ICS 35.040
CCS L 80

GM

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

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$f(\alpha,$