ICS 35.040
L 80
备案号：

中华人民共和国密码行业标准

GM/T XXXX—XXXX

金融IC卡密钥管理系统技术规范

Financial IC card Key Management System technology Specification

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

××××-××-××发布　　××××-××-××实施

国家密码管理局 发布

目　次

前　言

本标准依据GB/T1.1-2009给出的规则起草。

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这些专利的责任。

本标准中的附录A、附录B、附录C、附录D为规范性附录。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：北京江南天安科技有限公司、中金金融认证中心有限公司、北京宏基恒信科技股份公司、上海格尔软件股份有限公司、中钞格尔金融卡科技有限公司。

本标准起草人：齐志峰、董纪伟、王晨、李国、朱家雄、韩小军、谭武征、韩琳、王晓英、王莎。

金融IC卡密钥管理系统技术规范

1 范围

本标准规定了金融 IC 卡应用的密钥体系、安全机制，以及金融 IC 卡密钥管理系统的系统设计、系统功能、系统安全等有关内容。

本标准适用于指导金融 IC 卡密钥管理系统的设计、开发和使用。

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 0025-2013 中国金融集成电路（IC）卡规范（PBOC3.0）

GM/T 0002-2012 SM4 分组密码算法

GM/T 0003-2012 SM2 椭圆曲线公钥密码算法

GM/T 0004-2012 SM3 密码杂凑算法

GM/T 0006-2012 密码应用标识规范

GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范

GM/T 0020-2012 证书应用综合服务接口规范

3 术语和定义

下列术语和定义适用于本规范。

3.1

非对称密码技术 asymmetric cryptographic technique

加密和解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密，且由公钥求解私钥是计算不可行的。

3.2

发卡机构标识代码 bank identification number

用于标识发卡机构的代码。

3.3

认证中心 certification authority

对数字证书进行全生命周期管理的实体, 也称为电子认证服务机构。

3.4

证书 certificate

也称公钥证书，由认证中心（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.5

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.6

IC 卡 integrated circuit(s) card

实现密码运算和密钥管理的含CPU（中央处理器）的集成电路卡。

3.7

发卡机构 issuer

开展IC卡发卡业务的服务机构。

3.8

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

3.9

公钥 public key

非对称密码算法中可以公开的密钥。

3.10

公钥证书 public key certificate

由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.11

密钥管理 key management

根据安全策略，对密钥的产生、登记、认证、注销、分发、安装、存储、归档、撤销、衍生和销毁等操作制定并实施一组确定的规则。

3.12

SM2 算法 SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为256比特。

3.13

SM3 算法 SM3 algorithm

一种密码杂凑算法，其输出为256比特。

3.14

SM4 算法 SM4 algorithm

一种分组密码算法，其分组长度为128比特，密钥长度为128比特。

3.15

管理员 administrator

管理员负责密钥管理系统的配置和维护工作，对系统使用者进行授权，并负责密钥的生成、分发、备份和恢复等工作。

4 符号和缩略语

以下缩略语和符号适用于本规范：

IC：集成电路(Integrated Circuit)

MAC：报文鉴别码(Message Authentication Code)

PIN：个人识别码（Personal Identification Number）

PAN：主账号（Primary Account Number）

B：二进制(Binary)

Cn：压缩数字(compress numeric)

Var：变长(Variable)

5 密钥体系

5.1 概述

金融IC卡应用涉及到的密钥包括应用密钥、存储保护密钥和传输保护密钥。应用密钥用来安全保护金融IC卡应用数据；传输保护密钥用来安全传输应用密钥和敏感数据；存储保护密钥用来本地安全存储密钥数据。

