```
}
SMIMECapabilities ::= SEQUENCE OF SMIMECapability
SMIMECapability ::= SEQUENCE {
    algorithm   ALGORITHM.&id  ({SMIMEv3Algorithms}),
    parameters ALGORITHM.&Type  ({SMIMEv3Algorithms}{@algorithm})
}
SMIMEv3Algorithms ALGORITHM ::= { … -- See RFC 2633 -- }
```

8. PKCS #10：Certification Request Syntax Standard（证书请求语法标准）

PKCS #10 v1.7 描述了证书请求的语法格式。证书请求包括 DN 名称、公钥和一组可选属性，以及请求方对上述信息的签名。一个证书请求包括可辨别名、公开密钥和（可选的）一组属性，所有这些均由请求证书的用户签名。证书请求被发送给 CA，由 CA 基于证书请求中的内容签发数字证书。在 RFC 2986 中重新定义。

① 证书请求信息格式用 ASN.1 描述如下：

```
CertificationRequestInfo ::= SEQUENCE {
    version                 INTEGER { v1（0） }  （v1,...）,
    subject                 Name,
    subjectPKInfo       SubjectPublicKeyInfo{{ PKInfoAlgorithms }},
    attributes              [0] Attributes{{ CRIAttributes }}
}
SubjectPublicKeyInfo { ALGORITHM : IOSet} ::= SEQUENCE {
    algorithm               AlgorithmIdentifier {{IOSet}},
    subjectPublicKey   BIT STRING
}
PKInfoAlgorithms ALGORITHM ::= {
    ...     -- add any locally defined algorithms here -- }
Attributes { ATTRIBUTE:IOSet } ::= SET OF Attribute{{ IOSet }}
CRIAttributes   ATTRIBUTE   ::= {
    ...   -- add any locally defined attributes here -- }
Attribute { ATTRIBUTE:IOSet } ::= SEQUENCE {
    type     ATTRIBUTE.&id（{IOSet}）,
    values   SET SIZE（1..MAX）  OF ATTRIBUTE.&Type（{IOSet}{@type}）
}
```

② 证书请求格式用 ASN.1 描述如下：

```
CertificationRequest ::= SEQUENCE {
    certificationRequestInfo   CertificationRequestInfo,
    signatureAlgorithm   AlgorithmIdentifier{{ SignatureAlgorithms }},
    signature                           BIT STRING
}
AlgorithmIdentifier {ALGORITHM:IOSet } ::= SEQUENCE {
    algorithm     ALGORITHM.&id（{IOSet}）,
```

```
        parameters    ALGORITHM.&Type（{IOSet}{@algorithm}）  OPTIONAL
    }
    SignatureAlgorithms ALGORITHM ::= {
        ...   -- add any locally defined algorithms here -- }
```

9．PKCS #11：Cryptographic Token Interface Standard（密码 Token 接口标准）

PKCS #11 v2.2 定义了一种与密码设备（如智能卡）无关的编程接口技术。主要包括以下内容：

① 通用数据类型（Genaral Data Types）。主要分为 7 类。

A．通用信息类型：CK_VERSION、CK_INFO、CK_NOTIFICATION；

B．Slot 及 Token 类型：CK_SLOT_ID、CK_SLOT_INFO、CK_TOKEN_INFO；

C．Session 类型：CK_SESSION_HANDLE、CK_USER_TYPE、CK_STATE、CK_SESSION_INFO；

D．对象类型：CK_OBJECT_HANDLE、CK_OBJECT_CLASS、CK_HW_FEATURE_TYPE、CK_KEY_TYPE、CK_CERTIFICATE_TYPE、CK_ATTRIBUTE_TYPE、CK_ATTRIBUTE、CK_DATE；

E．机制相关类型：CK_MECHANISM_TYPE、CK_MECHANISM、CK_ MECHANIS M_INFO；

F．函数类型：CK_RV、CK_NOTIFY、CK_C_XXX、CK_FUNCTION_LIST；

G．Locking 相关类型：CK_CREATEMUTEX、CK_DESTROYMUTEX、CK_LOCK-MUTEX、CK_UNLOCKMUTEX、CK_C_INITIALIZE_ARGS。

② 对象（Objects）。

主要分为以下几类：硬件特征对象、数据对象、证书对象、密钥对象、域参数对象和机制对象等。证书对象又分为 X.509 公钥证书对象、WTLS 公钥证书对象和 X.509 属性证书对象。密钥对象又分为公钥对象、私钥对象和秘密密钥对象。

