② RSA 解密：使用公钥 pk 对密文 ED 进行解密获得摘要数据 D（OCTET STRING 类型）。

③ 数据解码：摘要数据 D 是 DigestInfo 类型，解码后获得摘要值 MD 和摘要算法 ID。

④ 计算摘要并比较：根据摘要算法 ID，计算 M 的摘要值 MD'= HASH（M）。如果 MD'等于 MD，则验证成功，否则验证失败。

8.2 SM2

《SM2 密码算法使用规范》规定了数字证书 SM2 算法的公/私钥及加密签名格式。

1. SM2 公钥格式

SM2 公钥格式用 ASN.1 描述如下：

```
SM2PublicKey ::= BIT STRING
```

SM2 公钥是 SM2 曲线上的一个点，由横坐标和纵坐标两个分量来表示，记为（x，y），简记为 Q，每个分量长度为 256 位。SM2PublicKey 内容格式为：04 || X || Y。其中，X 和 Y 分别表示公钥的 x 分量和 y 分量，其长度各为 256 位。

2. SM2 私钥格式

SM2 私钥格式用 ASN.1 描述如下：

```
SM2PrivateKey ::= INTEGER
```

SM2 私钥是一个大于或等于 1 且小于 n-1 的整数（n 为 SM2 算法的阶），简记为 k，长度为 256 位。

3. SM2 加密数据格式

SM2 加密数据格式用 ASN.1 描述如下：

```
SM2Cipher :: = SEQUENCE {
    XCoordinate     INTEGER,   -- x 分量
    YCoordinate     INTEGER,   -- y 分量
    HASH            OCTET STRING SIZE（32），    --摘要值
    CipherText      OCTET STRING                  --密文
}
```

假设使用 SM2 公钥 Q（SM2PublicKey 类型）对明文 m（字符串类型）进行加密计算。则 XCoordinate 和 YCoordinate 为随机产生的公钥的 x 分量和 y 分量。HASH 为使用 SM3 算法对明文数据运算得到的摘要值，其长度为 256 位，HASH=SM3（x || m || y），其中 x 和 y 为 Q 的 x 分量和 y 分量。CipherText 是与明文等长的密文。

假设使用 SM2 私钥 d（SM2PrivateKey 类型）对密文 c（SM2Cipher 类型）进行解密计算，则解密后将获得明文 m，其长度等于密文（c→CipherText）的长度。

4. SM2 签名数据格式

SM2 签名数据格式用 ASN.1 描述如下：

```
SM2Signature :: = SEQUENCE {
    R    INTEGER,  -- 签名值的第一部分
    S    INTEGER,  -- 签名值的第二部分
}
```

其中，R 和 S 的长度各为 256 位。

假设使用签名方私钥 d（SM2PrivateKey 类型）对待签名数据 M（字符串类型）进行签名计算。具体计算步骤如下：

① 预处理 1：使用签名方的用户身份标识 ID（字符串类型）和签名方公钥 Q（SM2PublicKey 类型），通过运算得到 Z 值（字符串类型）。

$$Z = SM3（ENTL \| ID \| a \| b \| x_G \| y_G \| x_A \| y_A）$$

其中，ENTL 为 2 字节表示的 ID 的比特长度。ID 为用户身份标识，无特殊约定情况下，长度为 16 字节，默认值从左至右依次为：0x31，0x32，0x33，0x34，0x35，0x36，0x37，0x38，0x31，0x32，0x33，0x34，0x35，0x36，0x37，0x38。a 和 b 为系统曲线参数。x_G 和 y_G 为基点，x_A 和 y_A 为签名方公钥。

② 预处理 2：使用预处理 1 结果 Z 值（字符串类型）和待签名数据 M（字符串类型），通过 SM3 运算得到摘要值 H（字符串类型）。

$$H = SM3（Z \| M）$$

③ 签名：使用预处理 2 结果 H（字符串类型）和签名方私钥 d（SM2PrivateKey 类型），通过签名计算得到签名结果 sign（SM2Signature 类型）。

签名验证时，使用预处理 2 结果 H（字符串类型）、签名结果 sign（SM2Signature 类型）和签名方公钥 Q（SM2PublicKey 类型），通过验签计算确定签名结果是否通过验证。

5. SM2 密钥对保护数据格式

在 SM2 密钥对传递时，需要对 SM2 密钥对进行加密保护。

SM2 密钥对的保护数据格式用 ASN.1 描述如下：

```
SM2EnvelopedKey :: = SEQUENCE {
    symAlgID              AlgorithmIdentifier,    --对称密钥算法标识
    symEncryptedKey       SM2Cipher               --对称密钥密文
    Sm2PublicKey          SM2PublicKey,           --SM2 公钥
    Sm2EncryptedPrivateKey    BIT STRING          --SM2 私钥密文
}
```

其中，具体的保护方法为：

① 产生一个对称密钥。

② 按对称密钥算法标识指定的算法对 SM2 私钥进行加密，得到私钥密文。若对称算法为分组算法，则其运算模式为 ECB。

③ 使用外部 SM2 公钥加密对称密钥得到对称密钥密文。

④ 将私钥密文、对称密钥密文封装到密钥对保护数据中。

第 9 章　数字证书格式

9.1　基本格式

IETF RFC 3280 规定了 X.509 数字证书的基本格式。

9.1.1　证书域组成（Certificate）

X.509 数字证书由 3 个域组成，具体见表 9-1。

表 9-1　X.509 证书域组成

分　类	标　识	说　明
证书内容（待签名）	tbsCertificate	包含持有者公钥、持有者信息、签发者信息等
签名算法	signatureAlgorithm	包括摘要算法和公钥算法，如 sha1WithRSAEncryption，由算法标识和算法参数组成
签名值	signatureValue	使用签名算法，对证书内容 tbsCertificate 进行签名后的结果