6 应用密钥

6.1.1 密钥种类

金融IC卡的应用密钥有两类：

a） 基于数字证书的非对称密钥，实现对发卡机构和金融IC卡的认证；

b） 对称密钥，实现金融IC卡应用数据和卡片自身的安全性。

6.1.2 非对称密钥

对于借贷记或基于借贷记的金融IC卡应用，其非对称密钥体系是三级数字证书体系，如图1所示：

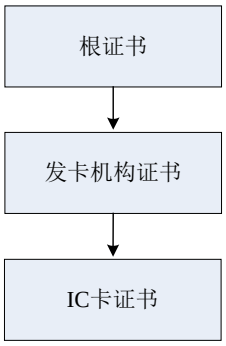

图1 金融IC卡应用的非对称密钥体系

IC卡证书由发卡机构签发,通过发卡机构证书进行验证;发卡机构证书由认证中心签发,通过根证书进行验证；根证书由认证中心自签发。

当IC卡作为认证终端设备时，IC卡中需要写入IC卡设备证书。IC卡设备证书由其业务系统的CA签发并认证。

对于应用密钥中的非对称密钥管理，金融IC卡密钥管理系统应具备以下功能：

a） 从认证中心安全获取根证书，并验证根证书的有效性；

b） 生成发卡机构的证书申请数据，并从认证中心安全获取发卡机构证书，验证发卡机构证书的有效性；

c） 生成并管理IC卡证书对应的公私钥对，并签发IC卡证书和静态应用数据。

5.2.3 对称密钥

金融IC卡应用的对称密钥包括应用密文密钥、安全报文认证密钥、安全报文加密密钥和主控密钥。各种密钥的作用如下：

a） 应用密文密钥,用于金融交易中产生应用密文，并用于卡片和发卡机构进行联机的卡认证和发卡机构认证；

b） 安全报文认证密钥，用于生成发卡后数据更新所需要的消息认证对话密钥，用于计算安全报文中的MAC值，进行校验发卡机构的脚本信息；

c） 安全报文加密密钥，用于生成发卡后更新机密数据（脱机PIN）进行加密的对话密钥，进行加密发卡机构的脚本机密信息；

d） 主控密钥用于保证卡片数据不被发卡机构之外的机构篡改。主控密钥分散生成卡片级密钥,用来实现卡片的个人化。主控密钥包括机构主控密钥和卡片主控密钥。

对于应用密钥中的对称密钥管理，金融IC卡密钥管理系统应具备以下功能：

a） 应用密文密钥、安全报文认证密钥、安全报文加密密钥三种密钥的获取、多级分散、子密钥下发；

b） 卡片主控密钥的获取、分发；

c） 机构主控密钥的获取、多级分散、子密钥下发。

5.3 传输保护密钥

金融IC卡应用涉及到的传输保护密钥包括发卡机构密钥交换密钥和数据加密密钥。这些密钥用于保证金融IC卡密钥管理系统和其关联系统之间应用密钥及敏感数据的机密性保护。密钥交换密钥用于保护金融IC卡密钥管理系统与数据准备系统之间应用密钥和敏感数据的机密性,数据加密密钥用于保护数据准备系统和个人化系统之间应用密钥和敏感数据的机密性。数据加密密钥并不是金融IC卡密钥管理系统进行维护管理的密钥。

对于传输保护密钥管理，金融IC卡密钥管理系统应具备以下功能：

a） 发卡机构密钥交换密钥的获取；

b） 使用发卡机构密钥交换密钥加密相关应用密钥及敏感数据。

5.4 存储保护密钥

存储保护密钥用于保障应用密钥和传输保护密钥在本地的存储安全性。存储保护密钥是发卡机构密钥管理系统硬件密码设备生成的密钥，如密码机的本地主密钥等。存储保护密钥并不是金融IC卡密钥管理系统进行管理维护的密钥。

金融IC卡密钥管理系统应能使用存储保护密钥加密本地存储的IC卡密钥数据。

6 安全机制

6.1 非对称密钥

6.1.1 概述

金融IC卡密钥管理系统应验证并管理根证书；管理发卡机构证书，包括申请、验证；管理IC卡证书的签发。同时，金融IC卡密钥管理系统还应对发卡机构公私钥对和IC卡公私钥对进行整个生命周期的管理。

6.1.2 密钥管理周期

金融IC卡密钥管理系统应采用国家密码管理局许可的硬件加密设备、国产商用密码算法、密钥管理安全协议、访问权限控制、日志审计等多种安全机制，保障密钥管理系统中所使用的非对称密钥，在密钥生成、存储、传输、使用、删除整个生命周期中的安全。

发卡机构公私钥对和IC卡公私钥对应在国家密码管理局许可的硬件加密设备中生成。

发卡机构公私钥对应保存在国家密码管理局许可的硬件加密设备中。金融IC卡密钥管理系统应支持预生成IC卡公私钥对。预生成的IC卡公私钥对应使用存储保护密钥加密，以密文形式存储在外部介质中。用过的IC卡公私钥对应及时删除。

金融IC卡密钥管理系统应能够签发IC卡证书和静态应用数据。IC卡证书及其对应的私钥在传输时应使用传输保护密钥加密保护,确保密钥数据的机密性,安全传输到外部关联系统。

金融IC卡密钥管理系统能够导入认证中心根证书并验证其有效性，包括验证证书有效期、验证数字签名。金融IC卡密钥管理系统能够导入发卡机构证书并验证其有效性，包括验证有效期、验证数字签名、检查CRL。

