客户端控件使用手册

辽宁CA

地址：

TEL：

FAX：

Http://

变更记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本 | 日期 | 作者 | 变更说明 | 状态 | 页数 |
| 1.0 | 2016-04-20 | 晨 曦 | Initiated |  |  |
| 1.0 | 2016-05-09 | 王铁松 |  | Draft | 11 |
| 1.1 | 2016-05-10 | 丰 洋 |  | Draft | 11 |
| 0.101.0.21 | 2017-07-25 | 赵爱新 | 升级EFile文件接口 | Draft |  |
| 0.101.0.21 | 2017-07-27 | 赵爱新 | KeyStore对象中添加函数GetKeySN | Draft |  |

目录

[客户端控件使用手册 0](#_Toc450570569)

[1 概述 3](#_Toc450570570)

[2 功能 3](#_Toc450570571)

[3 使用方法 4](#_Toc450570572)

[4 接口说明 4](#_Toc450570573)

[4.1 KeyManager 4](#_Toc450570574)

[4.1.1 枚举说有证书 4](#_Toc450570575)

[4.1.2 显示出指定分类的证书 4](#_Toc450570576)

[4.1.3得到用户选择的证书初始化Cert对象 5](#_Toc450570577)

[4.1.4获取全部证书个数 5](#_Toc450570578)

[4.1.5获取指定排序位置的证书BASE64编码 5](#_Toc450570579)

[4.1.6根据指定排序位置的证书初始化KeyStore对象 5](#_Toc450570580)

[4.1.7根据所选证书初始化KeyStore对象 6](#_Toc450570581)

[4.1.8根据所选证书初始化对应的SealArray对象 6](#_Toc450570582)

[4.2 Cert 6](#_Toc450570583)

[4.2.1设置证书对象 6](#_Toc450570584)

[4.2.2获取证书拓展项 6](#_Toc450570585)

[4.2.3获取证书拓展项袋 7](#_Toc450570586)

[4.2.4获取证书的属性 7](#_Toc450570587)

[4.3 keyStore 7](#_Toc450570588)

[4.3.1 判断KeyStore是否可用 8](#_Toc450570589)

[4.3.2对可见数据签名 8](#_Toc450570590)

[4.3.3对二进制数据签名 8](#_Toc450570591)

[4.3.4 获取签名结果 8](#_Toc450570592)

[4.3.5 获取取得base64编码的证书 8](#_Toc450570593)

[4.3.6 设定UKEY 的PIN码 9](#_Toc450570594)

[4.4 SealArray 9](#_Toc450570595)

[4.4.1获取项目名称 9](#_Toc450570596)

[4.4.2获取印章数组所存印章个数 10](#_Toc450570597)

[4.4.3从印章数组中取得指定索引号的印章 10](#_Toc450570598)

[4.5 Seal 10](#_Toc450570599)

[4.5.1获取印章图片的base64编码 10](#_Toc450570600)

[4.5.2 获取印章名称 11](#_Toc450570601)

# 1概述

JHKey控件是PC客户端使用数字证书对数据进行签名验签以及其他操作的中间件，只需要注册一次，就可以随时调用，从而简化PKI相关的编程操作。

# 2功能

用户证书登录

从服务器端获得随机数

(服务端通过http获取)

正确

选择所使用的客户端证书

服务器调用认证网关服务接口，将上述数据发送至认证网关进行验证。

验证客户端证书密码

对获得的随机数数据签名

将签名结果，公钥证书，签名原文发送给服务器端

通过控件访问服务器：用户用UKey登录，成功后，访问服务器时，首先从服务器端获得随机数，验证服务器证书，验证正确后，用客户端证书对随机数签名后，把随机数、公钥证书、签名结果一起发送给服务器，交由服务器端验证；

