ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0080—2020

SM9 密码算法使用规范

SM9 cryptographic algorithm application specification

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、深圳奥联信息安全技术有限公司、无锡华正天网信息安全系统有限公司。

本文件主要起草人：袁峰、王晓春、封维端、张立圆、王学进、药乐、蒋楠、程朝辉、蔡先勇、王一曲。

引　言

本文件是IBC(Identity-Based Cryptography)基于标识的密码技术系列标准之一,及依托于GB/T 38635.2《信息安全技术　SM9标识密码算法　第2部分:算法》。

本文件的目标是保证SM9密码算法使用的正确性,为SM9密码算法的使用制定统一的数据格式和使用方法。

本文件从算法应用的角度给出SM9密码算法的使用说明。

SM9 密码算法使用规范

1 范围

本文件定义了 SM9 密码算法的使用方法，以及密钥、加密与签名等的数据格式。

本文件适用于 SM9 密码算法的使用，以及支持 SM9 密码算法的设备和系统的研发和检测。

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 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 32918（所有部分） 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 38635.1—2020 信息安全技术 SM9 标识密码算法 第 1 部分：总则

GB/T 38635.2—2020 信息安全技术 SM9 标识密码算法 第 2 部分：算法

3 术语和定义

下列术语和定义适用于本文件。

3.1

算法标识 algorithm identifier

用于标明算法机制的数字化信息。

3.2

SM9 密码算法 SM9 algorithm

一种采用双线性对的椭圆曲线公钥密码算法。

3.3

签名主密钥 signature master key

密钥管理基础设施的根签名密钥对，包括签名主私钥和签名主公钥，用于进行数字签名、验签和为用户生成用户签名密钥。

3.4

加密主密钥 encryption master key

密钥管理基础设施的根加密密钥对，包括加密主私钥和加密主公钥，用于进行数字加密、解密和为用户生成用户加密密钥。

3.5

用户签名密钥 signature key

其中私钥由密钥管理基础设施产生并下发给用户。该类密钥包括用户签名私钥和签名公钥，用于数字签名和验签。