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。