通过控件可以对数据加密，解密，获得数据的散列值，获得签名证书、加密证书的详细信息；

通过控件用户可以修改、验证UKey的用户密码；

注：上文所说服务器，指的是业务系统自身的服务器，目前流程中，可以不使用服务器证书，仅下发随机数即可，客户端也不对服务器证书做验证。

# 3使用方法

首先必须先注册JHKey控件组件。方法：开始->运行->regsvr32 “控件或组件的绝对路径”。

# 4接口说明

该控件支持单个UKey和多个UKey的操作。有5个对象KeyManager，KeyStore，Cert ，SealArray，Seal

## 4.1 KeyManager

该组件枚举ukey中的证书，并提供对话框供用户从中选择证书并初始化ukey。

|  |  |
| --- | --- |
| 函数名称 | 函数功能 |
| EnumKeyStore | 枚举系统中所有证书 |
| ShowCertsDlg | 在对话框中显示出指定分类的证书供用户选择 |
| GetSelectedCert | 获取用户选择的证书 |
| GetCertCount | 获取全部系统中证书数量 |
| GetCert | 获取系统中的第几个的证书 |
| InitKeyStoreByIndex | 根据指定排序位置的证书初始化KeyStore对象 |
| InitKeyStore | 根据指定排序位置的证书初始化KeyStore对象 |
| InitSealStore | 根据指定排序位置的证书初始化的SealArray对象 |

### 4.1.1 枚举所有证书

|  |  |  |
| --- | --- | --- |
| 函数原型 | VOID EnumKeyStore() | |
| 功能描述 | 枚举所有证书 | |
| 参数 | 无 |  |
| 参数类型 | 无 |  |
| 返回值 | 无 | |

### 4.1.2 显示出指定分类的证书

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT ShowCertsDlg(lAlg, SigEnc) | |
| 功能描述 | 根据参数条件显示匹配的证书列表 | |
| 参数1 | lAlg | [IN]所显示证书类型  1：显示RSA证书  2：显示SM2证书  3：RSA与SM2证书都显示 |
| 参数类型 | INT | |
| 参数2 | SigEnc | [IN]所显示证书使用方式  1：显示签名证书  2：显示加密证书  3：签名或加密证书都显示 |
| 参数类型 | INT |  |
| 返回值 | 1. 用户选择了证书   0x1002 用户点击了取消按钮  0x1001 证书不存在，用户点击确认按键 | |

### 4.1.3得到用户选择的证书对象

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT GetSelectedCert(vi) | |
| 功能描述 | 获取用户选择的证书对象 | |
| 参数 | vi | Cert实例，KeyManger根据用户选择的证书将证书信息保存在Cert的实例 |
| 参数类型 | IDispatch\* | |
| 返回值 | 1. 成功   0x1002 证书格式错误  0x1003 证书主题解析错误  0x1004 base解码错误 | |

### 4.1.4获取全部证书个数

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT GetCertCount() | |
| 功能描述 | 获取全部证书个数 | |
| 参数 | 无 |  |
| 参数类型 | 无 | |
| 返回值 | 返回所有证书的个数 | |

### 4.1.5获取指定排序位置的证书(BASE64编码)

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetCert (nIndex) | |
| 功能描述 | 获取指定位置排序位置的证书(BASE64编码) | |
| 参数 | nIndex | 指定位置证书的索引 |
| 参数类型 | INT | |
| 返回值 | 返回对应的证书base64编码字符串 | |

### 4.1.6根据指定排序位置的证书生成KeyStore对象

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT InitKeyStoreByIndex (nIndex, vi) | |
| 功能描述 | 根据指定排序位置的证书生成KeyStore对象 | |
| 参数1 | nIndex | [IN] 指定位置证书的索引 |
| 参数类型 | INT | |
| 参数2 | Vi | [OUT]证书对应的KeyStore对象 |
| 参数类型 | IDispatch \* | |
| 返回值 | 1. 成功   0x1001 传入的Index超出了数组的大小  0x2004 驱动没有加载  0x2005 初始化key失败 | |

