数字证书应用工具包接口标准规范

**目 录**

[1. 项目范围 1](#_Toc444007011)

[1.1 项目描述 1](#_Toc444007012)

[1.2 项目背景 1](#_Toc444007013)

[1.3 项目目标 1](#_Toc444007014)

[2. 功能需求 1](#_Toc444007015)

[2.1语言显示 1](#_Toc444007016)

[2.2运行操作系统需求 1](#_Toc444007017)

[2.3消息的签名与验签 2](#_Toc444007018)

[2.3.1 SelectCertificate 2](#_Toc444007019)

[2.3.2 GetSignCertInfo 2](#_Toc444007020)

[2.3.3 SignMsgPKCS7 3](#_Toc444007021)

[2.3.4 VerifyMsgSignaturePKCS7Attached 3](#_Toc444007022)

[2.4文件的签名与验签 4](#_Toc444007023)

[2.4.1 SignFilePKCS7Detached 4](#_Toc444007024)

[2.4.2 VerifyFileSignaturePKCS7Detached 4](#_Toc444007025)

[2.5消息的加密与解密 5](#_Toc444007026)

[2.5.1 SelectEncryptCertificate 5](#_Toc444007027)

[2.5.2 SelectEncryptCertificate\_ByCert 5](#_Toc444007028)

[2.5.3 SelectEncryptCertificate\_BySoftCert 6](#_Toc444007029)

[2.5.4 GetEncrypCertInfo 6](#_Toc444007030)

[2.5.5 EncryptMsgCMSEnvelopeEx 7](#_Toc444007031)

[2.5.6 DecryptMsgCMSEnvelopeEx 7](#_Toc444007032)

[2.6文件的加密与解密 8](#_Toc444007033)

[2.6.1 EncryptFileCMSEnvelopeEx 8](#_Toc444007034)

[2.6.2 DecryptFileCMSEnvelopeEx 8](#_Toc444007035)

[2.7其他 9](#_Toc444007036)

[2.7.1 GetLastErrorDesc 9](#_Toc444007037)

[2.8安装程序 9](#_Toc444007038)

# 1. 项目范围

## 1.1 项目描述

该项目的主要内容为开发支持SM2、RSA签名、验签的证书工具包程序。

## 1.2 项目背景

中国金融认证中心对外演示的SM2、RSA签名、验签证书工具包程序。

## 1.3 项目目标

保证在所列出的操作系统平台（2.1）下的正常运行和技术支持。

# 2. 功能需求

## 2.1语言显示

页面语言环境支持：美国英文、简体中文。

## 2.2运行操作系统需求

* 32位操作系统

Windows XP、Windows Vista、Windows 7、Windows 8、WinServer2003、WinServer2008

* 64位操作系统

Windows Vista、Windows 7、Windows 8、WinServer2003、WinServer2008

* IE浏览器

IE6、IE7、IE8、IE9、IE10、IE11

* 非IE浏览器

Chrome 12.0-40.0、Firefox 4.0-Firefox35.0.1、Safari 5.0-5.34、Opera 11.0-27.0

## 2.3消息的签名与验签

### 2.3.1 SelectCertificate

HRESULT SelectCertificate(BSTR bstrSubjectDNFilter,BSTR bstrIssuerDNFilter, BSTR bstrSerialNumFilter , VARIANT\_BOOL\* pbSuccess)

