```
        version Version,
        digestAlgorithm DigestAlgorithmIdentifier,
        contentInfo ContentInfo,
        digest Digest }
    Digest ::= OCTET STRING
```

⑦ 密文消息内容用 ASN.1 描述如下：

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

6. PKCS #8：Private-Key Information Syntax Standard（私钥信息语法标准）

PKCS #8 v1.2 描述私钥信息的语法格式。私钥信息包括私钥和一组属性。该标准还描述了私钥密文的语法，且允许使用基于口令的加密算法来加密私钥。在 RFC 5208 中又重新定义。

① 私钥信息格式用 ASN.1 描述如下：

```
PrivateKeyInfo ::= SEQUENCE {
    version Version,
    privateKeyAlgorithm PrivateKeyAlgorithmIdentifier,
    privateKey PrivateKey,
    attributes [0] IMPLICIT Attributes OPTIONAL }
Version ::= INTEGER
PrivateKeyAlgorithmIdentifier ::= AlgorithmIdentifier
PrivateKey ::= OCTET STRING
Attributes ::= SET OF Attribute
```

② 私钥密文格式用 ASN.1 描述如下：

```
EncryptedPrivateKeyInfo ::= SEQUENCE {
    encryptionAlgorithm EncryptionAlgorithmIdentifier,
    encryptedData EncryptedData }
EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier
EncryptedData ::= OCTET STRING
```

7. PKCS #9：Selected Attribute Types（可供选择的属性类型）

PKCS #9 v2.0 定义了两个新的辅助对象类和精选的属性类型（基于这两个对象类）。

① 两个辅助对象类 pkcsEntity 和 naturalPerson 定义如下：

```
pkcsEntity OBJECT-CLASS ::=    {
    SUBCLASS OF { top }
    KIND auxiliary
    MAY CONTAIN { PKCSEntityAttributeSet }
    ID pkcs-9-oc-pkcsEntity
}
PKCSEntityAttributeSet ATTRIBUTE ::= {
```

```
        pKCS7PDU |userPKCS12 |    pKCS15Token | encryptedPrivateKeyInfo,
        ···-- For future extensions
    }
    naturalPerson OBJECT-CLASS    ::=    {
        SUBCLASS OF { top }
        KIND auxilary
        MAY CONTAIN { NaturalPersonAttributeSet }
        ID pkcs-9-oc-naturalPerson
    }
    NaturalPersonAttributeSet ATTRIBUTE ::= {
        emailAddress |    unstructuredName |    unstructuredAddress |
        dateOfBirth | placeOfBirth |    gender |    countryOfCitizenship |
        countryOfResidence |    pseudonym |    serialNumber,
        ···-- For future extensions
    }
```

② 基于 pkcsEntity 对象类的属性类型定义如下：

```
    pKCS7PDU ATTRIBUTE ::= {
        WITH SYNTAX ContentInfo
        ID pkcs-9-at-pkcs7PDU
    }
    userPKCS12 ATTRIBUTE ::= {
        WITH SYNTAX PFX
        ID pkcs-9-at-userPKCS12
    }
    pKCS15Token ATTRIBUTE ::= {
        WITH SYNTAX PKCS15Token
        ID pkcs-9-at-pkcs15Token
    }
    encryptedPrivateKeyInfo ATTRIBUTE ::= {
        WITH SYNTAX EncryptedPrivateKeyInfo
        ID pkcs-9-at-encryptedPrivateKeyInfo
    }
```

③ 基于 naturalPerson 对象类的属性类型定义如下：

```
    emailAddress ATTRIBUTE ::= {
        WITH SYNTAX IA5String  (SIZE (1..pkcs-9-ub-emailAddress))
        EQUALITY MATCHING RULE pkcs9CaseIgnoreMatch
        ID pkcs-9-at-emailAdress
    }
    unstructuredName ATTRIBUTE ::= {
        WITH SYNTAX PKCS9String {pkcs-9-ub-unstructuredName}
        EQUALITY MATCHING RULE pkcs9CaseIgnoreMatch
```

```
        ID pkcs-9-at-unstructuredName
    }
    unstructuredAddress ATTRIBUTE ::= {
        WITH SYNTAX DirectoryString {pkcs-9-ub-unstructuredAddress}
        EQUALITY MATCHING RULE caseIgnoreMatch
        ID pkcs-9-at-unstructuredAddress
    }
    dateOfBirth ATTRIBUTE ::= {
        WITH SYNTAX GeneralizedTime
        EQUALITY MATCHING RULE generalizedTimeMatch
        SINGLE VALUE TRUE
        ID pkcs-9-at-dateOfBirth
    }
    placeOfBirth ATTRIBUTE ::= {
        WITH SYNTAX DirectoryString {pkcs-9-ub-placeOfBirth}
        EQUALITY MATCHING RULE caseExactMatch
        SINGLE VALUE TRUE
        ID pkcs-9-at-placeOfBirth
    }
    gender ATTRIBUTE ::= {
        WITH SYNTAX PrintableString (SIZE (1) ^ FROM ("M" | "F" | "m" | "f"))
        EQUALITY MATCHING RULE caseIgnoreMatch
        SINGLE VALUE TRUE
        ID pkcs-9-at-gender
    }
    countryOfCitizenship ATTRIBUTE ::= {
        WITH SYNTAX PrintableString (SIZE (2) ^ CONSTRAINED BY {
    -- Must be a two-letter country acronym in accordance with ISO/IEC 3166 --})
        EQUALITY MATCHING RULE caseIgnoreMatch
        ID pkcs-9-at-countryOfCitizenship
    }
    countryOfResidence ATTRIBUTE ::= {
        WITH SYNTAX PrintableString (SIZE (2) ^ CONSTRAINED BY {
    -- Must be a two-letter country acronym in accordance with ISO/IEC 3166 --})
        EQUALITY MATCHING RULE caseIgnoreMatch
        ID pkcs-9-at-countryOfResidence
    }
    pseudonym ATTRIBUTE ::= {
        WITH SYNTAX DirectoryString {pkcs-9-ub-pseudonym}
        EQUALITY MATCHING RULE caseExactMatch
        ID id-at-pseudonym
    }
```

