PHP版服务器端工具包（Windows版）

软件需求说明书

（版本：3.0）

中国金融认证中心

2017年8月3日

版权声明：本文档的版权属于中国金融认证中心，任何人或组织未经许可，

不得擅自修改、拷贝或以其它方式使用本文档中的内容

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 | 需求初稿 | 2017/08/03 | 胡军华 | 贺 磊  张 哲 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

注：对该文件内容增加、删除或修改须填写此修订记录，详细记载变更信息，以保证其可追溯性。

目 录

[1 项目范围 1](#_Toc492368470)

[1.1 项目描述 1](#_Toc492368471)

[1.2 项目背景 1](#_Toc492368472)

[1.3 项目目标 1](#_Toc492368473)

[2 版本需求 1](#_Toc492368474)

[2.1 操作系统版本 1](#_Toc492368475)

[2.2 PHP版本 1](#_Toc492368476)

[3 接口列表 2](#_Toc492368477)

[3.1 SignData\_PKCS1 2](#_Toc492368478)

[3.2 SignData\_PKCS7Detached 3](#_Toc492368479)

[3.3 SignData\_PKCS7Attached 4](#_Toc492368480)

[3.4 VerifyDataSignature\_PKCS1 5](#_Toc492368481)

[3.5 VerifyDataSignature\_PKCS7Detached 6](#_Toc492368482)

[3.6 VerifyDataSignature\_PKCS7Attached 7](#_Toc492368483)

[3.7 GetSignSourceData 7](#_Toc492368484)

[3.8 SignFile\_PKCS7Detached 8](#_Toc492368485)

[3.9 VerifyFileSignature\_PKCS7Detached 9](#_Toc492368486)

[3.10 EncryptDataToCMSEnvelope 10](#_Toc492368487)

[3.11 DecryptDataFromCMSEnvelope 11](#_Toc492368488)

[3.12 SymEncryptFile 11](#_Toc492368489)

[3.13 SymDecryptFile 12](#_Toc492368490)

[3.14 VerifyCertificate 13](#_Toc492368491)

[3.15 GetCertificateInfo 14](#_Toc492368492)

[3.16 GetPublicCertFromPFX 15](#_Toc492368493)

[3.17 CalculateDataHash 16](#_Toc492368494)

[3.18 CalculateFileHash 17](#_Toc492368495)

[3.19 GetLastErrorDesc 17](#_Toc492368496)

[4 提供程序 18](#_Toc492368497)

# 项目范围

## 项目描述

该项目的主要内容为开发Windows下PHP调用的服务器端工具包。

## 项目背景

Windows下PHP可以调用COM组件。为使得PHP程序能够完成证书相关业务操作，所以实现COM版服务器端工具包，供应用程序调用。

## 项目目标

保证在系统需求中所列出的操作系统及PHP下的正常运行。

# 版本需求

## 操作系统版本

支持以下操作系统:

WinServer2008 64bit、

WinServer2012 64bit。

## PHP版本

支持以下版本的PHP：

PHP5.6系列；

PHP7.0系列；

PHP7.1系列。

# 接口列表

以ATL COM组件形式实现。

## SignData\_PKCS1

HRESULT SignData\_PKCS1(BSTR bstrSignAlg,

BSTR bstrSourceData,

BSTR bstrPfxFilePath,

BSTR bstrPfxPassWord,

BSTR bstrHashAlg,

BSTR\* pbstrBase64PKCS1Signature)

**描述:**

按指定的算法类型（SM2/RSA），使用软证书对数据进行PKCS#1签名。

**参数：**

BSTR bstrSignAlg:[IN]算法类型，传入“SM2”或“RSA”，不区分大小写；

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 bstrPfxFilePath:[IN]用于签名的软证书文件的路径，路径中不许有中文；

BSTR bstrPfxPassWord:[IN]用于签名的软证书文件的密码；

BSTR bstrHashAlg:[IN] 哈希算法，传入“SHA-1”或“SHA-256”，不区分大小写。此参数仅在RSA签名时才起作用；SM2签名默认使用SM3哈希算法，忽略此参数;

