

CFCA

中金金融认证中心标准

30002.01—2012

RSA 数字证书申请及应用 CSP 接口调用规范

Interface specification of CSP

for RSA 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. RSA 数字证书申请调用 CSP 接口规范 2

 4.1 RSA 数字证书申请流程 2

 4.2 CSP 接口描述..... 2

5. RSA 数字证书导入调用 CSP 接口规范 4

 5.1 RSA 签名证书导入流程 4

 5.2 RSA 加密证书导入流程 5

6. RSA 私钥结构定义 10

 6.1 RSA 加密证书导入私钥密文格式..... 10

RSA 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 RSA 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。

PKCS#1 RSA Cryptography Standard

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。

对称密码算法

加密和解密使用相同密钥的密码算法。

对称密钥

用于对称密码算法的密钥。

DES

Data Encryption Standard，是一种使用密钥加密的块密码。

3DES

Triple DES，三重数据加密算法块密码的通称。相当于对每个数据块应用 3 次 DES 加密算法。

ECB

Electronic Code Book Operation Mode，分组密码算法的一种工作模式，其特征是将明文分组直接作为算法的输入，对应的输出作为密文分组。

4. RSA 数字证书申请调用 CSP 接口规范

4.1 RSA 数字证书申请流程

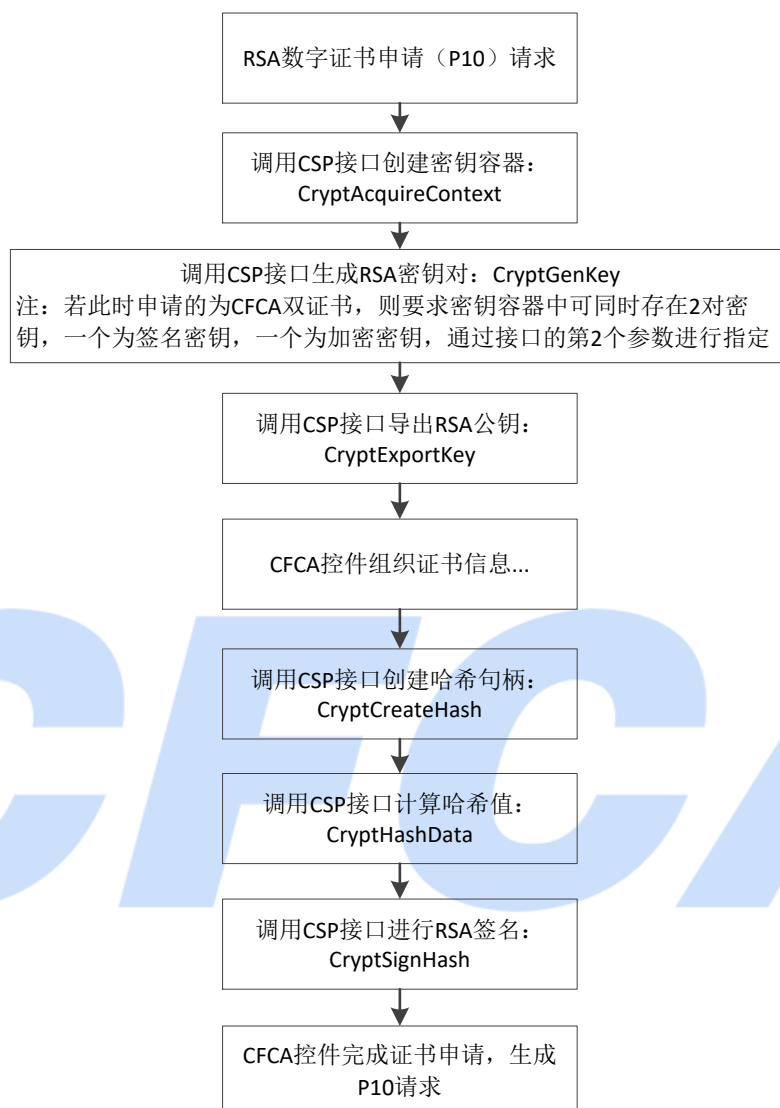


图 1 RSA 数字证书申请流程

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: PROV_RSA_FULL
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 RSA 密钥对。

特殊参数取值说明： **Algid**: AT_SIGNATUR 表示签名密钥
 AT_KEYEXCHANGE 表示加密密钥

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 RSA 公钥。

特殊参数取值说明： **dwBlobType**: PUBLICKEYBLOB
pbData: 公钥数据

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： 创建哈希句柄。

特殊参数取值说明： **Algid**: 哈希算法

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：对哈希值进行 RSA 签名。

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

5. RSA 数字证书导入调用 CSP 接口规范

5.1 RSA 签名证书导入流程

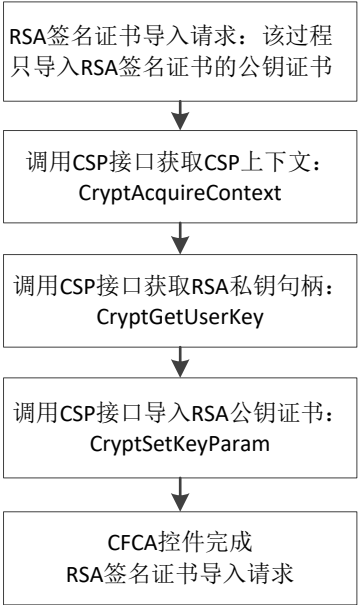


图 2 RSA 签名证书导入流程

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: PROV_RSA_FULL
dwFlags: CRYPT_VERIFYCONTEXT

