CFCA SM2 数字证书申请及证书应用

CSP 接口调用规范

（版本：3.0.5）

中国金融认证中心

2014 年 08 月 15 日

文档修订记录

本文档会随时保持更新，请与中国金融认证中心索要最新版本。

版本	内容	日期	编写	审核
3.0.0	初稿完成	2012/8/1	李哲	林峰
3.0.1	修改文档中的书写错误	2012/8/14	李哲	
3.0.2	SM2 私钥结构修改	2012/8/15	李哲	
3.0.3	SM2 私钥需要以加密方式倒入 USB key（类数字信封）	2012/9/28	林峰	
3.0.4	SM2 私钥修改为直接使用 SM2 临时公钥加密的方式倒入	2012/9/29	林峰	
3.0.5	增加一种 SM2 密钥对的密文格式 C1||C3||C2，以支持国密最新标准	2014/10/20	秘相友	

目　录

1. 概述 1

1.1 文档描述 1

1.2 参考文件 1

2. SM2 数字证书申请调用 CSP 接口规范 2

2.1 SM2 数字证书申请流程 2

2.2 CSP 接口描述 3

2.2.1 CryptAcquireContext 3

2.2.2 CryptGenKey 3

2.2.3 CryptExportKey 4

2.2.4 CryptCreateHash 4

2.2.5 CryptHashData 4

2.2.6 CryptSignHash 5

3. SM2 数字证书导入调用 CSP 接口规范 5

3.1 SM2 签名证书导入流程 5

3.1.1 CSP 接口描述 6

3.1.1.1 CryptAcquireContext 6

3.1.1.2 CryptGetUserKey 7

3.1.1.3 CryptSetKeyParam 7

3.2 SM2 加密证书导入流程 7

3.2.1 CSP 接口描述 8

3.2.1.1 CryptAcquireContext 8