**描述:**

通过传入的字符串作为DN的筛选条件，选择出符合DN条件的带私钥的SM2/RSA签名证书。如果筛选字符串为空，则对相应条件不进行筛选。

若为RSA证书，仅选择已注册的证书；

若为SM2证书，仅选择未注册的证书。

**参数:**

BSTR bstrSubjectDNFilter: [IN]目标证书主题DN中所包含的字符串，作为该筛选条件选出证书。

BSTR bstrIssuerDNFilter: [IN]目标证书颁发者DN中所包含的字符串，作为该筛选条件选出证书。

BSTR bstrSerialNumFilter: [IN]目标证书的序列号，作为该筛选条件选出证书。

VARIANT\_BOOL\* pbSuccess: [OUT，RETVAL] 成功返回VARIANT\_TRUE，否则返回VARIANT\_FALSE。

### 2.3.2 GetSignCertInfo

HRESULT GetSignCertInfo（BSTR bstrInfoType,BSTR\* pbstrInfoContent）

**描述:**

根据传入的标识，获得已选定证书（通过SelectCertificate选定的证书）的相关信息。

**参数:**

BSTR bstrInfoType: [IN]要获取的信息类型标识（不区分大小写）。

“SubjectDN”: 证书主题DN；

“SubjectCN”: 证书主题CN；

“SerialNumber”: 证书序列号；

“CSPName”: 证书对应的CSP名称；

“CertType”： 证书类型；SM2或RSA。

“IssuerDN”： 颁发者DN；

“CertTimeFrom”： 证书有效开始日期；

“CertTimeOut”： 证书有效截止日期；

“CertContent”： 公钥证书的Base64编码。

BSTR\* pbstrInfoContent: [OUT，RETVAL] 成功返回获取到的信息，失败返回空。

### 2.3.3 SignMsgPKCS7

HRESULT SignMsgPKCS7（BSTR bstrSourceData, BSTR bstrHashAlg,

VARIANT\_BOOL bWithSourceData, BSTR\* pbstrSignature）

**描述:**

对字符串进行SM2/RSA签名，返回Base64编码的PKCS#7签名结果。

**参数:**

BSTR bstrSourceData: [IN] 待签名的字符串，签名之前控件会将其转换为UTF-8编码。

BSTR bstrHashAlg:[IN] 使用RSA签名的算法。传入“SHA-1”、“SHA-256”，不区分大小写。

VARIANT\_BOOL bWithSourceData: [IN] 签名结果是否带原文。

VARIANT\_TRUE: 带原文；VARIANT\_FALSE: 不带原文。

BSTR\* pbstrSignature: [OUT，RETVAL] Base64编码的PKCS#7签名结果。

### 2.3.4 VerifyMsgSignaturePKCS7Attached

HRESULT VerifyMsgSignaturePKCS7Attached（BSTR bstrSignature, BSTR bstrSignatureType,VARIANT\_BOOL\* pbSuccess）

**描述:**

对SM2/RSA 签名结果进行PKCS#7带原文验签。

**参数:**

BSTR bstrSignature: [IN] Base64编码的PKCS#7带原文签名结果。

BSTR bstrSignatureType:[IN] 签名类型。SM2、RSA算法。

VARIANT\_BOOL\* pbSuccess: [OUT，RETVAL] 验签结果，VARIANT\_TRUE: 成功，VARIANT\_FALSE: 失败。

## 2.4文件的签名与验签

.com、.exe、.bat、.cmd、.vbs、.vbe、.js、.jse、.wsf、.wsh、.msc、.dll格式文件均不可进行签名及加密操作。

### 2.4.1 SignFilePKCS7Detached

HRESULT SignFilePKCS7Detached(BSTR bstrSourceFile, BSTR bstrHashAlg, BSTR\* pbstrSignature)

**描述:**

使用SelectCertificate选中的SM2/RSA证书对文件进行PKCS#7不带原文签名。

**参数:**

BSTR bstrSourceFile: [IN] 待签名的文件路径。

BSTR bstrHashAlg:[IN] 使用RSA签名的算法。传入“SHA-1”、“SHA-256”，不区分大小写。

BSTR\* pbstrSignature: [OUT，RETVAL] Base64编码的PKCS#7签名值。

### 2.4.2 VerifyFileSignaturePKCS7Detached

HRESULT VerifyFileSignaturePKCS7Detached（BSTR bstrSignature, BSTR bstrSigngnatureType, BSTR bstrSourceFile, VARIANT\_BOOL\* pbSuccess）