X.509 证书域格式用 ASN.1 描述如下：

```
Certificate ::=  SEQUENCE  {
    tbsCertificate          TBSCertificate,
    signatureAlgorithm      AlgorithmIdentifier,
    signatureValue          BIT STRING  }
AlgorithmIdentifier  ::=  SEQUENCE  {
    Algorithm               OBJECT IDENTIFIER,
    Parameters              ANY DEFINED BY algorithm OPTIONAL  }
```

9.1.2　证书内容（tbsCertificate）

X.509 数字证书内容见表 9-2。

表 9-2　X.509 证书内容

分　类	标　识	说　明
版本号	version	用于区分证书格式版本，最新版本为 v3，缺省值为 v1
序列号	serialNumber	证书唯一标识，由签发者统一分配
签名算法	signature	必须与证书域中的签名算法相同
证书签发者	issuer	用于区分证书签发者，包含证书签发者身份信息
证书有效期	validity	由生效日期和失效日期组成
证书持有者	subject	用于区分证书持有者，包含证书持有者身份信息

（续表）

分　类	标　识	说　明
证书持有者公钥	subjectPublicKeyInfo	包含证书持有者公钥信息
证书签发者 ID	issuerUniqueID	表示证书签发者唯一标识
证书持有者 ID	subjectUniqueID	表示证书持有者唯一标识
扩展项	extensions	包含其他可扩展信息

X.509 证书内容格式用 ASN.1 描述如下：

```
TBSCertificate  ::=  SEQUENCE  {
version              [0]  EXPLICIT Version DEFAULT v1,
serialNumber              CertificateSerialNumber,
signature                 AlgorithmIdentifier,
issuer                    Name,
validity                  Validity,
subject                   Name,
subjectPublicKeyInfo SubjectPublicKeyInfo,
issuerUniqueID   [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                                  -- If present, version MUST be v2 or v3
subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                                  -- If present, version MUST be v2 or v3
extensions       [3]  EXPLICIT Extensions OPTIONAL
                                  -- If present, version MUST be v3
}
```

1. 版本号 version

version 用于区分证书格式版本，最新版本为 v3，缺省值为 v1。当使用扩展项时，version=v3。当使用 issuerUniqueID 或 subjectUniqueID 时，version=v2 或 v3。如果只使用基本内容，则 version=v1 或 v2 或 v3。

version 格式用 ASN.1 描述如下：

```
version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }
```

2. 序列号 serialNumber

serialNumber 是证书的唯一标识，由证书签发者统一分配。serialNumber 必须是正整数，同一个证书签发者（CA）所签发的每个证书的序列号必须不同，通过签发者和序列号可以区分每个证书。

serialNumber 格式用 ASN.1 描述如下：

```
CertificateSerialNumber  ::=  INTEGER
```

3. 签名算法 signature

signature 必须与证书域中的签名算法相同，即：signature=Certificate→signatureAlgorithm。

signature 格式用 ASN.1 描述如下：

```
AlgorithmIdentifier  ::=  SEQUENCE  {
```

```
    Algorithm           OBJECT IDENTIFIER,
    Parameters          ANY DEFINED BY algorithm OPTIONAL   }
```

4. 证书签发者 issuer

issuer 用于区分证书签发者，必须包含一个非空的 X.500 DN 项。DN 是 Distinguished Name 的缩写，表示可识别的名称，且 DN 项被定义为 X.501 规范中的 Name 类型。

issuer 格式用 ASN.1 描述如下：

```
Name ::= CHOICE {     RDNSequence     }
RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
RelativeDistinguishedName ::=    SET OF AttributeTypeAndValue
AttributeTypeAndValue ::= SEQUENCE {
    type        AttributeType,
    value       AttributeValue }
AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY AttributeType
```

Name 类型采用分层结构，由多个属性 AttributeTypeAndValue 组成；每个属性由属性类型 AttributeType 和属性值 AttributeValue 组成；AttributeValue 的具体类型由 AttributeType 决定，通常采用 DirectoryString 类型。DirectoryString 用 ASN.1 描述如下：

```
DirectoryString ::= CHOICE {
    teletexString           TeletexString (SIZE (1..MAX)),
    printableString         PrintableString (SIZE (1..MAX)),
    universalString         UniversalString (SIZE (1..MAX)),
    utf8String              UTF8String (SIZE (1..MAX)),
    bmpString               BMPString (SIZE (1..MAX)) }
```

issuer 中的属性值应优先采用 UTF8String 编码。X.500 系列规范中定义了属性的标准集合，X.509 数字证书只使用其中的一部分属性。issuer 和 subject 包含的主要属性类型如表 9-3 所示。

表 9-3　issuer 和 subject 包含的主要属性类型

分　类	OID	说　明
country	id-at 6	国家，C
organization	id-at 10	单位，O
organization unit	id-at 11	部门，OU
distinguished name qualifier	id-at 46	DN 限定符
state or province name	id-at 8	省份或州，ST
common name	id-at 3	通用名称，CN
serial number	id-at 5	序列号，SN
locality	id-at 7	城市，L
domain component	0.9.2342.19200300. 100.1.25	域名组件，等同于 DNS，DC
title	id-at 12	头衔