BSTR\* pbstrBase64PKCS1Signature:[OUT, RETVAL] Base64编码的PKCS#1签名结果；

## SignData\_PKCS7Detached

HRESULT SignData\_PKCS7Detached(BSTR bstrSignAlg,

BSTR bstrSourceData,

BSTR bstrPfxFilePath,

BSTR bstrPfxPassWord,

BSTR bstrHashAlg,

BSTR\* pbstrBase64PKCS7DetachedSignature)

**描述:**

按指定的算法类型（SM2/RSA），使用软证书对数据进行PKCS#7不带原文签名。

**参数：**

BSTR bstrSignAlg:[IN]算法类型，传入“SM2”或“RSA”，不区分大小写；

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 bstrPfxFilePath:[IN]用于签名的软证书文件的路径，路径中不许有中文；

BSTR bstrPfxPassWord:[IN]用于签名的软证书文件的密码；

BSTR bstrHashAlg:[IN] 哈希算法，传入“SHA-1”或“SHA-256”，不区分大小写。此参数仅在RSA签名时才起作用；SM2签名默认使用SM3哈希算法，忽略此参数;

BSTR\* pbstrBase64PKCS7DetachedSignature:[OUT, RETVAL] Base64编码的PKCS#7不带原文签名结果；

## SignData\_PKCS7Attached

HRESULT SignData\_PKCS7Attached(BSTR bstrSignAlg,

BSTR bstrSourceData,

BSTR bstrPfxFilePath,

BSTR bstrPfxPassWord,

BSTR bstrHashAlg,

BSTR\* pbstrBase64PKCS7AttachedSignature)

**描述:**

按指定的算法类型（SM2/RSA），使用软证书对数据进行PKCS#7带原文签名。

**参数：**

BSTR bstrSignAlg:[IN]算法类型，传入“SM2”或“RSA”，不区分大小写；

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 bstrPfxFilePath:[IN]用于签名的软证书文件的路径，路径中不许有中文；

BSTR bstrPfxPassWord:[IN]用于签名的软证书文件的密码；

BSTR bstrHashAlg:[IN] 哈希算法，传入“SHA-1”或“SHA-256”，不区分大小写。此参数仅在RSA签名时才起作用；SM2签名默认使用SM3哈希算法，忽略此参数;

BSTR\* pbstrBase64PKCS7AttachedSignature:[OUT, RETVAL] Base64编码的PKCS#7不带原文签名结果；

## VerifyDataSignature\_PKCS1

HRESULT VerifyDataSignature\_PKCS1(BSTR bstrSignAlg,

BSTR bstrSourceData,

BSTR bstrBase64CertContent,

BSTR bstrHashAlg,

BSTR bstrBase64PKCS1Signature,

VARIANT\_BOOL\* pbSuccess)

**描述:**

按指定的算法类型（SM2/RSA），验证PKCS#1签名。

**参数：**

BSTR bstrSignAlg:[IN]算法类型，传入“SM2”或“RSA”，不区分大小写；

BSTR bstrSourceData:[IN] 被签名的字符串，验签之前控件会将其转换为UTF-8编码；

BSTR bstrBase64CertContent:[IN] 用于验签的公钥证书内容（Base64编码，不带证书头、尾）；

BSTR bstrHashAlg:[IN] 哈希算法，传入“SHA-1”或“SHA-256”，不区分大小写。此参数仅在RSA签名时才起作用；SM2签名默认使用SM3哈希算法，忽略此参数;

BSTR bstrBase64PKCS1Signature:[IN] Base64编码的PKCS#1签名结果；

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

## VerifyDataSignature\_PKCS7Detached

HRESULT VerifyDataSignature\_PKCS7Detached (BSTR bstrSignAlg,

BSTR bstrSourceData,

BSTR bstrBase64PKCS7DetachedSignature,

BSTR\* pbstrBase64SignCertContent)

**描述:**

按指定的算法类型（SM2/RSA），验证PKCS#7不带原文签名。

**参数：**

BSTR bstrSignAlg:[IN]算法类型，传入“SM2”或“RSA”，不区分大小写；

BSTR bstrSourceData:[IN] 被签名的字符串，验签之前控件会将其转换为UTF-8编码；

BSTR bstrBase64PKCS7DetachedSignature:[IN] Base64编码的PKCS#7不带原文签名结果；

BSTR\* pbstrBase64SignCertContent:[OUT, RETVAL] PKCS#7中的签名证书（Base64编码）;