### 4.1.7根据所选证书生成KeyStore对象

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT InitKeyStore (vi) | |
| 功能描述 | 根据所选证书生成KeyStore对象 | |
| 参数 | vi | [OUT]证书对应的KeyStore对象 |
| 参数类型 | IDispatch\* | |
| 返回值 | 1. 成功   0x1001 选择的证书超出了数组的大小  0x2004 驱动没有加载  0x2005 初始化key失败 | |

### 4.1.8根据所选证书生成对应的SealArray对象

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT InitSealStore (para1) | |
| 功能描述 | 根据所选证书生成对应的SealArray对象 | |
| 参数 | para1 | [OUT]证书对应的KeyStore对象 |
| 参数类型 | IDispatch\* | |
| 返回值 | 印章的个数  0x1001 选择的证书超出了数组的大小 | |

## 4.2 Cert

证书信息组件，用于从证书实体中获取该证书各种属性信息，比如

### 4.2.1设置证书对象

|  |  |  |
| --- | --- | --- |
| 函数原型 | VOID SetCert(szCertBase64) | |
| 功能描述 | 设置证书对象 | |
| 参数 | szCertBase64 | [IN]证书的base64 |
| 参数类型 | BSTR\* | |
| 返回值 | 无 | |

### 4.2.2获取证书拓展项

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetCertExt (szExtIOD,) | |
| 功能描述 | 获取证书拓展项 | |
| 参数 | szExtIOD | [IN]证书的扩展项ID \*偏移量是2 |
| 参数类型 | BSTR \* | |
| 返回值 | 证书拓展项字符串 | |

### 4.2.3获取证书拓展项

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetCertExt2(szExtIOD，offset) | |
| 功能描述 | 获取证书拓展项 | |
| 参数1 | szExtIOD | [IN]证书的扩展项ID |
| 参数类型 | BSTR \* | |
| 参数2 | offset | [OUT]偏移量 |
| 参数类型 | INT | |
| 返回值 | 证书拓展项字符串 | |

### 4.2.4获取证书的属性

|  |  |  |
| --- | --- | --- |
| 属性名称 | 属性类型 | 属性说明 |
| IsValidCert | INT | 证书格式是否正确 1:正确，0：不正确 |
| CertType | INT | 证书类型，1:RSA，2:SM2 |
| CertSN | BSTR | 证书序列号 |
| CertOuI | BSTR | 证书OUI项 |
| CertOuA | BSTR | 证书OUA项 |
| CertCN | BSTR | 证书CN项 |
| CertOu | BSTR | 证书OU项 |
| CertSubject | BSTR | 证书主题项 |
| CertIssuerSubject | BSTR | 证书颁发者主题项 |
| CertNotBefore | BSTR | 证书生效时间 |
| CertNotAfter | BSTR | 证书失效时间 |
| CertPubKey | BSTR | 证书公钥信息 |
| Body | BSTR | 证书的base64编码 |
| CertUsage | INT | 证书用法，1:签名，2:加密 |

## 4.3 keyStore

KeyStore组件需要由KeyManager 进行初始化后，可以对数据进行签名等操作

|  |  |
| --- | --- |
| 函数名称 | 函数功能 |
| IsValid | 判断该KeyStore是否可用 |
| SignData | 对可见数据签名 |
| SignDataBase64 | 对二进制数据签名 |
| GetSignData | 取得签名数据 |
| GetCertBase64 | 取得base64编码的证书 |
| SetWorkPin | 设置默认pin码 |
| GetKeySN | 获取设备硬件码列表值（ukey ID） |

### 4.3.1 判断KeyStore是否可用

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT IsValid () | |
| 功能描述 | 判断keystore是否可用 | |
| 参数 | 无 |  |
| 参数类型 | 无 | |
| 返回值 | 1可用 0 不可用 | |