③ 函数（Functions）。

主要分为以下几类：

A．通用功能函数。共 4 个：C_Initialize、C_Finalize、C_GetInfo、C_GetFunctionList；

B．Slot 及 Token 管理函数。共 9 个：C_GetSlotList、C_GetSlotInfo、C_GetTokenInfo、C_WaitForSlotEvent、C_GetMechanismList、C_GetMechanismInfo、C_InitToken、C_InitPIN、C_SetPIN；

C．Session 管理函数。共 8 个：C_OpenSession、C_CloseSession、C_CloseAllSessions、C_GetSessionInfo、C_GetOperationState、C_SetOperationState、C_Login、C_Logout；

D．对象管理函数。共 9 个：C_CreateObject、C_CopyObject、C_DestroyObject、C_GetObjectSize、C_GetAttributeValue、C_SetAttributeValue、C_FindObjectsInit、C_FindObjects、C_FindObjectsFinal；

E．加密函数。共 4 个：C_EncryptInit、C_Encrypt、C_EncryptUpdate、C_EncryptFinal；

F．解密函数。共 4 个：C_DecryptInit、C_Decrypt、C_DecryptUpdate、C_DecryptFinal；

G．消息摘要函数。共 5 个：C_DigestInit、C_Digest、C_DigestUpdate、C_DigestKey、C_DigestFinal；

H．签名及 MAC 函数。共 6 个：C_SignInit、C_Sign、C_SignUpdate、C_SignFinal、C_SignRecoverInit、C_SignRecover；

I．验证签名及 MAC 函数。共 6 个：C_VerifyInit、C_Verify、C_VerifyUpdate、C_VerifyFinal、C_VerifyRecoverInit、C_VerifyRecover；

J．双功能（dual-purpose）密码函数。共 4 个：C_DigestEncryptUpdate、C_DecryptDigestUpdate、C_SignEncryptUpdate、C_DecryptVerifyUpdate；

K．密钥管理函数。共 5 个：C_GenerateKey、C_GenerateKeyPair、C_WrapKey、C_UnwrapKey、C_DeriveKey；

L．随机数生成函数。共 2 个：C_SeedRandom、C_GenerateRandom；

M．并行函数管理函数。共 2 个：C_GetFunctionStatus、C_CancelFunction。

④ 机制（Mechanisms）。

机制规定了特定的密码操作过程如何准确地执行。主要包括以下几类：

RSA、DSA、Elliptic Curve、Diffie-Hellman、KEA、Wrapping/unwrapping private keys、Generic secret key、HMAC mechanisms、RC2、RC4、RC5、AES、General block cipher、Key derivation by data encryption – DES & AES、Double and Triple-length DES、SKIPJACK、BATON、JUNIPER、MD2、MD5、SHA-1、SHA-256、SHA-384、SHA-512、FASTHASH、PKCS #5 and PKCS #5-style password-based encryption（PBE）、PKCS #12 password-based、encryption/authentication mechanisms、RIPE-MD、SET、LYNKS、SSL、TLS、WTLS、Miscellaneous simple key derivation mechanisms、CMS、Blowfish、Twofish。

10．PKCS #12：Personal Information Exchange Syntax Standard（个人信息交换语法标准）

PKCS #12 v1.0 描述了用于存储和传递个人身份信息的语法格式。个人身份信息包括私钥、证书、各种秘密及扩展等。支持本标准的机器设备、应用系统、浏览器、上网亭（Internet Kiosk）等应允许用户导入、导出和操作这种格式的个人身份信息。它的目标是为各种应用提供一个标准的单一密钥文件。常见的 PFX 文件就是遵循 PKCS#12 格式的文件。

个人身份信息格式用 ASN.1 描述如下：

```
PFX ::= SEQUENCE {
    version     INTEGER {v3（3）}（v3,...）,
    authSafe    ContentInfo,
    macData         MacData OPTIONAL
}
MacData ::= SEQUENCE {
    mac         DigestInfo,
    macSalt     OCTET STRING,
    iterations  INTEGER DEFAULT 1
    -- Note: The default is for historical reasons and its use is deprecated. A higher
    -- value, like 1024, is recommended.
}
```

11．PKCS #15：Cryptographic Token Information Format Standard（密码 Token 信息格式标准）

PKCS #15 v1.1 描述了存储于密码 Token 中密码凭证的一种格式标准，允许密码令牌的用户向应用程序标识自己。此标准独立于 PKCS＃11 接口或其他 API。RSA 已经放弃了这个标准的 IC 卡的相关部分，并提交给了 ISO/IEC 7816-15。