金融IC卡密钥管理系统使用的数字签名的产生和验签算法请参见附录A。

6.2 对称密钥

6.2.1 概述

对称密钥包括应用密钥中的应用密文密钥、安全报文认证密钥、安全报文加密密钥和主控密钥，以及传输保护密钥中的密钥交换密钥。

6.2.2 密钥生成

应用密文密钥、安全报文认证密钥、安全报文加密密钥和主控密钥的生成应在金融IC卡密钥管理系统的硬件加密设备中由随机因子合成，或随机生成。

密钥交换密钥既可在金融IC卡密钥管理系统的硬件加密设备中随机生成，也可由外部安全导入。

金融IC卡密钥管理系统应能够根据密钥索引关联指定应用密文密钥、安全报文认证密钥、安全报文加密密钥和主控密钥。

6.2.3 密钥备份

应用密文密钥、安全报文认证密钥、安全报文加密密钥和主控密钥的合成因子应以介质的方式存储在安全区域内。

6.2.4 密钥分散

应用密文密钥、安全报文认证密钥、安全报文加密密钥和主控密钥应能够分散生成IC卡级子密钥或下级机构子密钥。

应用密文密钥、安全报文认证密钥、安全报文加密密钥和主控密钥的分散算法请见附录B。

6.2.5 密钥下发

应用密文密钥、安全报文认证密钥、安全报文加密密钥和主控密钥分散的子密钥应能够安全传输到关联设备中。这些子密钥需要使用传输保护密钥加密，以密文形式传输到关联设备。

在多级机构框架下，应用密文密钥、安全报文认证密钥、安全报文加密密钥需要逐级分散为机构级子密钥，最后分散为卡片级子密钥。机构级子密钥在上级机构的密钥管理系中分散生成。机构子密钥需要从上级机构安全下发到本地机构。