**描述:**

对SM2/PFX文件签名结果进行PKCS#7不带原文验签。

**参数:**

BSTR bstrSignature：[IN] Base64编码的PKCS#7签名结果。

BSTR bstrSigngnatureType:[IN] 签名类型。SM2、RSA算法。

BSTR bstrSourceFile：[IN] 原文件路径。

VARIANT\_BOOL\* pbSuccess：[OUT，RETVAL] 验签结果，VARIANT\_TRUE：成功，VARIANT\_FALSE：失败。

## 2.5消息的加密与解密

### 2.5.1 SelectEncryptCertificate

HRESULT SelectEncryptCertificate（BSTR bstrSubjectDNFilter, BSTR bstrIssueDNFilter, BSTR bstrSerialNumFilter, BSTR\* pbstrSubjectDN）

**描述:**

按照过滤条件(Subject DN / IssuerDN/ SerialNumber)选择一个用于加密的SM2/RSA公钥证书。

此函数用于基于USBKey的加密。

若为RSA证书，仅选择已注册的证书；

若为SM2证书，仅选择未注册的证书。

**参数:**

BSTR bstrSubjectDNFilter: [IN]目标证书中主题DN中所包含的字符串，作为该筛选条件选出证书。

BSTR bstrIssueDNFilter: [IN]目标证书中颁发者DN中所包含的字符串，作为该筛选条件选出证书。

BSTR bstrSerialNumFilter:[IN]目标证书中证书序列号中所包含的字符串，作为该筛选条件选出证书。

BSTR \* pbstrSubjectDN: [OUT，RETVAL] 返回被选出SM2/RSA公钥证书的主题DN。

### 2.5.2 SelectEncryptCertificate\_ByCert

HRESULT SelectEncryptCertificate\_ByCert（BSTR bstrBase64CertContent , BSTR bstrCertType, BSTR\* pbstrSubjectDN）

使用传入的SM2/RSA公钥证书，选择一个用于加密的公钥证书。

**参数:**

BSTR bstrBase64CertContent: [IN] ] SM2/RSA公钥证书，该证书需采用Base64编码。

BSTR bstrCertType:[IN]用于加密公钥证书类型。SM2、RSA。

BSTR \* pbstrSubjectDN: [OUT，RETVAL] 返回被选出SM2/RSA公钥证书的主题DN。

### 2.5.3 SelectEncryptCertificate\_BySoftCert

HRESULT SelectEncryptCertificate\_BySoftCert（BSTR bstrSoftCertFileName, BSTR bstrCertType, BSTR\* pbstrSubjectDN）

使用传入的SM2/RSA公钥证书，选择一个用于加密的公钥证书。

**参数:**

BSTR bstrSoftCertFileName: [IN] SM2/RSA公钥证书(.cer)路径，该证书需为去掉头尾的Base64编码内容。

BSTR bstrCertType:[IN]用于加密公钥证书类型。SM2、RSA。

BSTR \* pbstrSubjectDN: [OUT，RETVAL] 返回被选出SM2/RSA公钥证书的主题DN。

### 2.5.4 GetEncrypCertInfo

HRESULT GetEncrypCertInfo（BSTR bstrInfoType, BSTR\* pbstrInfoContent）

**描述:**

根据传入的标识，获得已选定证书（选定的证书）的相关信息。

**参数:**

BSTR bstrInfoType: [IN]要获取的信息类型标识（不区分大小写）。

“SubjectDN”: 证书主题DN；

“SubjectCN”: 证书主题CN；

“SerialNumber”: 证书序列号；

“CSPName”: 证书对应的CSP名称；

“CertType”： 证书类型；SM2或RSA。

“IssuerDN”： 颁发者DN；

“CertTimeFrom”： 证书有效开始日期；

“CertTimeOut”： 证书有效截止日期；

“CertContent”： 公钥证书的Base64编码。

BSTR\* pbstrInfoContent: [OUT，RETVAL] 成功返回获取到的信息，失败返回空。

### 2.5.5 EncryptMsgCMSEnvelopeEx

HRESULT EncryptMsgCMSEnvelopeEx（BSTR bstrMessage, BSTR bstrEncryptAlg, BSTR\* pbstrEnvelope）