29.2　ISO 7816 系列

ISO/IEC 7816 是电子识别卡或智能卡的国际标准，由 ISO（International Organization for Standardization）和 IEC（International Electrotechnical Commission）组织共同维护，目前包括 14 部分。

1．ISO 7816-1：Physical characteristics（卡的物理特性）

本部分规定了带触点集成电路卡的基本技术要求，主要包括以下内容：

① 物理特性、记录方法、物理接口要求，主要定义了该类卡的基本物理特性；

② 电气信号和传输协议，规定了该类卡和终端间的电源、电气信号协议和信息交换协议，涉及卡的信号频率、电压值、电流值、校验、操作规程和传输与通信协议。

2．ISO 7816-2：Cards with contacts：Dimensions and location of the contacts（触点集成电路卡：触点的尺寸与位置）

本部分定义了 ID-1 类型集成电路卡每个触点的尺寸与位置，同时提供了哪个标准定义了这些触点的信息。

3．ISO 7816-3：Cards with contacts：Electrical interface and transmission protocols（触点集成电路卡：电信号和传输协议）

本部分规定了电源和信号的结构，以及集成电路卡和接口设备（如终端）之间的信息交换。它还覆盖了信号速率、电压等级、电流值、奇偶约定、操作程序、传输机制及与卡的通信。但它不包括信息和指令的内容，如发行人和使用者的识别、服务和限制、安全功能、日志记录和指令定义等。

4．ISO 7816-4：Organization, security and commands for interchange（用于交换的结构、安全和命令）

本部分规定了：

① 由接口设备至卡以及相反方向所发送的报文、命令和响应的内容；

② 获取卡内数据对象和元素的方式；

③ 在复位应答期间卡所发送的历史字节的结构及内容；

④ 当处理交换用的命令时，在接口处所看到的文件和数据的结构；

⑤ 访问卡内文件和数据的方法；

⑥ 定义访问卡内文件和数据的权限的安全体系结构；

⑦ 安全报文交换的方法；

⑧ 访问卡所处理算法的方法。本标准不描述这些算法。

本规范没有涵盖卡内和/或外界的内部实现。

5. ISO 7816-5：Registration of application providers（卡应用提供者注册）

本部分定义了如何使用应用标识符（application identifier）确认卡上存在应用和从卡上获取应用。应用标识符标示卡中应用的元素，可以通过一个全局注册中心保证应用标识符的唯一性。

本标准确定了各种机构和规程，以确保和优化相应注册的可靠性。

6. ISO 7816-6：Interindustry data elements for interchange（行业间数据元）

本部分规定了在行业间使用的数据元素（包括复合数据元素），它定义了每个数据元素的以下特征：标识符、名称、说明和参考、格式和编码。

每个数据元素的布局以接口设备和卡之间可见的方式描述。

本文档提供了数据元素的定义而不考虑对它的任何使用限制。

本规范没有涵盖卡内和/或外界的内部实现。

7. ISO 7816-7：Interindustry commands for Structured Card Query Language（SCQL）（用于结构化卡查询语言（SCQL）的行业间命令）

本部分定义了：

① SCQL 数据库概念，SCQL（Structured Card Query Language）表示结构化卡查询语言，基于 SQL（参见 ISO 9075）；

② 相关的行业间增强命令。

8. ISO 7816-8：Commands for security operations（与安全相关的行业间命令）

本部分规定了用于密码操作的行业间命令，密码机制的选择和使用条件可能影响卡的输出，算法和协议的适宜性评估在本标准范围之外。本部分规定了：

① 卡中使用的安全协议；

② 安全报文交换扩展；

③ 卡的安全功能/服务上的安全机制的映射，包括卡内安全机制的描述；

④ 安全支持的数据元；

⑤ 在卡上实现的算法的使用（算法本身并不详细描述）；

⑥ 证书的使用；

⑦ 与安全相关的命令。

本规范没有涵盖卡内和/或外界的内部实现，并且不强制卡支持本部分描述的所有命令或命令的所有选项。

9. ISO 7816-9：Commands for card management（用于卡管理的命令）

本部分规定了用于卡管理和文件管理的行业间命令。这些命令覆盖卡的整个生命周期，因此，有些命令在卡发行到持卡者手中之前就被使用，有些命令在卡终止后仍被使用。

本规范没有涵盖卡内和（或）外界的内部实现。

本规范的附件展示了如何控制加载数据（加载数据包括代码、密钥、小程序等）到卡中，如可以通过校验加载实体的权限、以安全消息方式传输数据等。