

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。