

CFCA

中金金融认证中心标准

30001.01—2012

SM2 数字证书申请及应用 CSP 接口调用规范

Interface specification of CSP

for SM2 certificate enrollment and application

2012-08-01 发布

2012-08-01 实施

中金金融认证中心

发布

目 录

1. 范围 1

2. 规范性引用文件..... 1

3. 术语和定义 1

4. SM2 数字证书申请调用 CSP 接口规范 2

 4.1 SM2 数字证书申请流程..... 2

 4.2 CSP 接口描述..... 3

5. SM2 数字证书导入调用 CSP 接口规范 5

 5.1 SM2 签名证书导入流程..... 5

 5.2 SM2 加密证书导入流程..... 6

6. SM2 证书数字签名调用 CSP 接口规范 8

 6.1 使用 SM2 证书进行数字签名流程..... 8

 6.2 CSP 接口描述..... 8

7. SM2 公私钥结构定义 10

 7.1 SM2, SM3 算法常量定义 10

 7.2 SM2 公钥结构 11

 7.3 SM2 私钥结构 12

SM2 数字证书申请及应用 CSP 接口调用规范

1. 范围

本规范中，描述了通过 CSP 接口实现 SM2 数字证书申请及应用时，所涉及接口的实现标准。
本规范中未涉及的接口，请参照微软 CSP 接口标准实现。

2. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件，凡是不注日期的引用文件，其最新版本适用于本文件。

GM/T 0002-2012	SM4 分组密码算法
GM/T 0003-2012	SM2 椭圆曲线公钥密码算法
GM/T 0004-2012	SM3 密码杂凑算法
GM/T 0009-2012	SM2 密码算法使用规范
GM/T 0010-2012	SM2 密码算法加密签名消息语法规范