机构级子密钥应使用安全方式进行下发，如密码信封、密钥传输卡等，以保障机构级子密钥下发的完整性和私密性保护。

6.2.6 密钥传输

密钥交换密钥由外部安全导入到金融IC卡密钥管理系统中时，应由金融IC卡密钥管理系统的发卡机构公钥加密保护。

6.2.6 密钥存储

应用密文密钥、安全报文认证密钥、安全报文加密密钥和主控密钥应保存在国家密码管理局许可的硬件加密设备，使用存储保护密钥加密保护。

7 系统设计

7.1 系统设计原则

系统应遵循标准化、模块化设计原则。

系统应设置相对独立的功能模块，实现各项功能。

各模块使用的密码运算应在密码设备中完成。

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功能。

系统在实现密钥管理功能的同时，应充分考虑系统本身的安全性。

应支持金融 IC 卡多应用的密钥管理。

7.2 系统框架

金融 IC 卡密钥管理系统由发卡机构证书管理模块、IC 卡证书管理模块、非对称密钥管理模块、对称密钥管理模块和机构密钥分级管理模块五个模块构成，如图 2 所示。

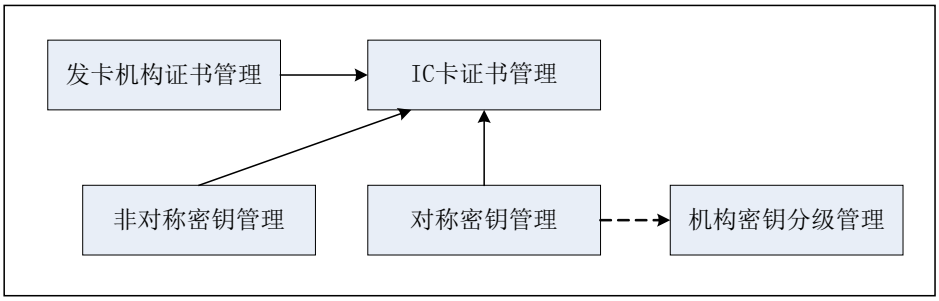

图2 金融IC卡密钥管理系统框架图

发卡机构证书管理模块应实现认证中心根证书的验证及导入、发卡机构证书申请数据的生成、发卡机构证书的验证及导入，以及发卡机构根证书的下发等功能。

IC 卡证书管理模块应实现 IC 卡证书的签发、IC 卡静态数据的签发等功能。

非对称密钥管理模块应实现管理维护 IC 卡公私钥对、发卡机构证书及其公私钥对，以及管理认证中心根证书等功能。

对称密钥管理模块应实现管理维护存储保护密钥、传输保护密钥和应用密钥等功能。

机构密钥分级管理模块应实现机构的定义和划分，机构密钥的管理。本模块是具体应用的可选模块。

7.3 外部关联

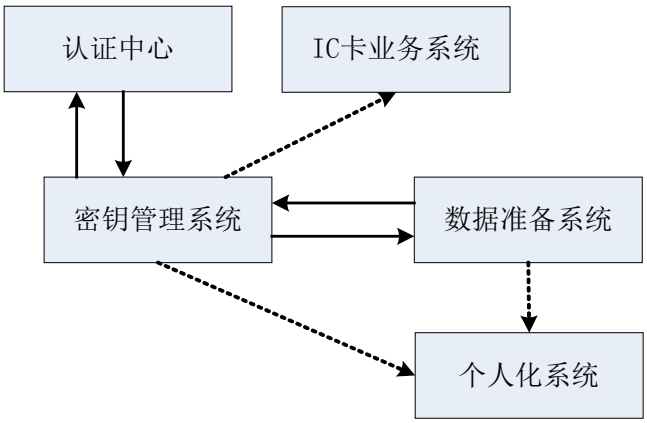

图3 金融IC卡密钥管理系统外部关联图

金融IC卡密钥管理系统应能够与认证中心、数据准备系统、个人化系统以及IC卡业务系统关联，配合完成金融IC卡的发卡及业务应用整体的安全保障，如图3所示。

下面介绍金融IC卡密钥管理系统与这些外部关联系统之间的业务关系：

a） 与认证中心：金融IC卡密钥管理系统能够与认证中心交互，实现发卡机构证书的注册、申请、下发；实现认证中心根证书的导入；

b） 与数据准备系统：金融IC卡密钥管理系统能够响应数据准备系统发来的IC卡密钥及证书、业务密钥的获取请求，生成IC卡公私钥对和业务密钥，签发IC卡证书，并下发给数据准备系统；

c） 与个人化系统：金融IC卡密钥管理系统能够下发主控密钥给个人化系统，供个人化系统写卡使用；

d） 与IC卡业务系统：金融IC卡密钥管理系统能够下发IC卡应用密钥给IC卡业务系统。

7.4 系统功能

7.4.1 发卡机构证书管理

能够导入认证中心根证书并验证其有效性，包括验证证书有效期、验证数字签名；

能够生成发卡机构证书申请数据并向认证中心提出证书申请；能够验证发卡机构证书并导入；

能够管理发卡机构公钥证书，包括归档、删除、导出。

7.4.2 IC卡证书管理

能够响应IC卡证书申请，生成IC卡证书申请数据并签发IC卡证书；能够支持在线或离线的IC证书签发；

能够签发IC卡静态数据。

7.4.3 非对称密钥管理

能够生成并管理IC卡公私钥对；需要支持预生成IC卡公私钥并管理；

能够生成并管理发卡机构公私钥对。

7.4.4 对称密钥管理

能够生成并管理各种对称密钥，包括应用密钥、存储保护密钥和传输保护密钥；

支持应用密钥的多级分散。

7.4.5 机构密钥分级管理

能够实现密钥管理机构的定义和划分，实现机构密钥的管理。

7.5 对外接口

7.5.1 与认证中心之间的接口

7.5.1.1 发卡机构证书申请数据格式和发卡机构证书格式

金融IC卡密钥管理系统应能够产生发卡机构证书申请数据，向认证中心申请发卡机构证书。

发卡机构证书申请数据格式、发卡机构证书格式参见附录C。

7.5.1.2 认证中心根证书格式

金融IC卡密钥管理系统应能够将认证中心根证书导入系统用于验证发卡机构证书。

认证中心根证书的格式参见附录C。

7.5.2 与数据准备系统之间的接口

IC卡公钥证书格式、IC卡静态数据签名格式和IC卡密钥数据的格式可参见附录D。

7.5.3 与个人化系统之间的接口

金融IC卡密钥管理系统应能够同步主控密钥到个人化系统，同步主控密钥的数据格式不做具体规定。

7.5.4 与IC卡业务系统之间的接口

金融IC卡密钥管理系统应能够同步业务密钥到IC卡业务系统，同步业务密钥的数据格式不做具体规定。

8 系统安全

8.1 密码算法

金融IC卡密钥管理系统本身的系统密钥应使用SM2、SM3、SM4算法。具体算法实现和使用请见GM/T 0002-2012、GM/T 0003-2012、GM/T 0004-2012等标准。

金融IC卡密钥管理系统管理的应用密钥的密码算法实现应参照具体的金融IC卡业务应用规范。

8.2 密码设备

金融IC卡密钥管理系统应使用国家密码管理局审批的密码设备。

8.3 系统要求

金融 IC 卡密钥管理系统所使用的操作系统，除满足服务器服务管理之外，其余功能或服务应全部关闭或裁减。

8.4 管理要求

8.4.1 管理工具

金融 IC 卡密钥管理系统应能够通过管理工具实现对该密钥管理系统的管理功能。

管理工具可安装密钥管理系统上，也可安装在密钥管理系统之外的管理终端上。

8.4.2 管理员管理

金融IC卡密钥管理系统的管理员应采用金融密码钥匙、金融IC卡等硬件装置与登录口令相结合的方式登录系统，也可使用证书进行身份验证。管理员通过身份认证后，才能进行初始化、系统配置、应用管理、密钥管理、日志审计等操作。

