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
```