### 4.3.2对可见数据签名

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT SignData (bfSrc) | |
| 功能描述 | 对可见数据签名 | |
| 参数 | bfSrc | [IN] bfSrc 可见签名原文 |
| 参数类型 | BSTR | |
| 返回值 | 0 成功  0x2009 RSAkey 密码输入错误  0x2010 没有插key或者用户取消输入密码  Ox2006 SM2Key 密码检验错误  0x2007 SM2Key 密码被锁死 | |

### 4.3.3对二进制数据签名

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT SignDataBase64 (bfSrc) | |
| 功能描述 | 对不可见数据进行签名 | |
| 参数 | bfSrc | [IN] bfSrc 不可见字符的BASE64编码 |
| 参数类型 | BSTR | |
| 返回值 | 0 成功  0x2009 RSAkey 密码输入错误  0x2010 没有插key或者用户取消输入密码  Ox2006 SM2Key 密码检验错误  0x2007 SM2Key 密码被锁死 | |

### 4.3.4获取签名结果

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetSignData() | |
| 功能描述 | 获取签名结果 | |
| 参数 | 无 |  |
| 参数类型 | 无 | |
| 返回值 | 返回签名结果的BASE64编码 | |

### 4.3.5 获取取得base64编码的证书

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetCertBase64 () | |
| 功能描述 | 获取取得base64编码的证书 | |
| 参数 | 无 |  |
| 参数类型 | 无 | |
| 返回值 | 返回当前keystore的BASE64编码证书 | |

### 4.3.6设定UKEY 的PIN码

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT SetWorkPin(szPin) | |
| 功能描述 | 设定UKEY 的PIN码 | |
| 参数 | szPin | [IN] UKEY PIN码 |
| 参数类型 | BSTR | |
| 返回值 | 返回值预留没意义 | |

### 4.3.7获取设备硬件码列表值（ukey ID）

|  |  |
| --- | --- |
| 函数原型 | BSTR GetKeySN () |
| 功能描述 | 获取设备硬件码列表值（ukey ID） |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 设备硬件码列表值（ukey ID） |

## 4.4 SealArray

SealArray 组件为ukey中的印章列表信息, 该组件也需要通过KeyManager进行初始化后可使用。

|  |  |
| --- | --- |
| 函数名称 | 函数功能 |
| GetUserName | 获取项目名称 |
| GetSealCount | 获取印章数组所存印章个数 |
| GetSeal | 从印章数组中取得指定索引号的印章 |

### 4.4.1获取项目名称

|  |  |  |
| --- | --- | --- |
|  | BSTR GetUserName ()预留 | |
| 功能描述 | 获取项目名称 | |
| 参数 | 无 |  |
| 参数类型 | 无 |  |
| 返回值 | 返回项目名称BSTR | |

### 4.4.2获取印章数组所存印章个数

|  |  |  |
| --- | --- | --- |
|  | INT GetSealCount () | |
| 功能描述 | 获取印章数组个数 | |
| 参数 | 无 |  |
| 参数类型 | 无 |  |
| 返回值 | 返回印章个数 | |

### 4.4.3从印章数组中取得指定索引号的印章

|  |  |  |
| --- | --- | --- |
|  | INT GetSeal(nIndex, iSeal) | |
| 功能描述 | 从印章数组中取得指定索引号的印章 | |
| 参数1 | nIndex | [IN]印章数组中指定印章的索引号 |
| 参数类型 | INT | |
| 参数2 | iSeal | [IN] CSealcom对象 |
| 参数类型 | IDispatch\* | |
| 返回值 | 返回值没实际意义 | |

## 4.5 Seal

Seal组件保存ukey中单个印章的信息，比如印章图片，印章名称

|  |  |
| --- | --- |
| 函数名称 | 函数功能 |
| GetPic | 获取印章图片的base64编码 |
| GetName | 获取印章名称 |

