ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0081—2020

SM9 密码算法加密签名消息语法规范

SM9 cryptographic algorithm encryption and signature message syntax 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、西安工业大学、深圳奥联信息安全技术有限公司、中国科学院自动化研究所苏州研究院。

本文件主要起草人：袁峰、王晓春、容晓峰、杜志强、蔡先勇、药乐、张立圆、封维端、蒋楠、汪雪林。

SM9 密码算法加密签名消息语法规范

1 范围

本文件定义了使用 SM9 密码算法的加密签名消息语法。

本文件适用于使用 SM9 算法进行加密和签名操作时对操作结果的标准化封装。

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 33560 信息安全技术 密码应用标识规范

GB/T 38635(所有部分) 信息安全技术 SM9 标识密码算法

GM/T 0080 SM9 密码算法使用规范

GM/Z 4001—2013 密码术语

3 术语和定义

GB/T 38635(所有部分)和 GM/Z 4001—2013 界定的以及下列术语适用于本文件。

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

一种国家商用双线性对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。

3.6

用户加密密钥 encryption key

其中私钥由密钥管理基础设施产生并下发给用户。该类密钥包括用户加密私钥和加密公钥，用于