3.2.1.2 CryptImportKey 9

3.2.1.3 CryptSetKeyParam 9

4. SM2 证书数字签名调用 CSP 接口规范 10

4.1 使用 SM2 证书进行数字签名流程 10

4.2 CSP 接口描述 10

4.2.1 CryptAcquireCertificatePrivateKey 11

4.2.2 CryptCreateHash 11

4.2.3 CryptHashData 11

4.2.4 CryptGetHashParam 12

4.2.5 CryptSignHash 12

5. SM2 公私钥结构定义 13

5.1 SM2, SM3 算法常量定义 13

5.2 SM2 公钥结构 13

5.3 SM2 私钥结构 14

1. 概述

1.1 文档描述

本文档描述了：

1、 申请 CFCA SM2 数字证书所需调用的 CSP 接口。

2、 导入 CFCA SM2 数字证书（包括签名证书及加密证书）所需调用的 CSP 接口。

3、 使用 CFCA SM2 数字证书完成数字签名所需调用的 CSP 接口。

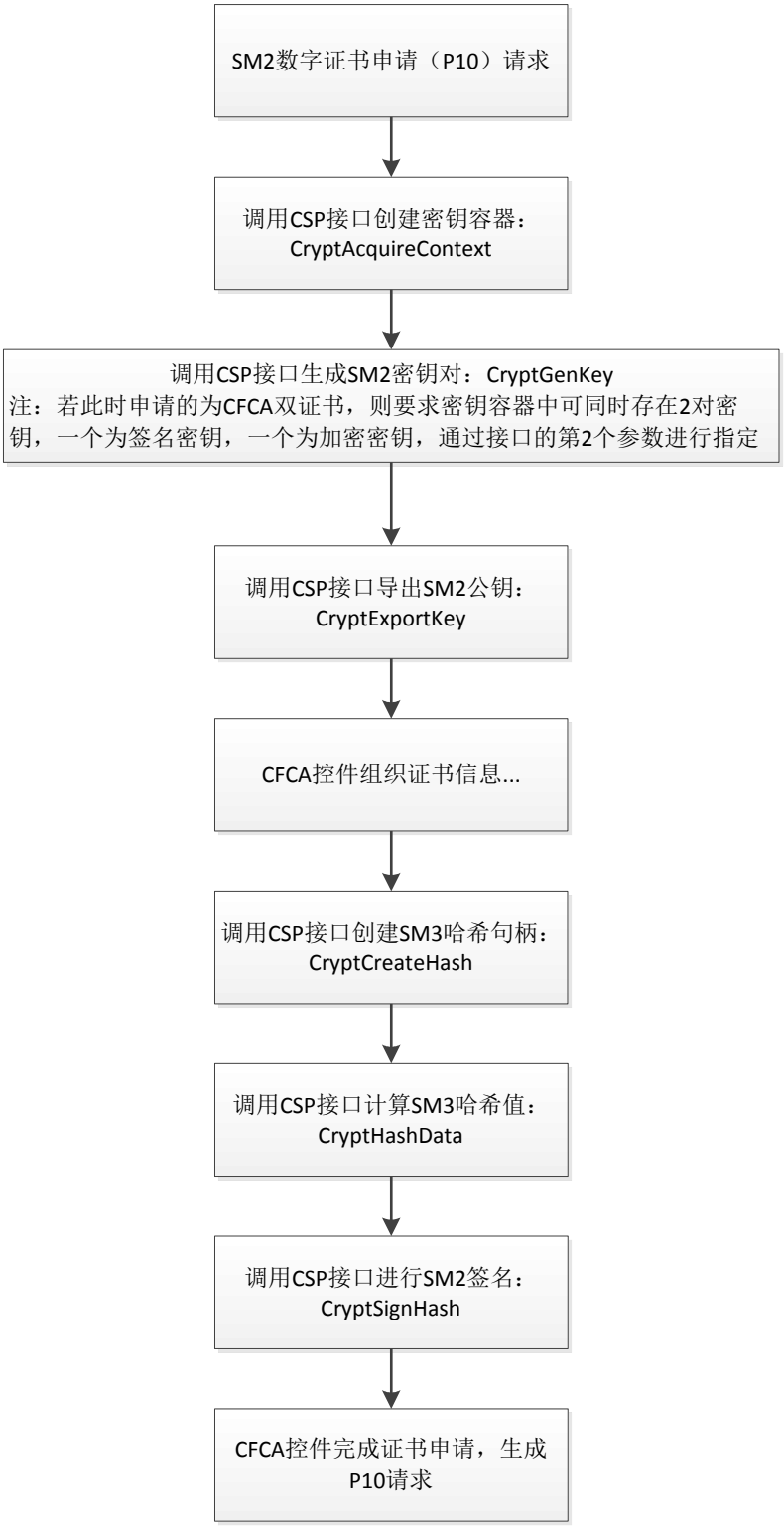
在 CSP 接口描述中，特殊说明的参数需注意，没有特殊说明的参数均按照微软的接口标准实现。

1.2 参考文件

参考文件名	发布日期	评述
《SM2 椭圆曲线公钥密码算法》	2012-03-21	

2. SM2 数字证书申请调用 CSP 接口规范

2.1 SM2 数字证书申请流程



2.2 CSP 接口描述

2.2.1 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

2.2.2 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　签名密钥；CALG_SM2_KEYX 加密密钥，