### 4.5.1获取印章图片的base64编码

|  |  |  |
| --- | --- | --- |
|  | BSTR GetPic() | |
| 功能描述 | 从印章图片的base64编码 | |
| 参数 | 无 |  |
| 参数类型 | 无 | |
| 返回值 | 印章图片base64编码 | |

### 4.5.2 获取印章名称

|  |  |  |
| --- | --- | --- |
|  | BSTR GetName () | |
| 功能描述 | 获取印章名称 | |
| 参数 | 无 |  |
| 参数类型 | 无 | |
| 返回值 | 印章名称 | |

## 4.6 Util

该组件为编码转换提供支持

|  |  |
| --- | --- |
| 函数名称 | 函数功能 |
| JHBase64Encode | 数据Base64编码 |
| JHBase64Decode | 数据Base64解码 |
| Sm2Hash | 数据sm2哈希 |
|  |  |

### 4.6.1数据Base64编码

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR JHBase64Encode(input) | |
| 功能描述 | 对传入的input 进行base64编码 | |
| 参数 | input | [IN] 传入二进制或字串数据 |
| 参数类型 | VARIANT& | |
| 返回值 | 返回传入数据base64编码字符串 | |

### 4.6.2数据Base64解码

|  |  |  |
| --- | --- | --- |
| 函数原型 | VOID JHBase64Decode(input, inputLen , output, outputLen) | |
| 功能描述 | 对传入的二进制 进行base64解码 | |
| 参数1 | input | [IN] 传入二进制或字串数据 |
| 参数类型 | [in] BYTE\* | |
| 参数2 | inputLen | [IN] 传入二进制或字串数据长度 |
| 参数类型 | [in] INT | |
| 参数3 | output | [out]传出解码数据 |
| 参数类型 | [out] BYTE\* | |
| 参数4 | outputLen | [out]传出解码数据长度 |
| 参数类型 | [out] INT\* | |
| 返回值 | 无 | |

### 4.6.3数据取哈希

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR Sm2Hash(input, cert) | |
| 功能描述 | 对传入的数据用sm2证书取哈希值 | |
| 参数1 | input | [IN] 传入base64数据 |
| 参数类型 | [in] VARIANT |  |
| 参数2 | cert | [IN] 传入base64的sm2证书 |
| 参数类型 | [in] BSTR |  |
| 返回值 | 哈希值的base64编码 | |

## 4.7 KeyDetector

该组件为获取key相关信息等提供支持

|  |  |
| --- | --- |
| 函数名称 | 函数功能 |
| EnumUKey | 枚举Key |
| GetDrvNum | 取key类型编号 |
| CheckDriver | 检查驱动是否安装 |
| GetKeyBrandName | 取得指定key品牌中文名 |
| GetKeyName | 取得指定key英文名 |
| GetKeyCSPName | 取得指定Key CSP名 |
|  |  |
| GetKeyVersion | 取得JHKey控件版本 |
| GetDriverVersion | 取得指定Key 驱动版本号 |
|  |  |

### 4.7.1枚举Key

|  |  |
| --- | --- |
| 函数原型 | INT EnumUKey() |
| 功能描述 | 检测当前电脑插入的key |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 当前电脑插入key的数量 |

### 4.7.2 取key类型编号

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT GetDrvNum(nIdx) | |
| 功能描述 | 取当前key列表指定key类型编号 | |
| 参数 | nIdx | [IN] 传入0起始的索引值 |
| 参数类型 | [in] INT | |
| 返回值 | key类型编号(1华大 2海泰 3龙肪 4大明) | |

### 4.7.3 检查驱动是否安装

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT CheckDriver( nDrv） | |
| 功能描述 | 根据key类型编号返回对应驱动是否安装 | |
| 参数 | nDrv | [IN] 传入key类型编号 |
| 参数类型 | [in] INT | |
| 返回值 | 驱动已安装返回0 ，驱动未安装返回1 | |