3. 术语和定义

数字证书

也称公钥证书，由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按用途可分为签名证书、加密证书。

公钥

非对称密码算法中可以公开的密钥。

私钥

非对称密码算法中，只能由拥有者使用的不公开密钥。

椭圆曲线密码算法

基于有限域上椭圆曲线离散对数问题的非对称密码算法。

SM2 密码算法

一种椭圆曲线密码算法，密钥长度为 256 比特。

SM3 算法

一种杂凑算法，输出长度为 256 比特。

SM4 算法

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

4. SM2 数字证书申请调用 CSP 接口规范

4.1 SM2 数字证书申请流程

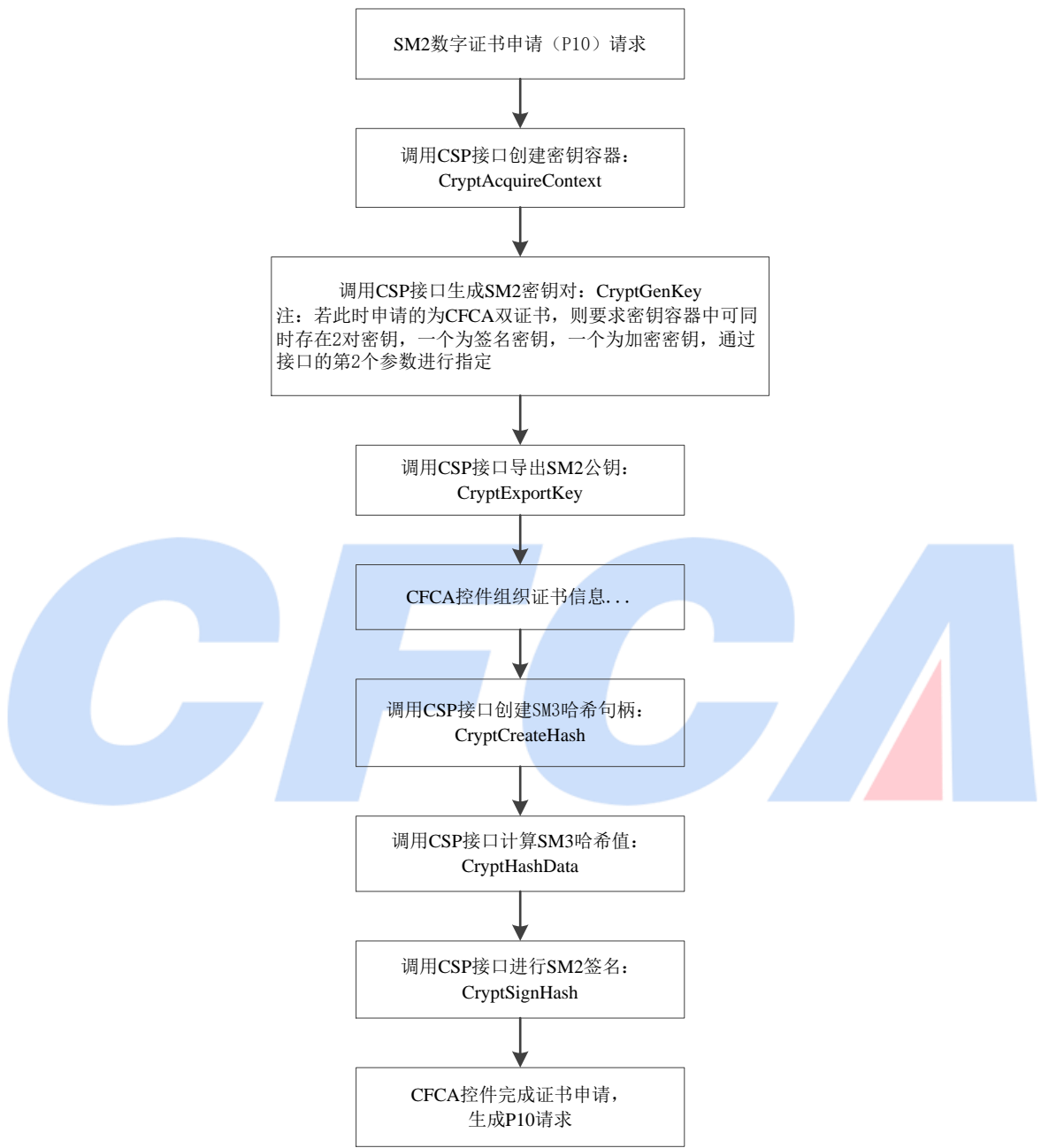


图 1 SM2 数字证书申请流程

4.2 CSP 接口描述

4.2.1 CryptAcquireContext

```

BOOL WINAPI CryptAcquireContext(__out HCRYPTPROV *phProv,
                                __in LPCTSTR pszContainer,
                                __in LPCTSTR pszProvider,
                                __in DWORD dwProvType,
                                __in DWORD dwFlags)

```

描述：创建密钥容器。

特殊参数取值说明：pszContainer：待创建的密钥容器的名称

dwProvType：1

dwFlags：CRYPT_NEWKEYSET

4.2.2 CryptGenKey

```

BOOL WINAPI CryptGenKey(__in HCRYPTPROV hProv,
                        __in ALG_ID Algid,
                        __in DWORD dwFlags,
                        __out HCRYPTKEY *phKey)

```

描述：生成 SM2 密钥对。

特殊参数取值说明：Algid：CALG_SM2_SIGN 代表签名密钥，对应的密钥用法为 AT_SIGNATURE；CALG_SM2_KEYX 代表加密密钥，对应的密钥用法为 AT_KEYEXCHANGE，详细定义详见章节 7

4.2.3 CryptExportKey

```

BOOL WINAPI CryptExportKey(__in HCRYPTKEY hKey,
                           __in HCRYPTKEY hExpKey,
                           __in DWORD dwBlobType,
                           __in DWORD dwFlags,
                           __out BYTE *pbData,
                           __inout DWORD *pdwDataLen)

