

PHP 版服务器端工具包（Linux 版）

接口使用手册

（版本：3.0）

中国金融认证中心

2017 年 8 月 17 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 | 建立文档 | 2017/08/17 | 胡军华 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

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 文档描述..... | 1 |
| 2 版本需求..... | 1 |
| 2.1 操作系统版本..... | 1 |
| 2.2 PHP 版本 | 1 |
| 2.3 运行环境依赖..... | 1 |
| 3 接口列表..... | 2 |
| 3.1 cfca_initialize | 2 |
| 3.2 cfca_uninitialize..... | 2 |
| 3.3 cfca_signData_PKCS1..... | 3 |
| 3.4 cfca_signData_PKCS7Detached | 4 |
| 3.5 cfca_signData_PKCS7Attached | 5 |
| 3.6 cfca_verifyDataSignature_PKCS1..... | 6 |
| 3.7 cfca_verifyDataSignature_PKCS7Detached | 8 |
| 3.8 cfca_verifyDataSignature_PKCS7Attached | 8 |
| 3.9 cfca_signFile_PKCS7Detached | 9 |
| 3.10 cfca_verifyFileSignature_PKCS7Detached | 10 |
| 3.11 cfca_encryptDataToCMSEnvelope..... | 11 |
| 3.12 cfca_decryptDataFromCMSEnvelope | 12 |
| 3.13 cfca_symEncryptFile | 13 |
| 3.14 cfca_symDecryptFile..... | 14 |
| 3.15 cfca_verifyCertificate..... | 15 |
| 3.16 cfca_getCertificateInfo | 16 |
| 3.17 cfca_getPublicCertFromPFX | 17 |
| 3.18 cfca_calculateDataHash..... | 18 |
| 3.19 cfca_calculateFileHash | 19 |
| 4 提供程序..... | 20 |
| 5 Demo 使用方法 | 20 |

1 文档描述

该文档主要描述 Linux 版 PHP 服务器端工具包接口的定义以及使用，帮助使用者了解接口的调用方式。

2 版本需求

2.1 操作系统版本

支持以下操作系统:

CentOS 7.0 64bit

CentOS 7.1 64bit。

2.2 PHP 版本

PHP5.6 系列(NTS);

PHP7.0 系列(NTS);

PHP7.1 系列(NTS)。

2.3 运行环境依赖

扩展库在开发中用到了 C++11 的特性，其对运行时环境要求如下：
CXXABI 版本不低于 1.3.7（GCC4.8.0）；GLIBC 版本不低于 2.14。

CentOS7.0 和 7.1 自带环境已经满足要求。

3 接口列表

本工具包为 PHP 的扩展库，使用时需要 PHP 允许加载扩展库并将工具包添加到 PHP 要加载的扩展列表中。待 PHP 加载当前扩展工具包之后，工具包中的接口才能正常使用。

3.1 cfca_initialize

```
integer cfca_initialize(string strConfigFilePath);
```

描述：

扩展初始化。

调用本函数库中其它函数之前调用 cfca_initialize()。如果需要在多线程环境下调用此函数库中的函数，cfca_initialize()需要在开启多线程之前调用。

此函数只需要调用一次。

参数：

strConfigFilePath: [IN]配置文件路径，路径中不许有中文。

返回值：

0: 成功；

其它: 失败。

3.2 cfca_uninitialize

```
integer cfca_uninitialize();
```

描述:

调用本函数库中其它函数之后调用 `cfca_uninitialize()`。如果需要在多线程环境下调用此函数库中的函数，`cfca_uninitialize()`需要在多线程结束之后调用。

此函数只需要调用一次。

返回值:

0: 成功;

其它: 失败。

3.3 cfca_signData_PKCS1

```
integer cfca_signData_PKCS1(string strSignAlg,  
                             string strSourceData,  
                             string strPfxFilePath,  
                             string strPfxPassWord,  
                             string strHashAlg,  
                             string strBase64PKCS1Signature)
```

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:

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

`string strSourceData:[IN]`待签名的字符串，需使用 UTF8 格式编码，以保持与

其他系统兼容；

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

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

string strHashAlg:[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；

string strBase64PKCS1Signature:[OUT] Base64 编码的 PKCS#1 签名结果；

返回值：

0：成功；

其它：失败。

3.4 cfca_signData_PKCS7Detached

```
integer cfca_signData_PKCS7Detached(string strSignAlg,  
                                     string strSourceData,  
                                     string strPfxFilePath,  
                                     string strPfxPassWord,  
                                     string strHashAlg,  
                                     string strBase64PKCS7DetachedSignature)
```

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:

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

string strSourceData:[IN]待签名的字符串，需使用 UTF8 格式编码，以保持与其他系统兼容；

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

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

string strHashAlg:[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；

string strBase64PKCS7DetachedSignature:[OUT] Base64 编码的 PKCS#7 不带原文签名结果；

返回值:

0: 成功；

其它: 失败。

3.5 cfca_signData_PKCS7Attached

```
integer cfca_signData_PKCS7Attached(string strSignAlg,  
                                     string strSourceData,  
                                     string strPfxFilePath,  
                                     string strPfxPassWord,  
                                     string strHashAlg,
```


string strBase64PKCS7AttachedSignature)

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:

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

string strSourceData:[IN]待签名的字符串，需使用 UTF8 格式编码，以保持与其他系统兼容；

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

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

string strHashAlg:[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；

string strBase64PKCS7AttachedSignature:[OUT] Base64 编码的 PKCS#7 不带原文签名结果；

返回值:

0: 成功；

其它: 失败。

3.6 cfca_verifyDataSignature_PKCS1

integer cfca_verifyDataSignature_PKCS1(string strSignAlg,

```
string strSourceData,  
  
string strBase64CertContent,  
  
string strHashAlg,  
  
string strBase64PKCS1Signature)
```

描述:

按指定的算法类型（SM2/RSA），验证 PKCS#1 签名。

参数:

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

string strSourceData:[IN] 签名原字符串，需使用 UTF8 格式编码，以保持与其他系统兼容；

string strBase64CertContent:[IN] 用于验签的公钥证书内容（Base64 编码，不带证书头、尾）；

string strHashAlg:[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；

string strBase64PKCS1Signature:[IN] Base64 编码的 PKCS#1 签名结果；

返回值:

0: 成功；

其它: 失败。

3.7 cfca_verifyDataSignature_PKCS7Detached

```
integer cfca_verifyDataSignature_PKCS7Detached (string strSignAlg,  
                                                string strSourceData,  
                                                string strBase64PKCS7DetachedSignature,  
                                                string strBase64SignCertContent)
```

描述:

按指定的算法类型（SM2/RSA），验证 PKCS#7 不带原文签名。

参数:

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

string strSourceData:[IN]签名原文字符串，需使用 UTF8 格式编码，以保持与其他系统兼容；

string strBase64PKCS7DetachedSignature:[IN] Base64 编码的 PKCS#7 不带原文签名结果；

string strBase64SignCertContent:[OUT] PKCS#7 中的签名证书（Base64 编码；

返回值:

0: 成功；

其它: 失败。

3.8 cfca_verifyDataSignature_PKCS7Attached

```
integer cfca_verifyDataSignature_PKCS7Attached (string strSignAlg,
```

```
string strBase64PKCS7AttachedSignature,  
string strBase64SignCertContent,  
string strSourceData)
```

描述:

按指定的算法类型（SM2/RSA），验证 PKCS#7 带原文签名。

参数:

string strSignAlg:[IN] 算法类型，传入“SM2”或“RSA”，不区分大小写；
string strBase64PKCS7AttachedSignature:[IN] Base64 编码的 PKCS#7 带原文签名结果；
string strBase64SignCertContent:[OUT] PKCS#7 中的签名证书（Base64 编码）；
string strSourceData:[OUT] PKCS#7 签名原文字符串；

返回值:

0：成功；

其它：失败

3.9 cfca_signFile_PKCS7Detached

```
integer cfca_signFile_PKCS7Detached (string strSignAlg,  
string strSourceFilePath,  
string strPfxFilePath,  
string strPfxPassWord,  
string strHashAlg,
```

string strBase64PKCS7DetachedSignature)

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:

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

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

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

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

string strHashAlg:[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；

string strBase64PKCS7DetachedSignature:[OUT] Base64 编码的 PKCS#7 不带原文签名结果；

返回值:

0: 成功；

其它: 失败。

3.10 cfca_verifyFileSignature_PKCS7Detached

integer cfca_verifyFileSignature_PKCS7Detached(string strSignAlg,

string strSourceFilePath,

```
string strBase64PKCS7DetachedSignature,  
string strBase64SignCertContent)
```

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:

string strSignAlg:[IN] 算法类型，传入“SM2”或“RSA”，不区分大小写；
string strSourceFilePath:[IN] 待验签的文件原文路径，路径中不许有中文；
string strBase64PKCS7DetachedSignature:[IN] Base64 编码的 PKCS#7 不带原文
签名结果；

string strBase64SignCertContent:[OUT] 返回 PKCS#7 中的签名证书（Base64
编码；

返回值:

0: 成功；

其它: 失败。

3.11 cfca_encryptDataToCMSEnvelope

```
integer cfca_encryptDataToCMSEnvelope (string strAlgorithm,  
string strPlainData,  
string strBase64EncryptCert,  
string strSymEncAlg,  
string strBase64CMSEnvelope)
```

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:

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

string strPlainData:[IN] 待加密的明文字符串，需使用 UTF8 格式编码，以保持与其他系统兼容；

string strBase64EncryptCert:[IN] 用于加密的公钥证书内容（Base64 编码，不带证书头、尾）；

string strSymEncAlg:[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；

string strBase64CMSEnvelope:[OUT] 加密后的 Base64 编码数字信封；

返回值:

0: 成功；

其它: 失败

3.12 cfca_decryptDataFromCMSEnvelope

integer cfca_decryptDataFromCMSEnvelope (string strAlgorithm,

string strBase64CMSEnvelope,

string strPfxFilePath,

string strPfxPassWord,

string strPlainData)

描述:

按指定的算法类型（SM2/RSA），解密 CMS 格式的数字信封。

参数:

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

string strBase64CMSEnvelope:[IN] 待解密的 Base64 编码数字信封；

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

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

string strPlainData:[OUT] 解密出的明文字符串；

返回值:

0: 成功；

其它: 失败

3.13 cfca_symEncryptFile

integer cfca_symEncryptFile(string strSymEncAlgorithm,

string strPlainFilePath,

string strEncryptFilePath,

string strSymKey)

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密钥。

注意：待加密的明文文件大小不能超过 1G!

参数：

string strSymEncAlgorithm:[IN] 对称加密算法，传入 “3DES_CBC” 或 “SM4_CBC”，不区分大小写；

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

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

string strSymKey:[OUT] 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；

返回值：

0：成功；

其它：失败

3.14 cfca_symDecryptFile

```
integer cfca_symDecryptFile(string strSymEncAlgorithm,  
                             string strEncryptFilePath,  
                             string strSymKey,  
                             string strPlainFilePath)
```

描述：

使用指定的算法对文件进行解密。

参数:

string strSymEncAlgorithm:[IN] 对称解密算法，传入“3DES_CBC”或“SM4_CBC”，不区分大小写；

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

string strSymKey:[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；

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

返回值:

0: 成功；

其它: 失败

3.15 cfca_verifyCertificate

```
integer cfca_verifyCertificate(string strBase64CertContent,  
                               integer nCertVerifyFlag,  
                               string strTrustedCACertFilePath,  
                               string strCRLFilePath)
```

描述:

验证证书有效性。

参数:

string strBase64CertContent:[IN] 待验证的公钥证书内容（Base64 编码，不带证书头、尾）；

integer 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；

string strTrustedCACertFilePath:[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；

string strCRLFilePath:[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；

返回值：

0：成功；

其它：失败

3.16 cfca_getCertificateInfo

integer cfca_getCertificateInfo (string strBase64CertContent,
string strInfoType,
string strInfoContent)

描述：

根据传入的标识，获取证书的相关信息。

参数:

string strBase64CertContent:[IN] 公钥证书内容 (Base64 编码, 不带证书头、尾);

string strInfoType:[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;

string strInfoContent:[OUT] 返回获取到的证书信息;

返回值:

0: 成功;

其它: 失败

3.17 cfca_getPublicCertFromPFX

integer cfca_getPublicCertFromPFX (string strAlgorithm,
string strPfxFilePath,
string strPfxPassWord,
string strBase64CertContent)

描述:

从指定的软证书文件中，获取公钥证书。

参数:

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

string strPfxFilePath:[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；

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

string strBase64CertContent:[OUT] 获取到的 Base64 编码公钥证书内容；

返回值:

0: 成功；

其它: 失败

3.18 cfca_calculateDataHash

```
integer cfca_calculateDataHash (string strSourceData,  
                                string strHashAlg,  
                                string strHexHashData)
```

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。

参数:

string strSourceData:[IN]待计算哈希的字符串，需使用 UTF8 格式编码，以保持与其他系统兼容；

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

string strHexHashData:[OUT] 十六进制编码的哈希计算结果。

返回值：

0：成功；

其它：失败

3.19 cfca_calculateFileHash

integer cfca_calculateFileHash (string strSourceFilePath,
string strHashAlg,
string strHexHashData)

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。

参数：

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

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

string strHexHashData:[OUT] 十六进制编码的哈希计算结果。

返回值：

0: 成功;

其它: 失败

4 提供程序

提供 PHP 调用的扩展库及 PHP 调用 Demo.

PHP5.6 库: libSADKExtension.so.3.4.0.1

PHP7.0 库: libSADKExtension.so.3.4.0.1

PHP7.1 库: libSADKExtension.so.3.4.0.1

5 Demo 使用方法

1、 安装对应版本的 PHP 及扩展所需的运行时环境

2、 修改PHP的配置文件php.ini

修改PHP配置文件php.ini, 使php允许加载扩展, 并将当前扩展添加到其扩展列表中。在php.ini中将enable_dl改为On, 如下所示:

```
enable_dl = On
```

然后, 在php.ini中添加下面一行的内容:

```
extension=libSADKExtension.so.3.4.0.1
```

3、 将扩展库拷贝至 PHP 的扩展文件夹下

通过命令 php-config 查看当前 PHP 的扩展路径 extension-dir 值, 然后将当前扩展工具包拷贝到该目录下。

4、 拷贝cfcalog.conf到与Demo同一文件夹下

5、 通过命令行终端运行 Demo 文件

```
php SADKExtension.php
```