## VerifyDataSignature\_PKCS7Attached

HRESULT VerifyDataSignature\_PKCS7Attached (BSTR bstrSignAlg,

BSTR bstrBase64PKCS7AttachedSignature,

BSTR\* pbstrBase64SignCertContent)

**描述:**

按指定的算法类型（SM2/RSA），验证PKCS#7带原文签名。

**参数：**

BSTR bstrSignAlg:[IN]算法类型，传入“SM2”或“RSA”，不区分大小写；

BSTR bstrBase64PKCS7AttachedSignature:[IN] Base64编码的PKCS#7带原文签名结果；

BSTR\* pbstrBase64SignCertContent:[OUT, RETVAL] PKCS#7中的签名证书（Base64编码）;

## GetSignSourceData

HRESULT GetSignSourceData (BSTR bstrBase64PKCS7AttachedSignature,

BSTR\* pbstrSourceData)

**描述**:

获取P7带原文签名结果中的签名原文。

**参数**：

BSTR bstrBase64PKCS7AttachedSignature:[IN] Base64编码的PKCS#7带原文签名结果；

BSTR\* pbstrSourceData:[OUT, RETVAL] PKCS#7中的签名原文;

## SignFile\_PKCS7Detached

HRESULT SignFile\_PKCS7Detached (BSTR bstrSignAlg,

BSTR bstrSourceFilePath,

BSTR bstrPfxFilePath,

BSTR bstrPfxPassword,

BSTR bstrHashAlg,

BSTR\* pbstrBase64PKCS7DetachedSignature)

**描述:**

按指定的算法类型（SM2/RSA），使用软证书对文件进行PKCS#7不带原文签名。

**参数：**

BSTR bstrSignAlg:[IN]算法类型，传入“SM2”或“RSA”，不区分大小写；

BSTR bstrSourceFilePath:[IN] 待签名的文件原文路径，路径中不许有中文；

BSTR bstrPfxFilePath:[IN]用于签名的软证书文件的路径，路径中不许有中文；

BSTR bstrPfxPassword:[IN]用于签名的软证书文件的密码；

BSTR bstrHashAlg:[IN] 哈希算法，传入“SHA-1”或“SHA-256”，不区分大小写。此参数仅在RSA签名时才起作用；SM2签名默认使用SM3哈希算法，忽略此参数;

BSTR pbstrBase64PKCS7DetachedSignature:[OUT, RETVAL] Base64编码的PKCS#7不带原文签名结果；

## VerifyFileSignature\_PKCS7Detached

HRESULT VerifyFileSignature\_PKCS7Detached(BSTR bstrSignAlg,

BSTR bstrSourceFilePath,

BSTR bstrBase64PKCS7DetachedSignature,

BSTR bstrBase64SignCertContent)

**描述:**

按指定的算法类型（SM2/RSA），验证文件PKCS#7不带原文签名。

**参数：**

BSTR bstrSignAlg:[IN]算法类型，传入“SM2”或“RSA”，不区分大小写；

BSTR bstrSourceFilePath:[IN] 待验签的文件原文路径，路径中不许有中文；

BSTR bstrBase64PKCS7DetachedSignature:[IN] Base64编码的PKCS#7不带原文签名结果；

BSTR bstrBase64SignCertContent:[OUT，RETVAL] 返回PKCS#7中的签名证书（Base64编码）;

## EncryptDataToCMSEnvelope

HRESULT EncryptDataToCMSEnvelope (BSTR bstrAlgorithm,

BSTR bstrPlainData,

BSTR bstrBase64EncryptCert,

BSTR bstrSymEncAlg,

BSTR\* pstrBase64CMSEnvelope)