8.4.3 密钥管理人员角色

应设置下列管理和操作人员：

——超级管理员

——系统管理员

——业务管理员

——业务操作员

——审计管理员

——审计操作员

“超级管理员”负责金融IC卡密钥管理系统的策略设置，以及设置系统管理员、审计管理员和业务管理员，并对它们管理的业务范围进行授权。

“系统管理员”负责金融IC卡密钥管理系统的参数配置、系统服务启动和停止，不具有业务操作的权限。

“业务管理员”负责金融IC卡密钥管理系统的业务管理，包括发卡机构证书和工作主密钥的管理、IC卡公私对的生成及管理，以及传输密钥的管理；并设置业务操作员并对其操作的权限进行授权。

“业务操作员”按其权限进行具体的业务操作，包括导入密钥申请数据文件、签发IC卡密钥与证书，以及查询统计IC卡签发情况等。

“审计管理员”负责金融IC卡密钥管理系统的审计管理，设置审计操作员并对其操作的权限进行授权。

“审计操作员”负责对涉及系统安全的事件和各类管理和操作人员的行为进行审计和监督。

上述各类人员使用证书进行登录，其中“超级管理员”“系统管理员”“业务管理员”和“审计管理员”的证书应在系统进行初始化时同时产生。

8.4.4 设备管理

金融IC卡密钥管理系统的初始化，除必须由厂商进行的操作外，系统配置、密钥的生成（恢复）与安装、生成管理员等均应由用户方设备管理人员完成。

8.5 日志和审计要求

日志应记录事件发生的时间、事件的操作者、操作类型及操作结果等信息。应能按时间、操作者、操作类型等对日志进行分类或综合查询。

应提供审计管理的界面，能够对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计。审计数据应能归档且不能被篡改。

8.6 网络部署要求

金融 IC 卡密钥管理系统应部署为独立网络，对外应仅能连接数据准备系统，不能连接

到外部网络。

部署防病毒服务器、入侵检测探测设备，并通过防火墙与数据准备系统连接。

8.7 环境安全要求

密钥管理系统应部署在单独的安全区域；此安全区域应设置监控探头、消防探头、门禁系统以及保险柜等设施，并设置监控室对区域进行实时监控。

在安全区域放置密钥管理服务器及连接的密码机、数据库服务器以及管理终端；并应在醒目的位置标识出设备在系统中的名称。

附录 A
（规范性附录）
数字签名的产生及验证

A.1 算法标识

使用《GM/T2012-0003 SM2椭圆曲线公钥密钥算法》标准进行数字签名和验证。SM2签名方案使用下面三种函数：

——一个依赖于私钥 S_K 的签名函数 Sign(S_K)[M]，该函数输出两个相同长度的数字 r 和 s；

——一个依赖于公钥 P_K 的验证函数 Verify(P_K)[M, Sign(S_K)[M]]，该函数输出 True 或 False，表示验证正确或失败；

——一个杂凑算法 SM3[ ]，将任意长度的报文映射为一个 32 字节的杂凑值。

A.2 数字签名产生

对任意长度的数据组成的报文MSG计算签名S的过程如下：

1) 计算Z_A=SM3[$ENTL_A$ || ID_A || a || b || x_G ||y_G || x_A || y_A]。其中ID_A固定设置为16字节定长的十六进制数据0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38, 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38；$ENTL_A$值为两个字节数据0x00, 0x80；
2) 计算报文MSG的32字节的HASH值 h:= SM3 [Z_A||MSG]；
3) 计算Sign(S_K)[h]，得到两个数字r和s；
4) 数字签名S被定义为S := $r||s$，即数字签名S由数字r和s串联而成。

A.3 数字签名验证

对任意长数据组成的报文MSG验证签名S的过程如下：

1) 计算Z_A=SM3[$ENTL_A$ || ID_A || a || b || x_G ||y_G || x_A || y_A]。其中ID_A固定设置为16字节定长的十六进制数据0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38, 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38；$ENTL_A$值为两个字节数据0x00, 0x80；
2) 计算报文MSG的32字节的HASH值 h:= SM3 [Z_A||MSG]；

Verify(P_K)[h, S]，若函数输出True表示验证正确，若输出False，表示验证失败。

附录 B
（规范性附录）
密钥分散机制

B.1 算法标识

——分组密码算法 SM4[ ]，使用 GM/T2012-0002《SM4 分组密码算法》标准。

B.2 输入参数

发卡机构主密钥，如应用密文密钥、安全报文认证密钥、安全报文加密密钥和主控密钥等，必须为16字节。；

IC卡的主账户及其序列号，以主账号和主账号序列号（如果主账号序列号不存在，则用一个字节“00”代替）的最右16个数字。

B.3 算法说明

1) 如果主账号和主账号序列号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“0”以获得8字节的Y。如果X的长度至少有16个数字，那么Y由X的最右边的16个数字组成。