5.1.1.2 CryptGetUserKey

```

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

```

描述： 获得私钥句柄。

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 RSA 公钥证书。

特殊参数取值说明： **hKey**: RSA 私钥句柄
dwParam: KP_CERTIFICATE

5.2 RSA 加密证书导入流程

根据密钥长度不同，对应的加密证书导入 CSP 方式也不同：

- 1、安装 RSA1024 位加密证书时，RSA 私钥以明文方式导入 CSP。
- 2、安装 RSA 2048/4096 位加密证书时，RSA 私钥以密文方式导入 CSP。

5.2.1 RSA 1024 位加密证书导入流程

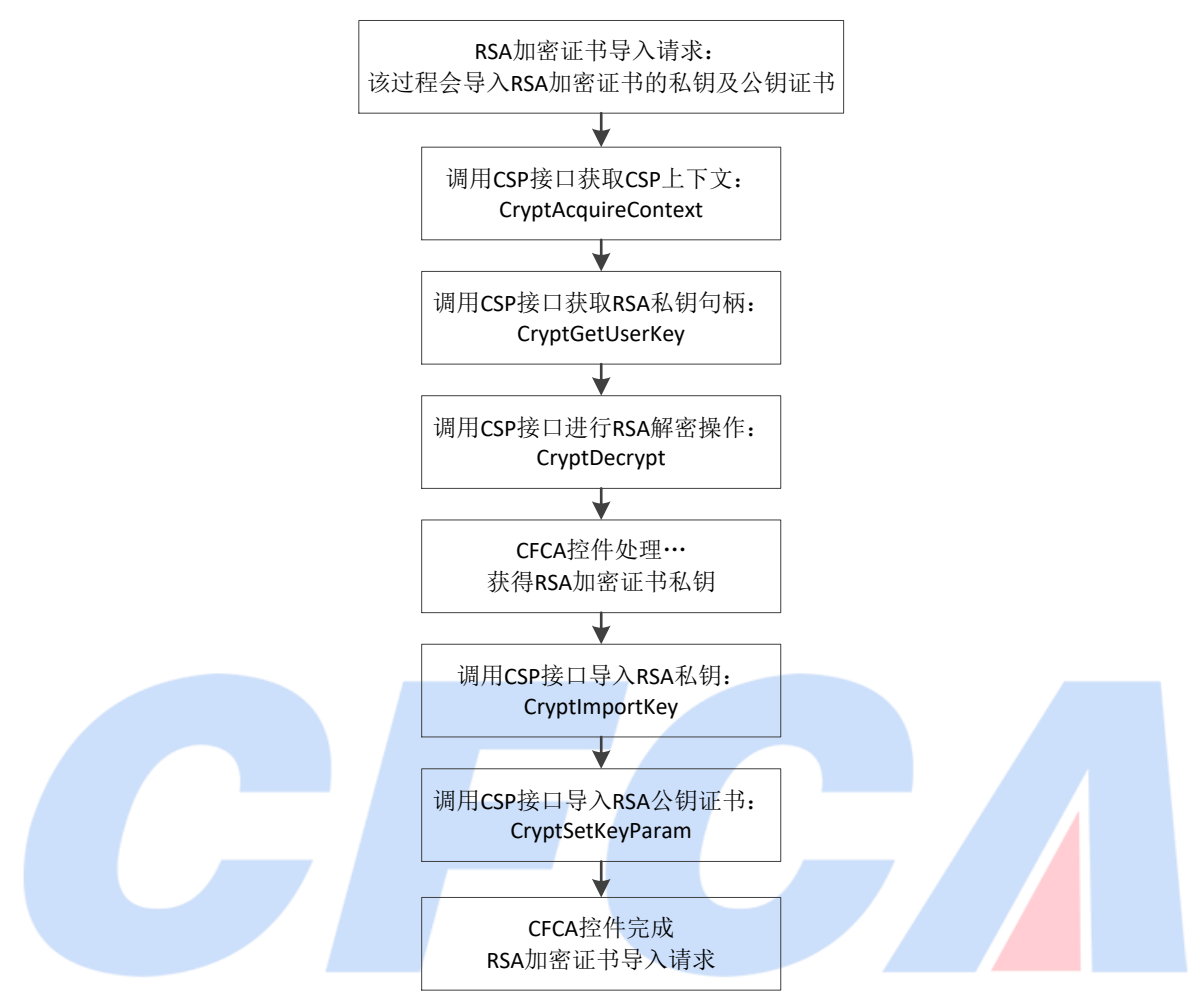


图 3 RSA 1024 位加密证书导入流程

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： PROV_RSA_FULL

dwFlags： CRYPT_VERIFYCONTEXT

5.2.1.2 CryptGetUserKey

```

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

```

描述： 获得 RSA 私钥句柄。

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

5.2.1.3 CryptDecrypt

```

BOOL WINAPI CryptDecrypt( __in   HCRYPTKEY    hKey,
                          __in   HCRYPTHASH  hHash,
                          __in   BOOL        Final,
                          __in   DWORD       dwFlags,
                          __inout BYTE       *pbData,
                          __inout DWORD      *pdwDataLen)

