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 SM2Signature,
    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(1)	Version	语法的版本号
digestAlgorithms	DigestAlgorithmIdentifiers	消息摘要算法标识符的集合
contentInfo	SM2Signature	被签名的数据内容，数据类型见 GM/T 0009
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(1)	Version	语法的版本号
issuerAndSerialNumber	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,本规范采用SM3算法
authenticatedAttributes	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
digestEncryptionAlgorithm	DigestEncryptionAlgorithmIdentifier	SM2-1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GM/T 0009。编码格式为r‖s。

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(1)	Version	语法的版本号
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

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(1)	Version	语法的版本号
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。