详细定义详见章节 5

CALG_SM2_SIGN 对应的密钥用法为 AT_SIGNATURE；

CALG_SM2_KEYX 对应的密钥用法为 AT_KEYEXCHANGE

2.2.3 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 5

2.2.4 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 5

2.2.5 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

2.2.6 CryptSignHash

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

描述：

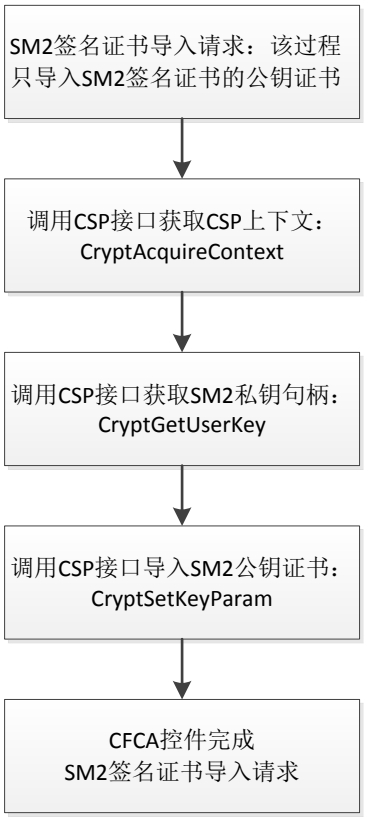
对 SM3 哈希值进行 SM2 签名。

特殊参数取值说明：

dwKeySpec：AT_KEYEXCHANGE 或 AT_SIGNATURE（使用微软标准定义）

3. SM2 数字证书导入调用 CSP 接口规范

3.1 SM2 签名证书导入流程



3.1.1 CSP 接口描述

3.1.1.1 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

3.1.1.2 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（采用微软标准定义）

3.1.1.3 CryptSetKeyParam

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

描述：

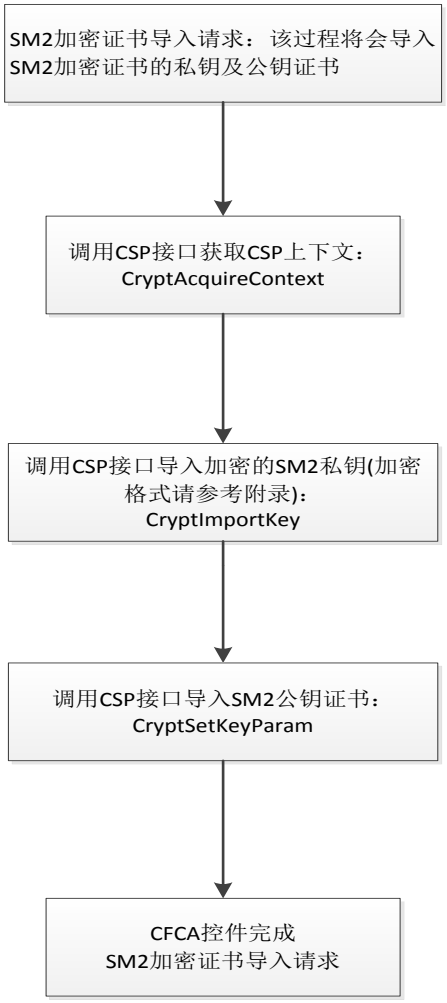
导入 SM2 公钥证书。

特殊参数取值说明：

hKey：SM2私钥句柄

dwParam：KP_CERTIFICATE

3.2 SM2 加密证书导入流程



3.2.1 CSP 接口描述

3.2.1.1 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

3.2.1.2 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5

hPubKey:此参数为NULL（倒入的公钥存在于pbData参数中）

3.2.1.3 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。

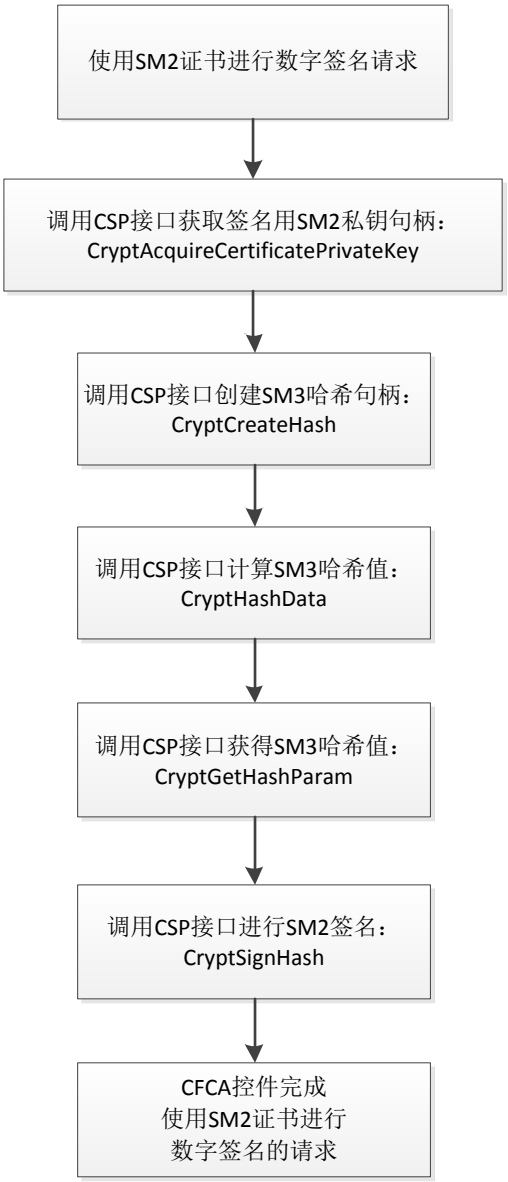
特殊参数取值说明：

hKey：SM2私钥句柄（此处的句柄是3.2.1.2小节中CryptImportKey函数传出的*phKey）

dwParam：KP_CERTIFICATE

4. SM2 证书数字签名调用 CSP 接口规范

4.1 使用 SM2 证书进行数字签名流程



4.2 CSP 接口描述

4.2.1 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（采用微软标准定义）

4.2.2 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 5

4.2.3 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

4.2.4 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

4.2.5 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（采用微软标准定义）

