



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 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 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) 6

11 加密数据类型(encryptedData) 7

12 密钥协商类型(keyAgreementInfo) 7

13 SM2 密钥格式 9

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

keyAgreementInfo 的标识符进行了定义, 详见表 1。

表 1 对象标识符

对象标识符 OID	对象标识符定义
1.2.156.10197.6.1.4.2	SM2 密码算法加密签名消息语法规范
1.2.156.10197.6.1.4.2.1	数据类型
1.2.156.10197.6.1.4.2.2	签名数据类型
1.2.156.10197.6.1.4.2.3	数字信封数据类型
1.2.156.10197.6.1.4.2.4	签名及数字信封数据类型
1.2.156.10197.6.1.4.2.5	加密数据类型
1.2.156.10197.6.1.4.2.6	密钥协商类型

6 基本类型定义

6.1 CertificateRevocationLists

CertificateRevocationLists 类型标明一个证书撤销列表的集合。
CertificateRevocationLists ::= SET OF CertificateRevocationList

6.2 ContentEncryptionAlgorithmIdentifier

ContentEncryptionAlgorithmIdentifier 类型标明一个数据加密算法。其 OID 见 GB/T 33560。
ContentEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.3 DigestAlgorithmIdentifier

DigestAlgorithmIdentifier 类型标明一个消息摘要算法, 本标准为 SM3 算法, 其 OID 见 GB/T 33560。
DigestAlgorithmIdentifier ::= AlgorithmIdentifier

6.4 DigestEncryptionAlgorithmIdentifier

DigestEncryptionAlgorithmIdentifier 类型标明一个签名算法, 本标准为 SM2 密码算法, 其 OID 见 GB/T 33560。
DigestEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.5 ExtendedCertificateOrCertificate

ExtendedCertificateOrCertificate 类型指定一个 PKCS # 6 扩展证书或者一个 X.509 证书。这一类型见 PKCS # 6 第 6 节推荐的语法:
ExtendedCertificateOrCertificate ::= CHOICE {
 certificate Certificate, -- X.509
 extendedCertificate [0] IMPLICIT ExtendedCertificate
}

6.6 ExtendedCertificatesAndCertificates

ExtendedCertificatesAndCertificates 类型指定一个扩展证书和 X.509 证书的集合。它表示集合足以包含从可识别的“根”或“顶级 CA”到所有签名者的证书链。

ExtendedCertificatesAndCertificates ::= SET OF
ExtendedCertificateOrCertificate

6.7 IssuerAndSerialNumber

IssuerAndSerialNumber 类型标明一个证书颁发者可识别名和颁发者确定的证书序列号,可据此确定一份证书和与此证书对应的实体及公钥。

IssuerAndSerialNumber ::= SEQUENCE {
 issuer Name,
 serialNumber CertificateSerialNumber
}

6.8 KeyEncryptionAlgorithmIdentifier

KeyEncryptionAlgorithmIdentifier 类型标明加密对称密钥的加密算法。

KeyEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

6.9 Version

Version 类型标明语法版本号。

Version ::= INTEGER(1)

6.10 ContentInfo

ContentInfo 类型标明内容交换通用语法结构,内容交换的通用语法结构定义如下:

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

ContentType ::= OBJECT IDENTIFIER

其中:

ContentType 内容类型是一个对象标识符,其定义见第 5 章。

content 内容,可选。

7 数据类型(Data)

数据类型 Data 结构定义如下:

Data ::= OCTET STRING

数据类型 Data 表示任意的字节串。

8 签名数据类型(signedData)

8.1 signedData 类型

signedData 数据类型由任意类型的数据和至少一个签名者的签名值组成。任意类型的数据能够同时被任意数量的签名者签名。

signedData 数据类型结构定义如下：

SignedData ::= SEQUENCE {
 version Version,
 digestAlgorithms DigestAlgorithmIdentifiers,
 contentInfo ContentInfo,
 certificates[0] IMPLICIT ExtendedCertificatesAndCertificates OPTIONAL,
 crls[1] IMPLICIT CertificateRevocationLists OPTIONAL,
 signerInfos SignerInfos
}

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

SignerInfos ::= SET OF SignerInfo

结构中各项含义见表 2。

表 2 signedData 数据类型

字段名称	数据类型	含义
version	Version	版本号,此处取值为 1
digestAlgorithms	DigestAlgorithmIdentifiers	消息摘要算法标识符的集合
contentInfo	ContentInfo	数据内容
certificates	ExtendedCertificatesandCertificates	PKCS#6 扩展证书和 X.509 证书的集合
crls	CertificateRevocationLists	证书撤销列表的集合
signInfos	SignerInfos	每个签名者信息的集合