```

描述：导出 SM2 公钥。

特殊参数取值说明：dwBlobType：PUBLICKEYBLOB

pbData：公钥数据，定义详见章节 7

4.2.4 CryptCreateHash

```

BOOL WINAPI CryptCreateHash( __in    HCRYPTPROV    hProv,
                             __in    ALG_ID        Algid,
                             __in    HCRYPTKEY      hKey,
                             __in    DWORD         dwFlags,
                             __out    HCRYPTHASH    *phHash)

```

描述： 创建 SM3 哈希句柄。

特殊参数取值说明： Algid: CALG_SM3 表示 SM3 哈希算法，详细定义详见章节 7

4.2.5 CryptHashData

```

BOOL WINAPI CryptHashData( __in HCRYPTHASH    hHash,
                           __in BYTE          *pbData,
                           __in DWORD         dwDataLen,
                           __in DWORD         dwFlags)

```

描述： 对数据进行 SM3 哈希运算。

特殊参数取值说明： 无

4.2.6 CryptSignHash

```

BOOL WINAPI CryptSignHash( __in    HCRYPTHASH    hHash,
                           __in    DWORD         dwKeySpec,
                           __in    LPCTSTR       sDescription,
                           __in    DWORD         dwFlags,
                           __out    BYTE          *pbSignature,
                           __inout DWORD         *pdwSigLen)

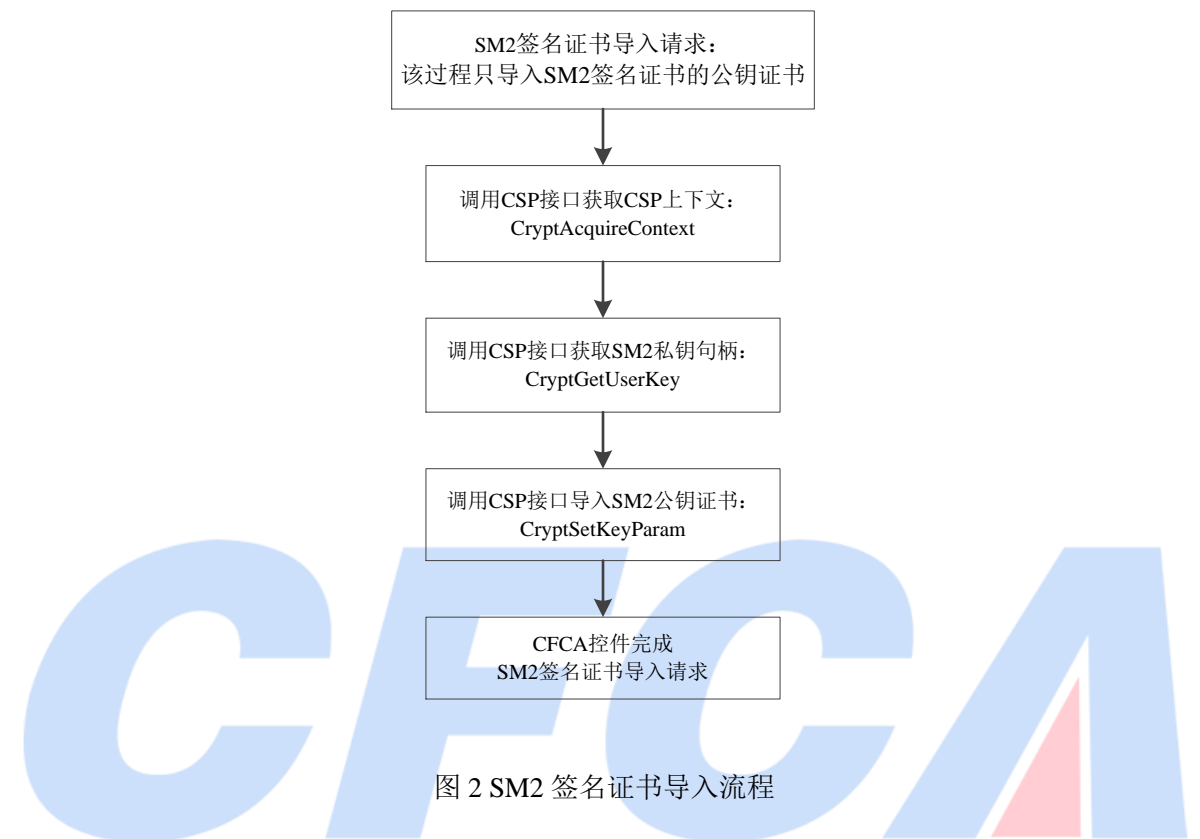
```

