钥分散过程

# 附 录 B
（资料性）
## 密钥下发机制（采用密钥母卡及认证卡的方式）

密钥管理系统采用密钥母卡及认证卡完成对称密钥的下发，具体的安全机制包括：

a） 认证卡和密钥母卡中写入同样的认证密钥，密钥母卡中存储有下发的业务密钥，密钥认证卡配套密钥母卡使用；

b） 密钥认证卡采用口令进行安全权限校验，只有口令校验通过后，才可以使用认证密钥计算认证密文；

c） 密钥母卡采用密钥认证进行安全权限校验，只有采用认证密钥校验认证密文通过后，才可以将密钥母卡中存储的业务密钥导出，业务密钥以密文的形式可以直接导入到密钥管理系统中或者密钥管理系统配套的密码模块中。

具体的应用流程见图 B.1。

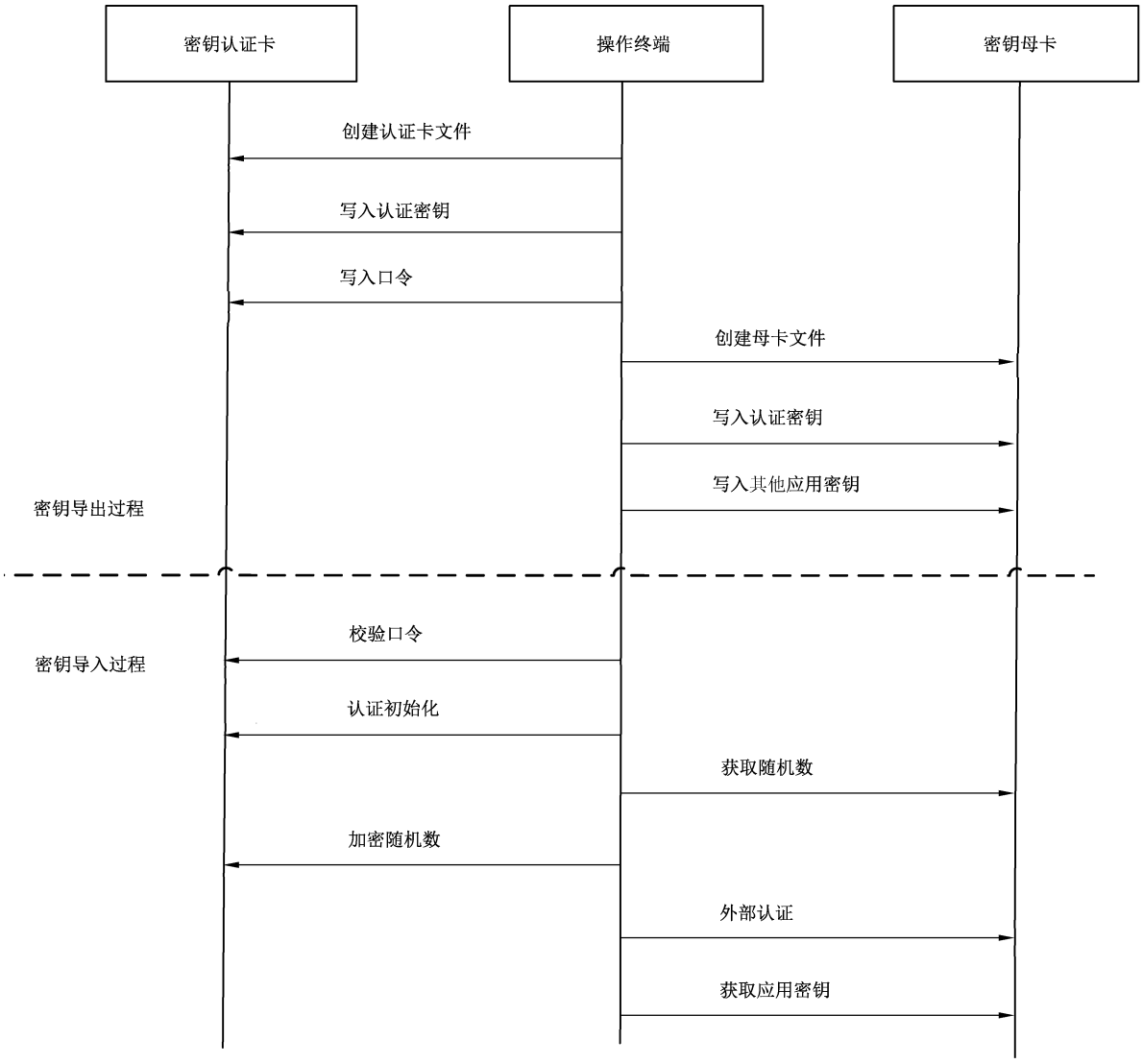


图 B.1 采用密钥母卡及认证卡进行密钥下发机制流程

# 参 考 文 献

[1] JR/T 0025—2018 中国金融集成电路(IC)卡规范
[2] JT/T 978 城市公共交通 IC 卡技术规范