④ 用于 PKCS #7 的属性类型定义如下：

```
contentType ATTRIBUTE ::= {
    WITH SYNTAX ContentType
    EQUALITY MATCHING RULE objectIdentifierMatch
    SINGLE VALUE TRUE
    ID pkcs-9-at-contentType
}
ContentType ::= OBJECT IDENTIFIER
messageDigest ATTRIBUTE ::= {
    WITH SYNTAX MessageDigest
    EQUALITY MATCHING RULE octetStringMatch
    SINGLE VALUE TRUE
    ID pkcs-9-at-messageDigest
}
MessageDigest ::= OCTET STRING
signingTime ATTRIBUTE ::= {
    WITH SYNTAX SigningTime
    EQUALITY MATCHING RULE signingTimeMatch
    SINGLE VALUE TRUE
    ID pkcs-9-at-signingTime
}
SigningTime ::= Time -- imported from ISO/IEC 9594-8
randomNonce ATTRIBUTE ::= {
    WITH SYNTAX RandomNonce
    EQUALITY MATCHING RULE octetStringMatch
    SINGLE VALUE TRUE
    ID pkcs-9-at-randomNonce
}
RandomNonce ::= OCTET STRING （SIZE（4..MAX）） -- At least four bytes long
sequenceNumber ATTRIBUTE ::= {
    WITH SYNTAX SequenceNumber
    EQUALITY MATCHING RULE integerMatch
    SINGLE VALUE TRUE
    ID pkcs-9-at-sequenceNumber
}
SequenceNumber ::= INTEGER （1..MAX）
counterSignature ATTRIBUTE ::= {
    WITH SYNTAX SignerInfo
    ID pkcs-9-at-counterSignature
}
```

⑤ 用于 PKCS #10 的属性类型定义如下：

```
challengePassword ATTRIBUTE ::= {
    WITH SYNTAX DirectoryString {pkcs-9-ub-challengePassword}
    EQUALITY MATCHING RULE caseExactMatch
    SINGLE VALUE TRUE
    ID pkcs-9-at-challengePassword
}
extensionRequest ATTRIBUTE ::= {
    WITH SYNTAX ExtensionRequest
    SINGLE VALUE TRUE
    ID pkcs-9-at-extensionRequest
}
ExtensionRequest ::= Extensions
extendedCertificateAttributes ATTRIBUTE ::= {
    WITH SYNTAX SET OF Attribute
    SINGLE VALUE TRUE
    ID pkcs-9-at-extendedCertificateAttributes
}
```

⑥ 用于 PKCS #12 或 PKCS #15 的属性定义如下：

```
friendlyName ATTRIBUTE ::= {
    WITH SYNTAX BMPString (SIZE(1..pkcs-9-ub-friendlyName))
    EQUALITY MATCHING RULE caseIgnoreMatch
    SINGLE VALUE TRUE
    ID pkcs-9-at-friendlyName
}
localKeyId ATTRIBUTE ::= {
    WITH SYNTAX OCTET STRING
    EQUALITY MATCHING RULE octetStringMatch
    SINGLE VALUE TRUE
    ID pkcs-9-at-localKeyId
}
```

⑦ S/MIME 规范中定义的属性如下：

```
signingDescription ATTRIBUTE ::= {
    WITH SYNTAX DirectoryString {pkcs-9-ub-signingDescription}
    EQUALITY MATCHING RULE caseIgnoreMatch
    SINGLE VALUE TRUE
    ID pkcs-9-at-signingDescription
}
smimeCapabilities ATTRIBUTE ::= {
    WITH SYNTAX SMIMECapabilities
    SINGLE VALUE
    ID pkcs-9-at-smimeCapabilities
```