2) 计算

Z：=SM4(IMK)[Y||(Y⊕(‘FF’||‘FF’||‘FF’||‘FF’||‘FF’||‘FF’||‘FF’||‘FF’))]

16字节的IC卡子密钥MK就等于Z。

附录 C
（规范性附录）
金融 IC 卡密钥管理系统与认证中心之间的消息格式

C.1 发卡机构证书申请数据

C.1.1 文件命名

发卡机构证书申请数据文件的文件名格式为：“YLTTTTTT.INP”。其中“YL”为前缀；“TTTTTT”是记录号，唯一标识一个发卡机构的一次公钥证书申请，由银联或行业管理机构统一管理和分发，发卡机构必须使用该记录号。例如：YL123456.INP。

C.1.2 发卡机构证书申请数据格式

发卡机构证书申请数据采用自签名方式，发卡机构利用所申请发卡机构证书对应的私钥对该发卡机构证书申请数据进行签名。认证中心使用该发卡机构证书申请数据中的公钥来验证签名。

表 C.1 发卡机构证书申请数据

字段名	长度（字节）	描述	格式
记录头	1	十六进制，值为‘23’	b
服务标识	4	标识一个中国银联借记贷记服务，将相应应用的私有应用标识扩展(PIX)，右补十六进制‘0’构成。 ‘01010000’ = 借、贷记 ‘01010100’ = 借记 ‘01010200’ = 贷记 ‘01010300’ = 准贷记	b
证书格式	1	十六进制‘12’	b
发卡机构标识	4	主帐号（PAN）最左面的 3-8 个数字。（不足部分右补十六进制数‘F’）	cn 8
证书失效日期	2	月和年(MMYY)，在该月最后一天之后证书失效	n 4
记录号	3	发卡机构公钥证书申请记录号	n 6
发卡机构公钥签名算法标识	1	标识发卡机构公钥签名算法，参见附录 A 算法标识	b
发卡机构公钥加密算法标识	1	标识发卡机构公钥加密算法，保留项	b
公钥参数标识	1	用于标识椭圆曲线参数	b
发卡机构公钥长度	1	SM2 算法为 64 字节	b
发卡机构公钥	N_I	SM2 算法表示椭圆曲线上的一个点	b
数字签名	N_I	发卡机构使用其私钥对本表从记录头依顺序到发卡行机构公钥的数据计算的 SM2 签名 r||s	b

C.2 发卡机构证书文件

发卡机构公钥证书文件由两部分组成，第一个部分是认证中心对发卡机构签发的发卡机构证书数据，第二个部分是未签名的扩展数据。

C.2.1 文件命名

发卡机构证书文件名格式为：AAAAAA.INN。其中：“AAAAAA”是申请记录号，与本规范第C.1.1节自签名发卡机构证书申请数据文件中的记录号相同；I是固定值(‘I’)表示发卡机构；NN是用来签发发卡机构公钥证书的认证中心公钥的索引。例如：010101.I01。

C.2.2 文件内容

发卡机构公钥证书输出文件由三部分组成，第一部分是未签名发卡机构公钥输出扩展，第二个部分是根CA对发卡机构公钥证书的签名，第三个部分是根CA公钥单独签名。针对RSA算法的格式和内容参见Q/CUP 046.6.2-2012。针对SM2算法的根CA公钥证书输出文件格式如表3所示。

表 C.2 发卡机构公钥证书输出文件

字段名	长度（字节数）	描述
未签名发卡机构公钥输出扩展	6	见 7.3.1 节
签名的发卡机构公钥证书	$N_{CA}+N_I+14$	见 7.3.2 节
根 CA 单独签名	N_{CA}	见 7.3.3 节

C.2.2.1 签名的发卡机构证书

认证中心签发的发卡机构证书数据是发卡机构证书文件的第一部分，由认证中心利用相应认证中心私钥对下表中的发卡机构证书申请数据进行签名产生。

表 C.3 根 CA 使用 SM2 算法签名的发卡机构公钥证书数据

字段名	长度	描述	格式
证书格式	1	十六进制，值为‘12’	b
发卡行标识	4	主账号最左面的 3-8 个数字（在右边补上十六进制数‘F’）	cn 8
证书失效日期	2	MMYY，在此日期后，这张证书无效	n4
证书序列号	3	由根 CA 分配给这张证书的，唯一的二进制数	b
发卡行公钥签名算法标识	1	标识发卡机构公钥加密算法，参见附录 A 算法标识	b
发卡行公钥加密算法标识	1	标识发卡行公钥对应的加密算法，暂不使用，取值‘00’	b
发卡行公钥参数标识	1	用于标识椭圆曲线参数	b
发卡行公钥长度	1	标识发卡行公钥的字节长度	b
发卡行公钥	N_I	该字段是椭圆曲线上的一个点	b
数字签名	N_{CA}	根 CA 对本表 1 至 9 项数据计算的 SM2 签名 r||s	b

