



# 中华人民共和国密码行业标准

GM/T 0086—2020

---

## 基于 SM9 标识密码算法的密钥管理系统 技术规范

Specification of key management system  
based on SM9 identity cryptography algorithm

2020-12-28 发布

2021-07-01 实施

---

国家密码管理局 发布

## 目 次

前言 .....	III
引言 .....	IV
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	3
5 基本特征描述 .....	3
6 标识密钥管理系统架构 .....	3
7 标识密钥管理系统组成与功能 .....	4
7.1 私钥生成系统 .....	4
7.2 注册服务系统 .....	5
7.3 公开参数服务系统 .....	6
7.4 终端实体 .....	7
7.5 本地代理 .....	7
8 密钥管理基本要求 .....	7
8.1 密钥申请登录认证 .....	7
8.2 密钥生成 .....	7
8.3 密钥传输 .....	8
8.4 密钥存储 .....	8
8.5 密钥更新 .....	8
8.6 密钥注销 .....	8
8.7 密钥备份 .....	8
8.8 密钥恢复 .....	8
8.9 系统主密钥管理 .....	9
9 标识密钥管理系统密码使用 .....	9
9.1 密码算法使用 .....	9
9.2 密码设备 .....	9
10 密钥管理安全操作流程 .....	10
10.1 系统初始化流程 .....	10
10.2 密钥载体初始化 .....	10
10.3 用户密钥生成流程 .....	10
10.4 标识状态发布流程 .....	11
10.5 更新用户标识密钥状态流程 .....	12
10.6 恢复用户标识密钥状态流程 .....	12
10.7 用户信息状态查询与响应流程 .....	12
10.8 主密钥更新流程 .....	13

11	标识密钥管理系统建设与安全防护	13
11.1	系统建设	13
11.2	安全防护设置	13
12	安全管理要求	15
12.1	安全管理机制	15
12.2	人员管理	15
12.3	管理制度	16
12.4	审计管理	16
12.5	管理平台	16
13	标识密钥管理系统层次结构	16
13.1	标识密钥管理系统类型	16
13.2	区分 KMS 的标识	17
13.3	注册下级 KMS	17
13.4	下级 KMS 主密钥生成流程	17
13.5	下级 KMS 主密钥发布	18
13.6	验证 KMS 主密钥	18
附录 A (规范性)	密码算法的 OID 与算法标识	19
附录 B (资料性)	标识密钥管理系统网络结构	20
附录 C (资料性)	用户第一次申请密钥流程	21
参考文献		23

## 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：上海信息安全工程技术研究中心、北京国脉信安科技有限公司、航天信息股份有限公司、深圳奥联信息安全技术有限公司、三未信安科技发展有限公司。

本文件主要起草人：袁文恭、袁峰、王晓春、郭宝安、蔡先勇、张岳公、封维端、张立圆、王学进、蒋楠、药乐、陈祎。

## 引 言

本文件依据我国 SM9 标识密码算法的应用需求而制定,给出了基于 SM9 标识密码的标识密钥管理系统(简称标识密钥管理系统)完整的架构包含组成说明、功能要求和技术规范,还给出了用户标识密钥(本文件中特指私钥)的申请、生成、签发、下载、更新、作废、验证以及公开参数查询等实现流程。

# 基于 SM9 标识密码算法的密钥管理系统 技术规范

## 1 范围

本文件规定了基于 SM9 标识密码算法的密钥管理系统架构及其建设要求。该架构可作为基于标识密码应用的普适性基础标准,为其提供密钥生成、管理以及公开参数查询等服务。

本文件适用于指导基于 SM9 标识密码的标识密钥管理系统设计、建设和管理,也可以用于相关系统的检测。

## 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 2887—2011 计算机场地通用规范  
 GB/T 9361—2011 计算机场地安全要求  
 GB 50174—2017 数据中心设计规范  
 GB/T 24363 信息安全技术 信息安全应急响应计划规范  
 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/Z 24364 信息安全技术 信息安全风险管理指南  
 GM/T 0044(所有部分) SM9 标识密码算法  
 GM/T 0057 基于 IBC 技术的身份鉴别规范  
 GM/Z 4001 密码术语

## 3 术语和定义

GM/T 0044(所有部分)和 GM/Z 4001 界定的以及下列术语和定义适用于本文件。

### 3.1

#### 鉴别 authentication

确认一个实体所声称的身份或属性。

### 3.2

#### 鉴别凭证 authentication credentials; AC

对用户进行身份鉴别时,被鉴别方提供的有效可信证据。

### 3.3

#### 双线性对 bilinear pairing

线性空间上的一种函数,其定义为:设  $V$  是数域  $F$  上的一个线性空间, $f(\alpha, \beta)$  是  $V$  上一个二元函数,对  $\forall \alpha, \beta \in V$ ,  $f$  确定  $F$  中唯一的数  $f(\alpha, \beta)$  与之对应。若对  $\forall \alpha, \alpha_1, \alpha_2, \beta, \beta_1, \beta_2 \in V, k_1, k_2 \in F$ ,  $f(\alpha, \beta)$  满足  $f(\alpha, k_1\beta_1 + k_2\beta_2) = k_1f(\alpha, \beta_1) + k_2f(\alpha, \beta_2)$ ; 和  $f(k_1\alpha_1 + k_2\alpha_2, \beta) = k_1f(\alpha_1, \beta) + k_2f(\alpha_2, \beta)$ , 则称  $f(\alpha,$