ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 41389—2022

信息安全技术
SM9 密码算法使用规范

Information security technology—
SM9 cryptographic algorithm application specification

2022-04-15 发布　　2022-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：北京国脉信安科技有限公司、上海信息安全工程技术研究中心、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、国网区块链科技(北京)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、王栋。

信息安全技术
SM9 密码算法使用规范

1 范围

本文件规定了 SM9 密码算法的使用要求，描述了密钥、加密与签名的数据格式。

本文件适用于 SM9 密码算法的正确和规范使用，以及指导 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 16262.1—2006 信息技术 抽象语法记法一(ASN.1) 第 1 部分：基本记法规范

GB/T 17964 信息安全技术 分组密码算法的工作模式

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 35276—2017 信息安全技术 SM2 密码算法使用规范

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

SM9 算法 SM9 algorithm

一种基于身份标识的椭圆曲线公钥密码算法。

3.2

签名主密钥 signature master key

密钥管理基础设施的根签名密钥对。

注：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。

3.3

加密主密钥 encryption master key

密钥管理基础设施的根加密密钥对。

注：包括加密主私钥和加密主公钥，用于进行数据加密、解密和为用户生成用户加密密钥。

3.4

用户签名密钥 user signature key

用户的签名密钥对。