根CA对表5中表1至9项的数据进行签名，形成了发卡行公钥证书。

C.2.2.2 未签名的扩展数据

未签名发卡机构公钥输出扩展是发卡机构公钥输出文件的第一部分，其格式见表4。该公钥输出扩展提供了该发卡机构公钥证书信息。

表 C.4 未签名发卡机构公钥输出扩展

字段名	长度	描述	格式

字段名	长度	描述	格式
记录头	1	十六进制，值为‘24’	b
服务标识	4	标识一个中国银联借记贷记服务,将相应应用的私有应用标识扩展(PIX)，右补十六进制‘0’构成。 ‘01010000’ = 借、贷记 ‘01010100’ = 借记 ‘01010200’ = 贷记 ‘01010300’ = 准贷记	b
根 CA 公钥索引	1	根 CA 系统用来签发发卡机构公钥证书的公钥索引	b

C.3 认证中心根证书文件

C.3.1 文件命名

认证中心根证书公钥文件名格式为：01010000.CAA。其中：
——01010000 标识银联借记/贷记服务；
——C 标识中国银联；
——AA 为认证中心的公钥索引，以 0xAA 表示。
例如：01010000.C01。

C.3.2 文件内容

认证中心公钥文件是二进制数据，其格式和内容如下表所示。

表 C.5 认证中心公钥文件格式

字段名	长度（字节数）	描述
自签名认证中心公钥	$N_{CA}+N_{CA}+15$	见下表

C.3.2 自签名认证中心公钥

自签名认证中心公钥是认证中心按照JR/T 0025-2013《中国金融集成电路（IC）卡规范（PBOC3.0）》第七部分第12章规定的签名算法利用认证中心签名私钥对其公钥证书数据（对下表进行签名所得）。

表 C.6SM2 算法根 CA 公钥证书格式

字段名	长度（字节数）	描述	格式
记录头	1	十六进制，值为‘21’	b
服务标识	4	标识一个中国银联借记贷记服务，将相应应用的私有应用标识扩展(PIX)，右补十六进制‘0’构成。 ‘01010000’= 借、贷记 ‘01010100’= 借记 ‘01010200’= 贷记 ‘01010300’= 准贷记	b
注册的应用提供商标识 (RID)	5	标识银联 RID：为十六进‘A000000333’	b
根 CA 公钥索引	1	唯一标识根 CA 公钥	b

字段名	长度（字节数）	描述	格式
证书失效日期	2	月和年(MMYY)，在该月最后一日之后证书失效	n 4
根 CA 公钥算法标识	1	标识根 CA 公钥对应的数字签名算法，（参见附录 A 算法标识）	b
公钥参数标识	1	用于标识椭圆曲线参数	b
根 CA 公钥长度	1	根 CA 公钥长度（64 字节）	b
根 CA 公钥	N_{CA}	该字段是椭圆曲线上的一个点	b
数字签名	N_{CA}	根 CA 对本表 1 至 9 项(即从记录头到根 CA 公钥）的数据计算的 SM2 签名 r||s	b

附录 D
（资料性附录）
金融 IC 卡密钥管理系统与数据准备系统之间的消息格式

金融 IC 卡密钥管理系统和数据准备系统之间有两种形式的接口：在线实时接口和离线文件接口。在线实时接口适用于在线即时签发 IC 卡证书；离线文件接口适用于大规模批量签发 IC 证书。

D.1 IC卡密钥与证书申请数据

IC 卡密钥与证书申请数据采用文本文件格式，字段之间采用“|”分割。

表 D.1 IC 卡密钥与证书申请数据

字段名	长度（字节）	描述	格式
发卡机构 BIN 号	4	发卡机构BIN，在右边填充十六进制值'F'。即主帐号（PAN）最左面的3-8 个数字。	cn 8
应用类别	1	发卡应用类型：01 表示标准 PBOC，02 表示电子现金，03 表示 qPBOC。	b
数据验证代码 DAC	2	发卡机构指定数值	b
证书格式	1	此域值为两种： 03 ：仅签发卡片静态数据签名 04 ：签发卡片证书和静态数据	b
证书有效期	2	MMYY，在此日期后，这张证书无效	n 4
分散密钥索引	1	对称密钥索引	b
发卡机构证书序列号	3	用于签发该卡片证书或卡片静态签名的发卡机构私钥对应的发卡机构证书序列号	b
IC 卡公钥模长	1	标识 IC 卡公钥的模的字节长度	b
签名的静态应用数据列表	用于表示签名的静态数据项的Tag顺序，Tag 之间用逗号“,”分割，不足后补空格（0x20）。	静态应用数据（规范推荐如下：） Tag:82---应用交互特征 AIP（如果支持 DDA） Tag:5F24--应用终止日期 Tag:5F25--应用有效日期 Tag:5A--应用主账户 (PAN) Tag: 5F34--应用主账户序列号 Tag:9F07--应用用途控制 AUC Tag:8E--持卡人验证方法（CVM）列表 Tag:9F0D--发卡机构行为代码（IAC）——缺省 Tag:9F0E--发卡机构行为代码（IAC）——拒绝 Tag:9F0F--发卡机构行为代码（IAC）——联机 Tag:9F28--发卡机构国家代码(若有应用用途控制则有此项) 字段内容意义和详细说明参见《中国金融集成电路（IC）卡借记/贷记规范第一部分：卡片规范》	