描述： 对 SM3 哈希值进行 SM2 签名。

特殊参数取值说明： dwKeySpec: AT_KEYEXCHANGE 或 AT_SIGNATURE

5. SM2 数字证书导入调用 CSP 接口规范

5.1 SM2 签名证书导入流程



5.1.1 CSP 接口描述

5.1.1.1 CryptAcquireContext

```
BOOL WINAPI CryptAcquireContext( __out    HCRYPTPROV    *phProv,
                                   __in     LPCTSTR       pszContainer,
                                   __in     LPCTSTR       pszProvider,
                                   __in     DWORD         dwProvType,
                                   __in     DWORD         dwFlags)
```

描述： 获取 CSP 上下文。

特殊参数取值说明： pszContainer：待获取的密钥容器的名称
 dwProvType： 1
 dwFlags： CRYPT_VERIFYCONTEXT

5.1.1.2 CryptGetUserKey

```

BOOL WINAPI CryptGetUserKey( __in   HCRYPTPROV   hProv,
                             __in   DWORD       dwKeySpec,
                             __out  HCRYPTKEY    *phUserKey)

```

描述： 获得 SM2 私钥句柄。

特殊参数取值说明： dwKeySpec: AT_KEYEXCHANGE 或 AT_SIGNATURE

5.1.1.3 CryptSetKeyParam

```

BOOL WINAPI CryptSetKeyParam( __in   HCRYPTKEY    hKey,
                              __in   DWORD       dwParam,
                              __in   const BYTE   *pbData,
                              __in   DWORD       dwFlags)

```

描述： 导入 SM2 公钥证书。

特殊参数取值说明： hKey: SM2 私钥句柄

dwParam: KP_CERTIFICATE

5.2 SM2 加密证书导入流程

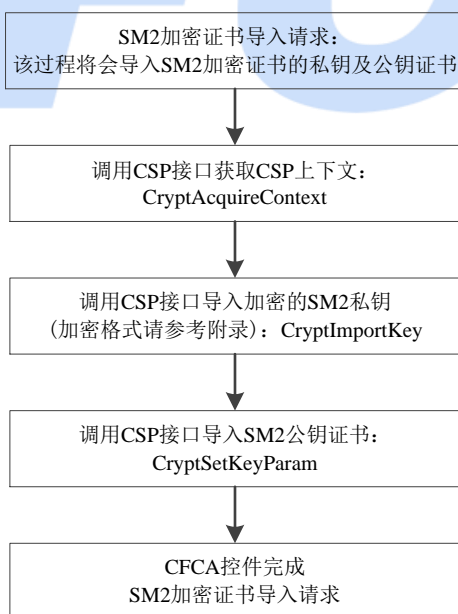


图 3 SM2 加密证书导入流程

5.2.1 CSP 接口描述

5.2.1.1 CryptAcquireContext

```

BOOL WINAPI CryptAcquireContext( __out    HCRYPTPROV    *phProv,
                                   __in     LPCTSTR      pszContainer,
                                   __in     LPCTSTR      pszProvider,
                                   __in     DWORD         dwProvType,
                                   __in     DWORD         dwFlags)

```

描述： 获取 CSP 上下文。

特殊参数取值说明： **pszContainer**: 待获取的密钥容器的名称
dwProvType: 1
dwFlags: CRYPT_VERIFYCONTEXT

5.2.1.2 CryptImportKey

```

BOOL WINAPI CryptImportKey( __in     HCRYPTPROV    hProv,
                             __in     BYTE         *pbData,
                             __in     DWORD         dwDataLen,
                             __in     HCRYPTKEY     hPubKey,
                             __in     DWORD         dwFlags,
                             __out    HCRYPTKEY     *phKey)