pbSignature：SM2 签名值，其中 R、S 均为小字节序

5. SM2 公私钥结构定义

5.1 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 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 ALG_TYPE_SM2     (15 << 9)
#define ALG_SID_SM2_ANY  0
#define CALG_SM3         (ALG_CLASS_HASH| ALG_TYPE_ANY | ALG_SID_SM3)
#define ALG_SID_SM3      15
```

5.2 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：

```
typedef struct Struct_SM2PUBLICKEYBLOB{
    ULONG      BitLen; //模数的实际位长度，取值为：256
    BYTE       XCoordinate[SM2_MAX_XCOORDINATE_BITS_LEN/8];
```

```
    BYTE        YCoordinate[SM2_MAX_YCOORDINATE_BITS_LEN/8];
}SM2PUBLICKEYBLOB, *PSM2PUBLICKEYBLOB;
```

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），且均为 32 个 byte，因此 XCoordinate、YCoordinate 的后 32byte 均补 0。

SM2 公钥数据例子（绿色部分为变量 XCoordinate 及 YCoordinate 的值）：

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 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

5.3 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。

① BLOBHEADER 结构取值如下：

```
typedef struct _PUBLICKEYSTRUC {
  BYTE   bType;    //取值为：PRIVATEKEYBLOB (0x7)
  BYTE   bVersion; //取值为：CUR_BLOB_VERSION (0x2)
  WORD   reserved; //取值为：0x1—代表 SM2 私钥是加密的格式
  ALG_ID aiKeyAlg; //取值为：CALG_SM2_KEYX
} BLOBHEADER, PUBLICKEYSTRUC;
```

② SM2PRIVATEKEYBLOB 数据结构定义：

```
typedef struct _SM2PRIVATEKEYBLOB {
    ULONG AlgID;                        //取值为：CALG_SM2_SIGN 或 CALG_SM2_KEYX
    ULONG EncryptedPrivateKeyBitLen; //加密 SM2 私钥 EncryptedPrivateKey 的实际位(bit)长度
    BYTE  *EncryptedPrivateKey;     //加密的 SM2 密钥对（公私钥）数据
}SM2PRIVATEKEYBLOB, *PSM2PRIVATEKEYBLOB;
```

注：1、参数 BitLen 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。