```

描述： RSA 解密。

特殊参数取值说明： hKey: RSA 私钥句柄
dwFlags: 0

5.2.1.4 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 RSA 私钥（以明文方式）。

特殊参数取值说明： pbData: RSA 私钥数据

备注：

RSA 私钥数据结构为微软标准的 Private key BLOBs。可以参考：

[http://msdn.microsoft.com/en-us/library/windows/desktop/aa375601\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa375601(v=vs.85).aspx)

5.2.1.5 CryptSetKeyParam

```

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

```

描述：导入 RSA 公钥证书。

特殊参数取值说明：hKey: RSA 私钥句柄

dwParam: KP_CERTIFICATE

5.2.2 RSA2048/4096 位加密证书导入流程

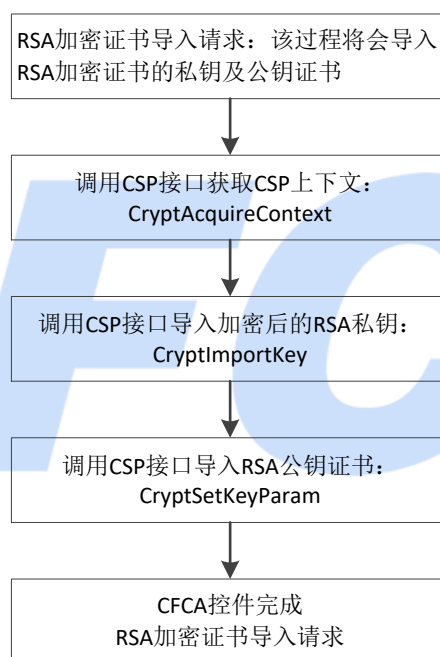


图 4 RSA2048/4096 位加密证书导入流程

5.2.2.1 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: PROV_RSA_FULL
dwFlags: CRYPT_VERIFYCONTEXT

5.2.2.2 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 RSA 私钥（以密文形式导入）。

特殊参数取值说明： **pbData**: 加密的 RSA 私钥数据，密文的数据结构定义详见章节 6
hPubKey: 此参数为 NULL（导入的公钥存在于 pbData 参数中）

5.2.2.3 CryptSetKeyParam

```

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

```

描述： 导入 RSA 公钥证书。

特殊参数取值说明： **hKey**: RSA 私钥句柄
dwParam: KP_CERTIFICATE

6. RSA 私钥结构定义

6.1 RSA 加密证书导入私钥密文格式

加密后的 RSA 私钥包含以下 2 部分：

BLOBHEADER;
RSAPRIVATEKEYBLOB

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

BLOBHEADER 结构取值如下：

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

其中：

bType 取值为：PRIVATEKEYBLOB (0x7)

bVersion 取值为：CUR_BLOB_VERSION (0x2)

reserved 取值为：0x1—代表私钥是加密的格式(RSA2048、4096 使用加密方式)

aiKeyAlg 取值为：CALG_RSA_KEYX

RSAPRIVATEKEYBLOB 结构取值如下：

```
typedef struct _RSAPRIVATEKEYBLOB{
    ULONG  AlgID;
    ULONG  BitLen;
    ULONG  EVPPrivateKeyBitLen;
    BYTE   *EVPPrivateKey;
}RSAPRIVATEKEYBLOB, *PRRSAPRIVATEKEYBLOB;
```

其中：

AlgID 取值为：CALG_RSA_KEYX

BitLen 取值为：RSA 加密证书私钥的实际位长度

EVPPrivateKeyBitLen 取值为：EVPPrivateKey 数据的实际位长度

EVPPrivateKey 取值为：加密私钥或明文私钥数据，加密私钥数据格式见 EVPPrivateKey。

EVPPrivateKey 为自定义的 ASN.1 格式（DER 编码）如下：

```
EVPPrivateKey ::= SEQUENCE {  
    Version          INTEGER,  
    AsymAlgID        OBJECT IDENTIFIER,  
    SymAlgID         OBJECT IDENTIFIER,  
    EncryptedSymKey  OCTET STRING,  
    EncryptedPrivateKey OCTET STRING  
}
```

其中：

Version：版本号，在本文档中，取值为 0x01。

AsymAlgID：非对称加密算法标识符，取值为：1.2.840.113549.1.1.1。

SymAlgID：对称加密算法标识符，本文档中为 3DES ECB，取值为：1.3.6.1.4.1.4929.1.7。

EncryptedSymKey：加密后的对称密钥，其格式为 RSA PKCS#1 加密结果。

EncryptedPrivateKey：用对称密钥加密过的私钥。