```

描述： 导入 SM2 私钥（对应于密钥容器中的 KEY EXCHANGE 类型）。

特殊参数取值说明： **pbData**: 加密的 SM2 私钥数据，数据结构定义详见章节 7
hPubKey: 此参数为 NULL（导入的公钥存在于 pbData 参数中）

5.2.1.3 CryptSetKeyParam

```

BOOL WINAPI CryptSetKeyParam( __in     HCRYPTKEY     hKey,
                               __in     DWORD         dwParam,
                               __in     const BYTE     *pbData,
                               __in     DWORD         dwFlags)

```

描述： 导入 SM2 公钥证书。

特殊参数取值说明： **hKey**: SM2 私钥句柄（此处的句柄是 5.2.1.2 小节中
CryptImportKey 函数传出的 *phKey）
dwParam: KP_CERTIFICATE

6. SM2 证书数字签名调用 CSP 接口规范

6.1 使用 SM2 证书进行数字签名流程

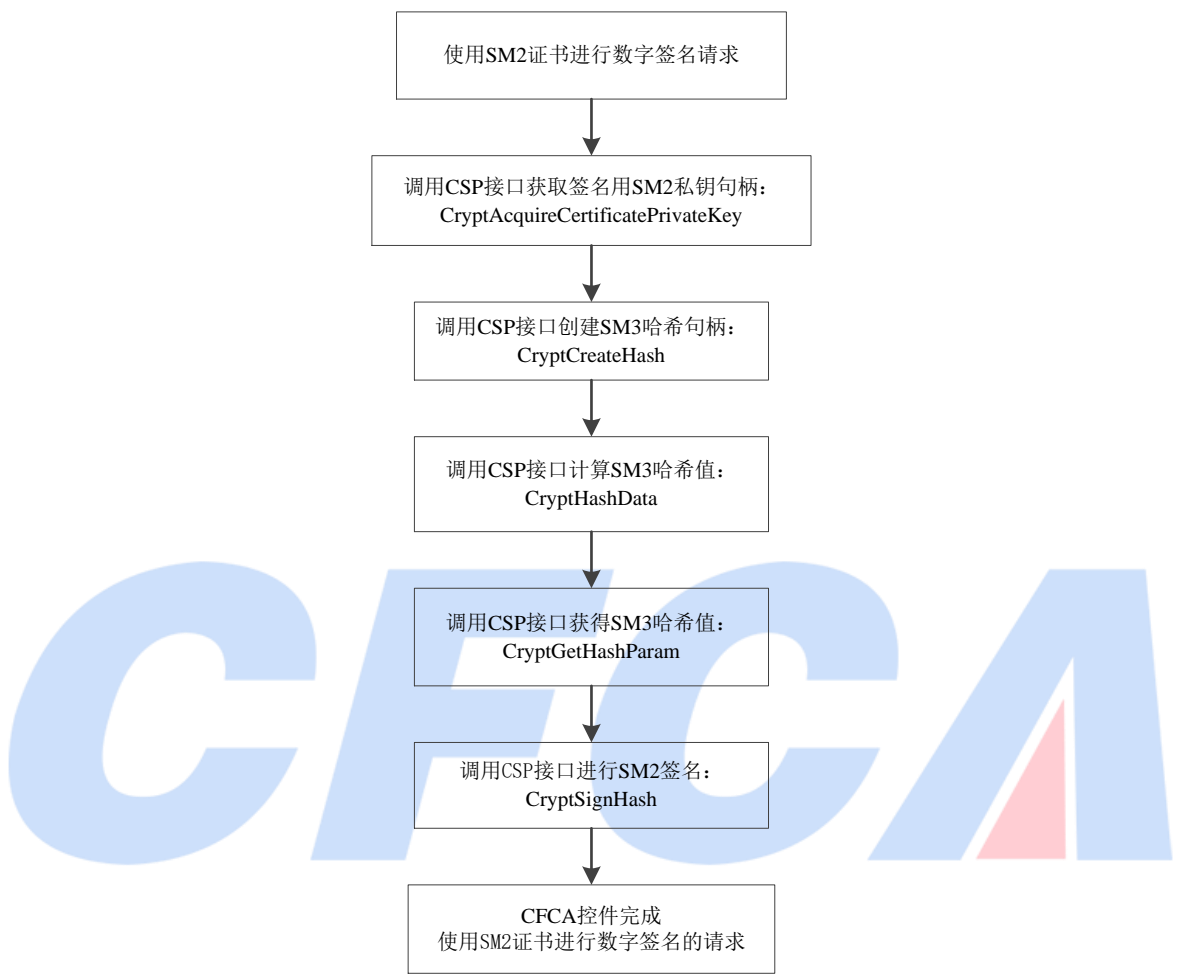


图 4 SM2 证书签名流程

6.2 CSP 接口描述

6.2.1 CryptAcquireCertificatePrivateKey

```
BOOL WINAPI CryptAcquireCertificatePrivateKey(  
    __in PCCERT_CONTEXT pCert,  
    __in DWORD dwFlags,  
    __in void *pvReserved,  
    __out HCRYPTPROV_OR_NCRYPT_KEY_HANDLE *phCryptProvOrNCryptKey,  
    __out DWORD *pdwKeySpec,  
    __out BOOL *pfCallerFreeProvOrNCryptKey)
```

描述： 获取指定证书的 CSP 上下文。

特殊参数取值说明： pdwKeySpec: AT_KEYEXCHANGE 或 AT_SIGNATURE

6.2.2 CryptCreateHash

```

BOOL WINAPI CryptCreateHash (__in    HCRYPTPROV    hProv,
                              __in    ALG_ID        Algid,
                              __in    HCRYPTKEY      hKey,
                              __in    DWORD          dwFlags,
                              __out    HCRYPTHASH    *phHash)

```

描述： 创建 SM3 哈希句柄。

特殊参数取值说明： Algid: CALG_SM3, 表示 SM3 哈希算法, 详细定义见章节 7

6.2.3 CryptHashData

```

BOOL WINAPI CryptHashData( __in HCRYPTHASH    hHash,
                           __in BYTE          *pbData,