金融 IC 卡密钥管理系统根据申请信息签发静态签名数据、IC 卡公钥证书和 IC 卡密钥数据，

并将这三部分数据通过离线或在线的方式发送给数据准备系统。

D.2 静态签名文件

D.2.1 文件命名

静态签名文件的文件名格式行如：“AAAAAAAAAA_BB.SSADNNNNNN”。其中“AAAAAAAAAA”为卡片主帐号（PAN）；“BB”是应用类别，“SSAD”为后缀，“NNNNNN”标识密钥管理系统签发该静态签名使用的发卡机构证书序列号。例如：6205182900000288_01.SSAD000189。

D.2.2 文件内容

表 D.2 静态签名文件格式

字段名	长度（字节）	描述
签名的卡片静态应用数据	N_I	发卡机构密钥管理系统利用相应发卡机构私钥对下表中的卡片公钥数据进行签名产生。
签名数据格式	1	十六进制，值为‘23’，表示为 SM2 签名
数据验证代码	2	由发卡机构分配的代码
静态签名应用数据	变成	所包含的数据项由发卡机构定义（可从 IC 卡密钥及信息数据文件中的静态签名数据 Tag 列表了解此域所包括的数据项），此域数据可从发卡机构签发请求输入文件中直接获取。

D.3IC卡公钥文件

D.3.1 文件命名

IC 卡公钥文件的文件名格式行如：“AAAAAAAAAA_BB.ICNNNNNN”。其中“AAAAAAAAAA” 为卡片主帐号（PAN）；“BB”是应用类别，“IC”为后缀，“NNNNNN”标识密钥管理系统签发该 IC 卡公钥证书使用的发卡机构证书序列号。例如：6205182900000288_01.IC000189。

D.3.2 文件内容

签名的卡片公钥证书由发卡机构利用相应发卡机构私钥对表 14 中的卡片公钥数据进行签名产生。

表 D.3 IC 卡公钥文件

字段名	长度	描述	格式
证书格式	1	十六进制，值为‘14’	b
应用主帐号	10	主帐号（在右边补上十六进制数‘F’）	cn 20
证书失效日期	2	MMYY，在此日期后，这张证书无效	n4
证书序列号	3	由发卡机构分配给这张证书的唯一的二进制数	b
保留项	1		b
IC 卡公钥算法标识	1	标识使用在 IC 卡公钥上的数字签名算法	b
IC 卡公钥长度	1	标识 IC 卡公钥的字节长度	b
保留项	1		b
IC 卡公钥	N_{IC}	IC 卡公钥值，长度为 N_{IC}	b
签名值	N_I	发卡机构私钥对上述数据的签名值，长度为 N_I	b

D.4 IC卡密钥文件

D.4.1 文件命名

IC卡密钥文件的文件名格式行如:“AAAAAAAAAA_BB.KEYNNNNNN”。其中“AAAAAAAAAA”为卡片主帐号（PAN);“BB”是应用类别，“KEY”为后缀，“NNNNNN”标识密钥管理系统签发该密钥对应的IC卡公钥证书使用的发卡机构证书序列号。例如：6205182900000288_01.KEY000189。

D.4.2 文件内容

文件采用DOS文本文件格式，数据字段之间,用“|”(0x7C)分割。数据内容如下：

表D.4 IC卡密钥文件

字段名	长度（字节）	描述	格式
发卡机构对称密钥索引	1	标示发卡机构密钥管理中心使用哪对对称密钥	b
分散出的应用子密钥	var	使用发卡机构应用主密钥根据PAN和序列号分散出的子密钥	使用密钥加密密钥加密，并做Base64编码
分散出的加密子密钥	var	使用发卡机构加密主密钥根据PAN和系列号分散出的子密钥	
分散出的数据认证子密钥	var	使用发卡机构认证主密钥根据PAN和系列号分散出的子密钥	
发卡机构控制的卡片主密钥KMU	var	发卡机构控制的卡片主密钥KMU	
静态应用数据列表	var	IC卡申请签发数据中SAD	b
IC卡私钥	var	IC私钥	使用密钥加密密钥加密，并做Base64编码