8.2 signerInfo 类型

signerInfo 类型结构定义如下：

SignerInfo ::= SEQUENCE {
 version Version,
 issuerAndSerialNumber IssuerAndSerialNumber,
 digestAlgorithm DigestAlgorithmIdentifier,
 authenticatedAttributes[0] IMPLICIT Attributes OPTIONAL,
 digestEncryptionAlgorithm DigestEncryptionAlgorithmIdentifier,
 encryptedDigest EncryptedDigest,
 unauthenticatedAttributes [1] IMPLICIT Attributes OPTIONAL
}

EncryptedDigest ::= OCTET STRING

结构中各项含义见表 3。

表 3 SignerInfo 数据类型

字段名称	数据类型	含义
version	Version	版本号,此处取值为 1
issuerAndSerial- Number	IssuerAndSerialNumber	一个证书颁发者可识别名和颁发者确定的证书序列号,可据此确定一份证书和与此证书对应的实体及公钥
digestAlgorithm	DigestAlgorithmIdentifier	对内容进行摘要计算的消息摘要算法,本标准采用 SM3 算法
authenticatedAt- tributes	Attributes	是经由签名者签名的属性的集合,该域可选。如果该域存在,该域中摘要的计算方法是对原文进行摘要计算结果
digestEncryptionAl- gorithm	DigestEncryptionAlgorithmIdentifier	SM2 椭圆曲线数字签名算法标识符
encryptedDigest	OCTET STRING	值是 SM2Signature,用签名者私钥进行签名的结果,其定义见 GB/T 35276

9 数字信封数据类型(envelopedData)

9.1 envelopedData 类型

数字信封 envelopedData 数据类型由加密数据和至少一个接收者的数据加密密钥的密文组成。其中,加密数据是用数据加密密钥加密的,数据加密密钥是用接收者的公钥加密的。

该类型用于为接收者的 data、digestedData 或 signedData 三种类型的数据做数字信封。

envelopedData 数据类型结构定义如下:

```

EnvelopedData ::= SEQUENCE {
    version Version,
    recipientInfos RecipientInfos,
    encryptedContentInfo EncryptedContentInfo
}

```

RecipientInfos ::= SET OF RecipientInfo

结构中各项含义见表 4。

表 4 EnvelopedData 数据类型

字段名称	数据类型	含义
version	Version	版本号,此处取值为 1
recipientInfos	RecipientInfos	每个接收者信息的集合,至少要有一个接收者
encryptedContentInfo	EncryptedContentInfo	加了密的内容信息

```

EncryptedContentInfo ::= SEQUENCE {
    contentType ContentType,
    contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier,
    encryptedContent[0] IMPLICIT EncryptedContent OPTIONAL,
    sharedInfo[1] IMPLICIT OCTET STRING OPTIONAL,
}

```



```

sharedInfo2 [2] IMPLICIT OCTET STRING OPTIONAL
}

```

EncryptedContent ::= OCTET STRING

结构中各项含义见表 5。

表 5 EncryptedContentInfo 数据类型

字段名称	数据类型	含义
contentType	ContentType	内容的类型
contentEncryptionAlgorithm	ContentEncryptionAlgorithmIdentifier	内容加密算法(和相应的参数)
encryptedContent	EncryptedContent	内容加密的结果,可选
sharedInfo1	OCTET STRING	协商好的共享信息,可选
sharedInfo2	OCTET STRING	协商好的共享信息,可选

9.2 recipientInfo 类型

每个接收者信息用 recipientInfo 类型表示,

recipientInfo 类型结构定义如下:

```

RecipientInfo ::= SEQUENCE{
    version Version,
    issuerAndSerialNumber IssuerAndSerialNumber,
    keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
    encryptedKey OCTET STRING
}

```

结构中各项含义见表 6。

表 6 RecipientInfo 数据类型

字段名称	数据类型	含义
version	Version	版本号,此处取值为 1
issuerAndSerial- Number	IssuerAndSerialNumber	颁发者可辨别名和颁发序列号
keyEncryptionAlgo- rithm	KeyEncryptionAlgorithmIdenti- fier	用接收者公钥加密数据加密密钥的算法,为 SM2 椭圆曲线加密算法
encryptedKey	OCTET STRING	数据加密密钥密文 SM2cipher,其定义见 GB/T 35276

10 签名及数字信封数据类型(signedAndEnvelopedData)

signedAndEnvelopedData 数据类型由任意类型的加密数据、至少一个接收者的数据加密密钥和至少一个签名者的签名组成。

signedAndEnvelopedData 数据类型结构定义如下:

```

SignedAndEnvelopedData ::= SEQUENCE {
    version Version,