                           __in DWORD          dwDataLen,
                           __in DWORD          dwFlags)

```

描述： 对数据进行 SM3 哈希运算。

特殊参数取值说明： 无

6.2.4 CryptGetHashParam

```

BOOL WINAPI CryptGetHashParam( __in    HCRYPTHASH    hHash,
                                __in    DWORD          dwParam,
                                __out    BYTE          *pbData,
                                __inout  DWORD          *pdwDataLen,
                                __in    DWORD          dwFlags)

```

描述： 获得 SM3 哈希值。

特殊参数取值说明： 无

6.2.5 CryptSignHash

```
BOOL WINAPI CryptSignHash( __in    HCRYPTHASH    hHash,
                           __in    DWORD         dwKeySpec,
                           __in    LPCTSTR       sDescription,
                           __in    DWORD         dwFlags,
                           __out    BYTE         *pbSignature,
                           __inout  DWORD        *pdwSigLen)
```

描述：对 SM3 哈希值进行 SM2 签名。

特殊参数取值说明： dwKeySpec: AT_KEYEXCHANGE 或 AT_SIGNATURE
pbSignature: SM2 签名值，其中 R、S 均为小字节序

7. SM2 公私钥结构定义

7.1 SM2, SM3 算法常量定义

```
#define SM2_MAX_XCOORDINATE_BITS_LEN    512
#define SM2_MAX_YCOORDINATE_BITS_LEN    512
#define SM2_MAX_MODULUS_BITS_LEN        512
#define ALG_TYPE_SM2                    (15 << 9)
#define ALG_SID_SM2_ANY                  0
#define ALG_SID_SM3                      15

#define CALG_SM2_SIGN                    (ALG_CLASS_SIGNATURE|ALG_TYPE_SM2|ALG_SID_SM2_ANY)
#define CALG_SM2_KEYX                    (ALG_CLASS_KEY_EXCHANGE|ALG_TYPE_SM2|ALG_SID_SM2_ANY)
#define CALG_SM3                         (ALG_CLASS_HASH|ALG_TYPE_ANY|ALG_SID_SM3)
```

