ICS 35.040
L 80

中华人民共和国国家标准

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

Information security technology—SM2 cryptographic algorithm encrypted signature message syntax specification

2017-12-29 发布　　2018-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:上海格尔软件股份有限公司、上海市数字证书认证中心有限公司、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、北京海泰方圆科技有限公司、兴唐通信科技有限公司、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。

本标准主要起草人:刘平、郑强、杨文山、韩玮、傅大鹏、李元正、蒋红宇、徐明翼、王妮娜、孔凡玉、袁锋。

信息安全技术　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。

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 35276　信息安全技术　SM2 密码算法使用规范

GB/T 33560　信息安全技术　密码应用标识规范

PKCS ＃6　扩展证书语法(Extended-certificate syntax)

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

SM2 密码算法　SM2 cryptographic algorithm

由 GB/T 32918 定义的一种算法。

3.3

SM3 密码算法　SM3 cryptographic algorithm

由 GB/T 32905 定义的一种算法。

4　缩略语

下列缩略语适用于本文件。

CA：证书认证机构(Certification Authority)

ECC：椭圆曲线密码(Elliptic Curve Cryptography)

OID：对象标识(Object Identity)

5　OID 定义

本标准对 6 个对象 data、signedData、envelopedData、signedAndEnvelopedData、encryptedData 和