**描述:**

按指定的算法类型（SM2/RSA），把数据加密成CMS格式的数字信封。

**参数：**

BSTR bstrAlgorithm:[IN]算法类型，传入“SM2”或“RSA”，不区分大小写；

BSTR bstrPlainData:[IN] 待加密的明文字符串，加密之前控件会将其转换为UTF-8编码；

BSTR bstrBase64EncryptCert:[IN] 用于加密的公钥证书内容（Base64编码，不带证书头、尾）；

BSTR bstrSymEncAlg:[IN] 对称加密算法，传入“RC4”或“3DES”，不区分大小写。此参数仅在加密RSA数字信封时才起作用；SM2类型的数字信封对称加密默认使用SM4，忽略此参数；

BSTR\* pstrBase64CMSEnvelope:[OUT, RETVAL] 加密后的Base64编码数字信封；

## DecryptDataFromCMSEnvelope

HRESULT DecryptDataFromCMSEnvelope (BSTR bstrAlgorithm,

BSTR bstrBase64CMSEnvelope,

BSTR bstrPfxFilePath,

BSTR bstrPfxPassWord,

BSTR\* pbstrPlainData)

**描述:**

按指定的算法类型（SM2/RSA），解密CMS格式的数字信封。

**参数：**

BSTR bstrAlgorithm:[IN]算法类型，传入“SM2”或“RSA”，不区分大小写；

BSTR bstrBase64CMSEnvelope:[IN] 待解密的Base64编码数字信封；

BSTR bstrPfxFilePath:[IN]用于解密的软证书文件的路径，路径中不许有中文；

BSTR bstrPfxPassWord:[IN]用于解密的软证书文件的密码；

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

## SymEncryptFile

HRESULT SymEncryptFile (BSTR bstrSymEncAlgorithm,

BSTR bstrPlainFilePath,

BSTR bstrEncryptFilePath,

BSTR\* pbstrSymKey)

**描述**：

使用指定的加密算法对文件进行对称加密，并输出随机产生的对称秘钥。

注意：待加密的明文文件大小不能超过1G!

**参数**：

BSTR bstrSymEncAlgorithm:[IN]对称加密算法，传入“3DES\_CBC”或“SM4\_CBC”，不区分大小写；

BSTR bstrPlainFilePath:[IN]待加密的明文文件路径，路径中不许有中文；

BSTR bstrEncryptFilePath:[IN]加密后生成的密文路径，路径中不许有中文；

BSTR\* pbstrSymKey:[OUT, RETVAL] 十六进制编码的对称密钥；使用3DES\_CBC对称加密算法时，十六进制编码的对称密钥前16个字符为IV，后48个字符为key；使用SM4\_CBC对称加密算法时，十六进制编码的对称密钥前32个字符为IV，后32个字符为key。

## SymDecryptFile

HRESULT SymDecryptFile (BSTR bstrSymEncAlgorithm,

BSTR bstrEncryptFilePath,

BSTR bstrSymKey,

BSTR bstrPlainFilePath,

VARIANT\_BOOL\* pbSuccess);

**描述**：

使用指定的算法对文件进行解密。

**参数**：

BSTR bstrSymEncAlgorithm:[IN]对称解密算法，传入“3DES\_CBC”或“SM4\_CBC”，不区分大小写；

BSTR bstrEncryptFilePath:[IN]待解密的密文路径，路径中不许有中文；

BSTR bstrSymKey:[IN] 十六进制编码的对称密钥；使用3DES\_CBC对称加密算法时，十六进制编码的对称密钥前16个字符为IV，后48个字符为key；使用SM4\_CBC对称加密算法时，十六进制编码的对称密钥前32个字符为IV，后32个字符为key。

BSTR bstrPlainFilePath:[IN]解密后生成的明文文件路径，路径中不许有中文；

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

## VerifyCertificate

HRESULT VerifyCertificate(BSTR bstrBase64CertContent,

INT nCertVerifyFlag,

BSTR bstrTrustedCACertFilePath,

BSTR bstrCRLFilePath,

VARIANT\_BOOL\* pbSuccess)

**描述:**

验证证书有效性。

**参数：**

BSTR bstrBase64CertContent:[IN] 待验证的公钥证书内容（Base64编码，不带证书头、尾）；

INT nCertVerifyFlag:[IN] 验证证书标识位。1:验证证书时间有效性；2:验证证书是否被吊销；4:验证证书链完整性。以上标识位可以组合使用，例如传入7就是全部都验证；