7.2 SM2 公钥结构

SM2 公钥包含包含以下 2 部分：

BLOBHEADER；

SM2PUBLICKEYBLOB。

其中 BLOBHEADER 为微软标准定义，SM2PUBLICKEYBLOB 为自定义数据结构。

SM2PUBLICKEYBLOB 数据结构定义如下：

```
typedef struct Struct_SM2PUBLICKEYBLOB{
    ULONG BitLen;
    BYTE XCoordinate[SM2_MAX_XCOORDINATE_BITS_LEN/8];
    BYTE YCoordinate[SM2_MAX_YCOORDINATE_BITS_LEN/8];
}SM2PUBLICKEYBLOB, *PSM2PUBLICKEYBLOB;
```

其中：

BitLen 取值为：256，代表模数的实际位长度

备注：

1、BLOBHEADER 取值目前可忽略

2、SM2 公钥的 X、Y 值为小字节序（LITTLE-ENDIAN），且目前均为 32 个 byte，剩余的 32byte 均补 0。

SM2 公钥数据例子：

```
06 02 00 00 00 3E 00 00 00 01 00 00 93 6E B0 FD
0C FB 4B AC CD 6F C0 A8 8D 5F 0B 29 EC EB 96 67
9F 6B 18 9D BD 14 09 8B F8 AA 66 C6 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 35 20 FA 26
CD 46 C4 DE 99 F8 2A C3 45 04 F1 94 A0 25 ED D8
5C 08 65 F4 17 06 22 4C 0C 91 62 8F 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00
```

7.3 SM2 私钥结构

SM2 私钥包含以下 2 部分：

BLOBHEADER;
SM2PRIVATEKEYBLOB

其中 BLOBHEADER 为微软标准定义，SM2PRIVATEKEYBLOB 为自定义数据结构。

BLOBHEADER 结构取值如下：

```
typedef struct _PUBLICKEYSTRUC {
    BYTE    bType;
    BYTE    bVersion;
    WORD    reserved;
    ALG_ID  aiKeyAlg;
} BLOBHEADER, PUBLICKEYSTRUC;
```

其中：

- 1、bType 取值为：PRIVATEKEYBLOB (0x7)
- 2、bVersion 取值为：CUR_BLOB_VERSION (0x2)
- 3、reserved 取值为：0x1，用于代表 SM2 私钥是加密的格式
- 4、aiKeyAlg 取值为：CALG_SM2_KEYX

SM2PRIVATEKEYBLOB 数据结构定义：

```
typedef struct _SM2PRIVATEKEYBLOB {
    ULONG    AlgID;
    ULONG    EncryptedPrivateKeyBitLen;
    BYTE     *EncryptedPrivateKey;
} SM2PRIVATEKEYBLOB, *PSM2PRIVATEKEYBLOB;
```

其中：

- 1、AlgID 取值为：CALG_SM2_SIGN 或 CALG_SM2_KEYX
- 2、EncryptedPrivateKeyBitLen 取值为：加密 SM2 私钥 EncryptedPrivateKey 的实际位(bit)长度
- 3、EncryptedPrivateKey 取值为：加密的 SM2 密钥对（公私钥）数据

备注：

- 1、参数 EncryptedPrivateKeyBitLen 的值代表加密私钥的实际位长度。
- 2、加密私钥密文 EncryptedPrivateKey 存在两种格式：
 - 一种为 C1||C2||C3（国密老的标准），另一种为 C1||C3||C2（国密最新标准）。
 - CSP 需要能够自动兼容上述两种私钥密文格式。
- 3、解密后的 SM2 密钥对为 x||y||d，其中 x，y 是 32 字节的公钥坐标点，d 是 32 字节的私钥。