```

```
recipientInfos RecipientInfos,  
digestAlgorithms DigestAlgorithmIdentifiers,  
encryptedContentInfo EncryptedContentInfo,  
certificates[0] IMPLICIT ExtendedCertificatesAndCertificates OPTIONAL,  
crls[1] IMPLICIT CertificateRevocationLists OPTIONAL,  
signerInfos SignerInfos  
}
```

结构中各项含义见表 7。

表 7 signedAndEnvelopedData 数据类型

字段名称	数据类型	含义
version	Version	版本号,此处取值为 1
recipientInfos	RecipientInfos	每个接受者信息的集合,至少一个元素
digestAlgorithms	DigestAlgorithmIdentifiers	消息摘要算法标识符的集合
encryptedContentInfo	EncryptedContentInfo	加了密的内容,可以是任何定义的数据类型
certificates	ExtendedCertificatesAndCertificates	PKCS#6 扩展证书和 X.509 证书的集合,是可选的
crls	CertificateRevocationLists	证书撤销列表的集合
signerInfos	SignerInfos	每个签名者的集合,至少要有一个元素

11 加密数据类型(encryptedData)

encryptedData 数据类型由任意类型的加了密的数据组成,数据类型既没有接收者也没有加密的数据加密密钥。

encryptedData 数据类型定义如下:

```
EncryptedData ::= SEQUENCE {  
    version Version,  
    encryptedContentInfo EncryptedContentInfo  
}
```

结构中各项含义见表 8。

表 8 encryptedData 数据类型

字段名称	数据类型	含义
version	Version	版本号,此处取值为 1
encryptedContentInfo	EncryptedContentInfo	已加密的内容信息

12 密钥协商类型(keyAgreementInfo)

密钥协商 keyAgreementInfo 数据类型标明两个用户之间建立一个共享秘密密钥的结构,通过这种方式能够确定一个共享秘密密钥的值。

该类型用于两个用户为产生共享秘密密钥进行的公共参数交换。

KeyAgreementInfo ::= SEQUENCE {
Version Version,
tempPublicKeyR SM2PublicKey,
userCertificate Certificate,
userID OCTET STRING
}

结构中各项含义见表 9。

表 9 keyAgreementInfo 数据类型

字段名称	数据类型	含义
version	Version	版本号,此处取值为 1
tempPublicKeyR	SM2PublicKey	临时公钥,结构定义见 GB/T 33560
userCertificate	Certificate	用户证书
userID	OCTET STRING	用户标识

13 SM2 密钥格式

13.1 椭圆曲线参数语法

椭圆曲线参数的表达采用与 ANSI X9.62 相同的 ASN.1 定义,其定义如下:

Parameters ::= CHOICE {
ecParameters ECPParameters,
namedCurve ObjectIdentifier,
implicitlyCA NULL }

在用于 SM2 密码算法表达时,只使用 namedCurve 这一种表达方法,SM2 密码算法曲线定义的 OID。见 GB/T 33560。

13.2 公钥语法

椭圆曲线公钥的表达采用与 X9.62 相同的 ASN.1 定义,其定义如下:

SubjectPublicKeyInfo ::= SEQUENCE {
algorithm AlgorithmIdentifier {{ECPKAlgorithms}},
subjectPublicKey SM2PublicKey
}

其中:

algorithm 定义了公钥的类型

subjectPublicKey 定义了公钥的实际值

AlgorithmIdentifier 是对象标识与参数的绑定,其定义如下:

AlgorithmIdentifier ::= SEQUENCE {
algorithm OBJECT IDENTIFIER,
parameters ANY DEFINED BY algorithm OPTIONAL

}

对于 SM2 密码算法,其 OID(algorithm)定义见 GB/T 33560。

13.3 私钥语法

椭圆曲线私钥的表达采用与 X9.62 相同的 ASN.1 定义,其定义如下:

```
ECPrivateKey{CURVES:IOSet} ::= SEQUENCE {
    version INTEGER { ecPrivkeyVer1(1) } (ecPrivkeyVer1),
    privateKey SM2PrivateKey,
    parameters [0] Parameters{{IOSet}} OPTIONAL,
    publicKey [1] SM2PublicKey
}
```

其中:

version 指定了私钥的版本号,这里使用整数 1 来表示 SM2 私钥的版本号。

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 SM2 密码算法
加密签名消息语法规范
GB/T 35275—2017

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址 www.spc.net.cn

总编室:(010)68533533 发行中心:(010)51780238

读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 1 字数 22 千字
2017 年 12 月第一版 2017 年 12 月第一次印刷

*

书号: 155066 · 1-58336 定价 18.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107



GB/T 35275-2017