BSTR bstrTrustedCACertFilePath:[IN] 可信根证书或中级证书的文件路径，路径中不许有中文。如果有多个证书文件，需要把多个文件路径以“|”为分隔，组合成一个字符串传入，例如:“D:/RootCert.cer|D:/ IntermediateCert.cer”。如果nCertVerifyFlag不包含4，此参数可以传入NULL；

BSTR bstrCRLFilePath:[IN] 证书吊销列表CRL文件路径，路径中不许有中文。如果nCertVerifyFlag不包含2，此参数可以传入NULL；

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

## GetCertificateInfo

HRESULT GetCertificateInfo (BSTR bstrBase64CertContent,

BSTR bstrInfoType,

BSTR\* pbstrInfoContent)

**描述:**

根据传入的标识，获取证书的相关信息。

**参数：**

BSTR bstrBase64CertContent:[IN] 公钥证书内容（Base64编码，不带证书头、尾）；

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

“CertType”： 证书类型，返回“SM2”或“RSA”。

“SubjectDN”: 证书主题DN；

“SubjectCN”: 证书主题CN；

“IssuerDN”: 颁发者主题DN；

“SerialNumber”: 证书序列号；

“ValidFrom”: 有效起始日期；

“ValidTo”: 有效截止日期；

BSTR\* pbstrInfoContent:[OUT, RETVAL] 返回获取到的证书信息；

## GetPublicCertFromPFX

HRESULT GetPublicCertFromPFX (BSTR bstrAlgorithm,

BSTR bstrPfxFilePath,

BSTR bstrPfxPassWord,

BSTR\* pbstrBase64CertContent)

**描述:**

从指定的软证书文件中，获取公钥证书。

**参数：**

BSTR bstrAlgorithm:[IN] 算法标识，传入“SM2”或“RSA”，不区分大小写；

BSTR bstrPfxFilePath:[IN] 用于提取公钥证书的软证书文件路径，路径中不许有中文;

如果pszAlgorithm指定了SM2算法，此处传入Base64编码的“.SM2”文件；如果pszAlgorithm指定了RSA算法，此处传入DER编码的“.pfx”文件；

BSTR bstrPfxPassWord:[IN] 用于提取公钥证书的软证书文件的密码;

BSTR\* pbstrBase64CertContent:[OUT, RETVAL] 获取到的Base64编码公钥证书内容。

## CalculateDataHash

HRESULT CalculateDataHash (BSTR bstrSourceData,

BSTR bstrHashAlg,

BSTR\* pbstrHexHashData)

**描述:**

计算传入数据的哈希值，传出十六进制编码的哈希计算结果。计算SM3哈希时，不带Z值。

**参数：**

BSTR bstrSourceData:[IN]待计算哈希的字符串，计算哈希之前控件会将其转换为UTF-8编码；；

BSTR bstrHashAlg:[IN] 哈希算法，传入“MD5”、“SHA-1”、“SHA-256”、“SM3”，不区分大小写;

BSTR\* pbstrHexHashData:[OUT, RETVAL] 十六进制编码的哈希计算结果。

## CalculateFileHash

HRESULT CalculateFileHash (BSTR bstrSourceFilePath,

BSTR bstrHashAlg,

BSTR\* pbstrHexHashData)

**描述:**

计算传入文件的哈希值，传出十六进制编码的哈希计算结果。计算SM3哈希时，不带Z值。

**参数：**

BSTR bstrSourceFilePath:[IN]待计算哈希的文件路径，路径中不许有中文；

BSTR bstrHashAlg:[IN] 哈希算法，传入“MD5”、“SHA-1”、“SHA-256”、“SM3”，不区分大小写;

BSTR\* pbstrHexHashData:[OUT,RETVAL] 十六进制编码的哈希计算结果。

## 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

# 提供程序

提供DLL程序、PHP调用Demo、C#调用Demo。

DLL名称：CryptoKit.Standard.x86.dll

CryptoKit.Standard.x64.dll