ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 35275—2026
代替 GB/T 35275—2017

网络安全技术　SM2 密码算法加密签名消息格式

Cybersecurity technology—SM2 cryptographic algorithm encryption and signature message format

2026-04-30 发布　　2026-11-01 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。

本文件代替GB/T 35275—2017《信息安全技术　SM2密码算法加密签名消息语法规范》，与GB/T 35275—2017相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了缩略语“CA”和“ECC”（见2017年版的第4章）；

b) 增加了摘要数据类型OID，鉴别数字信封数据类型OID（见第5章）；

c) 删除了ExtendedCertificateOrCertificate和ExtendedCertificatesAndCertificates基本类型定义（见2017年版的第6章）；

d) 更改了Version版本号取值为2（见6.8，表3，表4和表8，2017年版的6.8，表3，表4和表8）；

e) 增加了Attribute基本类型定义（见6.9）；

f) 增加了签名的计算过程（见第8章）；

g) 增加了摘要数据类型digestedData（见第10章）；

h) 增加了鉴别数字信封数据类型authEnvelopedData（见第12章）。

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。

本文件由全国网络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：格尔软件股份有限公司、北京国脉信安科技有限公司、广东省电子商务认证有限公司、智巡密码（上海）检测技术有限公司、北京信安世纪科技股份有限公司、北京数字认证股份有限公司、上海市数字证书认证中心有限公司、中电信量子信息科技集团有限公司、北京海泰方圆科技股份有限公司、长春吉大正元信息技术股份有限公司、中国电子技术标准化研究院、江苏意源科技有限公司、山东得安信息技术有限公司、山东大学、安徽问天量子科技股份有限公司、数盾信息科技股份有限公司、江苏翔晟信息技术股份有限公司、中安云科科技发展（山东）有限公司、天翼云科技有限公司、天翼安全科技有限公司、深圳市纽创信安科技开发有限公司、杭州弗兰科信息安全科技有限公司、华为技术有限公司、商用密码检测认证中心、北京中科卓信软件测评技术中心、成都安美勤信息技术股份有限公司、积至（海南）信息技术有限公司、北京天融信网络安全技术有限公司、中国信息通信研究院、亚数信息科技（上海）有限公司、国家工业信息安全发展研究中心、中国电子科技集团公司第十五研究所、麒麟软件有限公司、北京信长城科技发展有限公司、北京智芯微电子科技有限公司、中国电子信息产业集团有限公司第六研究所、杭州中焯信息技术股份有限公司、深圳海规网络科技有限公司、九源云（广州）智能科技有限公司、广州众诺微电子有限公司。

本文件主要起草人：郑强、刘平、封维端、陈树乐、罗俊、韩玮、焦靖伟、赵敏、王银平、王玉林、罗影、赵丽丽、黄晶晶、姜建功、马洪富、刘勇、孔凡玉、刘婧婧、黄晨、徐晓明、杨子晋、郑海森、辛晨、康和、王宗岳、谭波涛、魏玉科、刘中、毛颖颖、李远金、李劲雄、王媛娣、雷晓锋、安高峰、王娟娟、张国庆、孙晓峰、赵礼鹏、翟新元、刘晶、王伊婷、李艳俊、张大朋、岳佳圆、罗燕京、涂因子、王龙、李烁权、何忠靖、程刚、王波。

本文件及其所代替文件的历次版本发布情况为：

——2017年首次发布版为GB/T 35275—2017；

——本次为第一次修订。

网络安全技术　SM2 密码算法加密签名消息格式

1　范围

本文件规定了 SM2 密码算法在加密签名中的消息格式。

本文件适用于使用 SM2 密码算法进行加密签名操作时对操作结果的封装。

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 20518—2018　信息安全技术　公钥基础设施　数字证书格式

GB/T 25069　信息安全技术　术语

GB/T 32905　信息安全技术　SM3 密码杂凑算法

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 33560　网络安全技术　密码应用标识

GB/T 35276　信息安全技术　SM2 密码算法使用规范

GB/T 36624—2018　信息技术　安全技术　可鉴别的加密机制

GM/Z 4001　密码术语

3　术语和定义

GB/T 25069 和 GM/Z 4001 界定的术语和定义适用于本文件。

4　缩略语

下列缩略语适用于本文件。

OID：对象标识符(Object Identity)

5　概述

使用 ContentInfo 类型表示内容交换通用语法结构，其定义如下：

```
ContentInfo ::= SEQUENCE {
  contentType          ContentType,
  content              [0] EXPLICIT ANY DEFINED BY contentType OPTIONAL
}
ContentType ::= OBJECT IDENTIFIER
```