远洋地产服务器端工具包需求说明书

（版本：3.0）

中国金融认证中心

2011年10月10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 | 生成此文档 | 2011/10/10 | 廖洪琼 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目 录**

[1. 项目范围 1](#_Toc306288630)

[1.1 项目描述 1](#_Toc306288631)

[1.2 项目背景 1](#_Toc306288632)

[1.3 项目目标 1](#_Toc306288633)

[2. 环境 1](#_Toc306288634)

[2.1 语言显示 1](#_Toc306288635)

[2.2 操作系统 1](#_Toc306288636)

[2.3 提供版本 1](#_Toc306288637)

[3. 功能需求 2](#_Toc306288638)

[3.1 接口描述 2](#_Toc306288639)

[3.1.1 验签 2](#_Toc306288640)

[3.1.2 加密 2](#_Toc306288641)

[3.1.3 解密 3](#_Toc306288642)

[3.1.4 获取错误信息 3](#_Toc306288643)

# 1. 项目范围

## 1.1 项目描述

该文档描述远洋地产服务器端工具包需求。提供以下功能：

* 提供CMS标准的数字信封来加解密消息；
* 验证PKCS#7标准且带原文的签名；
* 验证证书有效性。

## 1.2 项目背景

远洋地产是需求方，中国金融认证中心（CFCA）是提供方。

## 项目目标

* 中国金融认证中心提供消息的加解密、验证PKCS#7标准且带原文的签名及验证证书有效性的相关API接口，以.dll形式提供；
* 提供相关接口的使用手册；
* 提供C#语言调用接口的Demo。

# 2. 环境

### 2.1 语言显示

页面语言环境支持：简体中文/美国英文；

### 2.2 操作系统

1. Server端需要支持Windows Server2003，Windows Server2008。

### 2.3 提供版本

提供32 位的版本。

# 3. 功能需求

## 3.1 接口描述

以COM组件的形式提供以下接口。

### 3.1.1 验签

**HRESULT VerifyMessageSignature(BSTR bstrSignature，long lCertVerifyFlag, BSTR bstrCACertFileNameList, BSTR bstrCRLFileName, BSTR \*pbstrSourceMessage)**

**描述：**

验证PKCS7标准（带原文）的消息签名。

**参数：**

BSTR bstrSignature：[IN] 签名结果（PKCS#7签名且带原文 ，Base64编码格式字符串（UTF-16 LE编码））。

long lCertVerifyFlag: [IN] 若为0则不检查证书有效性。最低位置1(0x1) 要求检查证书链表上所有证书的时间有效性；倒数第二位置1(0x02) 验证CRL签名以及证书是否在CRL列表中；倒数第三位置1(0x4) 检查证书链完整性及证书链上所有证书签名的有效性。若需要如下所示：

BSTR bstrCACertsFileName: [IN]颁发者证书链中所有证书路径及颁发CRL的证书路径。若存在多个证书，证书路径之间用“|”隔开。例如：“C:\cfcaOca.cer| C:\cfcaPca.cer| C:\cfcaRca.cer”；仅当lCertVerifyFlag 检查证书有效性时有效。证书的内容DER编码的二进制文件。

BSTR bstrCRLFileName: [IN] CRL文件的路径。仅当lCertVerifyFlag验证证书是否在吊销列表中时该参数有效。

BSTR \* pbstrSourceMessage：[IN] 返回消息原文。

### 3.1.2 加密

**HRESULT EncryptMessageasCMSEnvelope（BSTR bstrBase64EncodeCert，BSTR bstrSourceMessage, BSTR\* pbstrEncryptedMessage)**

**描述：**

用指定的公钥证书加密消息，加密后结果为CMS标准数字信封。

**参数：**

BSTR bstrBase64EncodeCert：[IN] 只带公钥的base64编码加密证书内容。

BSTR bstrSourceMessage：[IN] 原消息。

BSTR\* pbstrEncryptedMessage：[IN]加密后的消息。

### 3.1.3 解密

**HRESULT SelectDecryptCertificate（long lDeviceType, BSTR bstrPFXFileName, BSTR bstrPFXPassword)**

**描述：**

选择带私钥的解密证书。

**参数：**

long lDeviceType：设备类型。1-解密证书来自软库，即PFX文件；2-解密证书来自USBKey或者其它情况。

BSTR bstrPFXFileName：[IN]PFX文件名。当参数lDeviceType =1时有效。

BSTR bstrPFXPassword：[IN]PFX文件密码。当参数lDeviceType =1时有效。

**HRESULT DecryptCMSEnvelopMessage（BSTR bstrEncryptedMessage，BSTR \*pbstrSourceMessage)**

**描述：**

用上一接口选定的带私钥的证书解密消息。加密的消息为CMS标准的数字信封。

**参数：**

BSTR bstrEncryptedMessage：[IN]加密的消息（即CMS标准的数字信封）。

BSTR\* pbstrSourceMessage：[IN] 解密后的消息。

### 3.1.4 获取错误信息

**HRESULT GetLastErrorDesc（BSTR \*pbstrErrorDesc）**

**描述：**

显示最近一次调用接口导致发生错误的描述信息。

**参数：**

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