

ICS 35.040  
L 80  
备案号：38308—2013



# 中华人民共和国密码行业标准

GM/T 0010—2012

---

## SM2 密码算法加密签名消息语法规范

SM2 cryptography message syntax specification

2012-11-22 发布

2012-11-22 实施

---

国家密码管理局 发布

## 目 次

前言 .....	I
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 符号和缩略语 .....	1
5 OID 定义 .....	1
6 基本类型定义 .....	2
6.1 CertificateRevocationLists .....	2
6.2 ContentEncryptionAlgorithmIdentifier .....	2
6.3 DigestAlgorithmIdentifier .....	2
6.4 DigestEncryptionAlgorithmIdentifier .....	2
6.5 ExtendedCertificateOrCertificate .....	2
6.6 ExtendedCertificatesAndCertificates .....	3
6.7 IssuerAndSerialNumber .....	3
6.8 KeyEncryptionAlgorithmIdentifier .....	3
6.9 Version .....	3
6.10 ContentInfo .....	3
7 数据类型 data .....	3
8 签名数据类型 signedData .....	4
8.1 signedData 类型 .....	4
8.2 SignerInfo 类型 .....	4
9 数字信封数据类型 envelopedData .....	5
9.1 envelopedData 类型 .....	5
9.2 RecipientInfo 类型 .....	6
10 签名及数字信封数据类型 signedAndEnvelopedData .....	7
11 加密数据类型 encryptedData .....	7
12 密钥协商类型 keyAgreementInfo .....	8
附录 A (规范性附录) SM2 密钥格式 .....	9
A.1 椭圆曲线参数语法 .....	9
A.2 公钥语法 .....	9
A.3 私钥语法 .....	9
参考文献 .....	10

## 前 言

本标准按照 GB/T 1.1—2009 的规则编写。

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这些专利的责任。

本标准由国家密码管理局提出并归口。

本标准中的附录 A 为规范性附录。

本标准起草单位：上海格尔软件股份有限公司、北京海泰方圆科技有限公司、北京数字认证股份有限公司、无锡江南信息安全工程技术中心、成都卫士通信息产业股份有限公司、上海市数字证书认证中心有限公司、兴唐通信科技有限公司、上海颐东网络信息有限公司、山东得安信息技术有限公司、国家信息安全工程技术研究中心。

本标准起草人：刘平、谭武征、柳增寿、李述胜、徐强、李元正、刘承、王妮娜、夏东山、蒋红宇、孔凡玉、袁峰。

本标准涉及的密码算法按照国家密码管理部门的要求使用。

# SM2 密码算法加密签名消息语法规范

## 1 范围

本标准定义了使用 SM2 密码算法的加密签名消息语法。

本标准适用于使用 SM2 密码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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件,凡是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。

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

PKCS #6 Extended-Certificate Syntax

## 3 术语和定义

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

**SM2 算法 SM2 algorithm**

一种椭圆曲线密码算法,密钥长度为 256 比特。

## 4 符号和缩略语

下列缩略语适用于本标准:

ECC 椭圆曲线密码算法(Elliptic Curve Cryptography)

ID 用户标识(Identity)

OID 对象标识符(Object Identity)

## 5 OID 定义

本标准对 6 个对象 data, signedData, envelopedData, signedAndEnvelopedData, encryptedData 和 keyAgreementInfo 的标识符进行了定义,详见表 1。