**描述:**

使用SelectEncryptCertificate选择的SM2/RSA公钥证书将消息加密成CMS数字信封。

对字符串进行SM2/RSA加密，返回Base64编码的SM2/RSA加密结果；其中RSA签名可以使用3DES或RC4算法加密，SM2签名使用SM4算法加密。

此函数用于基于USBKey的加密。

**参数:**

BSTR bstrMessage: [IN] 待加密的字符串，(加密之前内部会将其转换为UTF-8编码）。

BSTR bstrEncryptAlg:[IN] 加密算法。传入“RC4”或“3DES”，不区分大小写。此参数只对RSA证书起作用，SM2证书默认使用SM4算法加密。

BSTR \* pbstrEnvelope: [OUT，RETVAL] 加密后的数字信封，Base64编码格式字符串。

### 2.5.6 DecryptMsgCMSEnvelopeEx

HRESULT DecryptMsgCMSEnvelopeEx（BSTR bstrEnvelope,BSTR bstrEnvelopeType,BSTR\* pbstrMessage）

**描述:**

使用SelectEncryptCertificate函数选择的SM2/RSA证书解密CMS数字信封。

**参数:**

BSTR bstrEnvelope: [IN] 用于解密的数字信封，Base64编码格式字符串。

BSTR bstrEnvelopeType:[IN]用于解密的证书类型。SM2、RSA证书。

BSTR\* pbstrMessage: [OUT，RETVAL]解密出的明文字符串。

## 2.6文件的加密与解密

.com、.exe、.bat、.cmd、.vbs、.vbe、.js、.jse、.wsf、.wsh、.msc、.dll格式文件均不可进行签名及加密操作。

### 2.6.1 EncryptFileCMSEnvelopeEx

HRESULT EncryptFileCMSEnvelopeEx（BSTR bstrSourceFile, BSTR bstrEncryptAlg, BSTR bstrEncryptedFile, VARIANT\_BOOL\* pbSuccess）

**描述:**

使用SelectEncryptCertificate选择的SM2/PFX公钥证书将文件加密成CMS数字信封。

此函数用于基于USBKey的加密。

**参数:**

BSTR bstrSourceFile: [IN] 待加密的文件。

BSTR bstrEncryptAlg: [IN] 加密算法。传入“RC4”或“3DES”，不区分大小写。此参数只对RSA证书起作用，SM2证书默认使用SM4算法加密。

BSTR bstrEncryptedFile: [IN] 加密后的文件输出路径(CMS数字信封)。

VARIANT\_BOOL\* pbSuccess: [OUT，RETVAL]加密是否成功，VARIANT\_TRUE: 加密成功， VARIANT\_FALSE: 加密失败。

### 2.6.2 DecryptFileCMSEnvelopeEx

HRESULT DecryptFileCMSEnvelopeEx（BSTR bstrEncryptedFile，BSTR bstrEnvelopeType，BSTR bstrPlainTextFile, VARIANT\_BOOL\* pbSuccess）

**描述:**

使用SelectEncryptCertificate函数选择的SM2/PFX证书解密CMS数字信封文件。

**参数:**

BSTR bstrEncryptedFile: [IN] 用于解密的的数字信封文件。

BSTR bstrEnvelopeType:[IN] 用于解密的证书类型。SM2、RSA证书。

BSTR bstrPlainTextFile: [IN] 解密出的明文文件。

VARIANT\_BOOL\* pbSuccess: [OUT，RETVAL]解密是否成功，VARIANT\_TRUE: 解密成功，VARIANT\_FALSE: 解密失败。

## 2.7其他

### 2.7.1 GetLastErrorDesc

HRESULT GetLastErrorDesc（BSTR\* pbstrErrorDesc）

**描述:**

获得最近一次调用接口导致发生错误的描述信息。此函数会根据不同的操作系统语言（简体中文/美国英语）来本地化错误描述。

**参数:**

BSTR\* pbstrErrorDesc: [OUT，RETVAL]错误描述信息。

## 2.8安装程序

1、提供cab包和exe安装程序。

CryptoKit.SDDR.x86.cab

CryptoKit.SDDR.x86.exe

CryptoKit.SDDR.x64.cab

CryptoKit.SDDR.x64.exe

npCryptoKit.SDDR.x86.exe