### 4.7.4 取得指定key品牌中文名

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetKeyBrandName(nDrv) | |
| 功能描述 | 取得指定Key类型编号对应的品牌中文名 | |
| 参数 | nDrv | [IN] 传入key类型编号 |
| 参数类型 | [in] INT | |
| 返回值 | 指定Key类型编号对应的品牌中文名如"华大","海泰" | |

### 4.7.5 取得指定key英文名

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetKeyName(nDrv） | |
| 功能描述 | 取得指定Key类型编号对应的品牌英文名 | |
| 参数 | nDrv | [IN] 传入key类型编号 |
| 参数类型 | [in] INT |  |
| 返回值 | 指定Key类型编号对应的品牌英文名如"HUADA","HAITAI" | |

### 4.7.6 取得指定Key CSP名

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetKeyCSPName(nDrv) | |
| 功能描述 | 取得指定Key类型编号对应的CSP | |
| 参数 | nDrv | [IN] 传入key类型编号 |
| 参数类型 | [in] INT |  |
| 返回值 | 指定Key类型编号对应的CSP名如"ZGHD Cryptographic Service Provider v1.0 For LNCA" | |

### 4.7.7 取得JHKey控件版本

|  |  |
| --- | --- |
| 函数原型 | BSTR GetKeyVersion(） |
| 功能描述 | 取得当前电脑安装的JHKey控件版本 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 当前电脑安装的JHKey控件版本如："0.100.0.7" |

### 4.7.8 取得指定Key 驱动版本号

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetDriverVersion(nDro） | |
| 功能描述 | 取得指定Key类型编号对应的驱动版本号 | |
| 参数 | nDro | [IN] 传入key类型编号 |
| 参数类型 | [in] INT |  |
| 返回值 | 指定Key类型编号对应的驱动版本号如"1.0.7.0" | |

## 4.8 GateOper

该组件为网关操作提供支持

|  |  |
| --- | --- |
| 函数名称 | 函数功能 |
| SetTimeout | 设置和服务器通信的超时时间 |
| SetURL | 设置服务器的url |
| ReqSM2Sign | 请求sm2签名 |
| ReqCertLogin | 请求登录 |
| ReqVerifySig | 请求验证签名 |
| GetLastSvrSig | 获取签名值 |
| GetLastSvrCert | 获取证书 |
| GetLastErrText | 获取错误信息 |
| GetToken | 获取令牌 |
| ReqUploadMedRecord | 上传签名记录 |
| GetSvrStorageSerial | 获取存储序列号 |
| GetSvrStorageId | 获取存储id |
| GetSvrStorageTime | 获取存储时间 |
| GetSvrStorageSig | 获取存储签名值 |
| GetSvrStoreCert | 获取存储证书 |
| GetClicert | 获取Clicert |
| GetClisig | 获取Clisig |
| GetSvrStorageTimestamp | 获取时间戳 |

### 4.8.1 设置和服务器通信的超时时间

|  |  |  |
| --- | --- | --- |
| 函数原型 | VOID SetTimeout(msMaxWait) | |
| 功能描述 | 多长时间服务器无动作算超时 | |
| 参数 | msMaxWait | [IN] 传入超时时间（单位：秒） |
| 参数类型 | [in] INT | |
| 返回值 | 无 | |

### 4.8.2 设置服务器的url

|  |  |  |
| --- | --- | --- |
| 函数原型 | VOID SetURL(szUrl) | |
| 功能描述 | 设置服务器的url | |
| 参数 | szUrl | [IN] 服务器url |
| 参数类型 | [in] BSTR |  |
| 返回值 | 无 | |

### 4.8.3请求sm2签名

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT ReqSM2Sign(szSrc, nFmt) | |
| 功能描述 | 对传入的数据提交到服务器进行sm2签名 | |
| 参数1 | szSrc | [IN] 传入原文base64数据 |
| 参数类型 | [in] BSTR | |
| 参数2 | nFmt | 暂时没用到 |
| 参数类型 | [in] VOID | |
| 返回值 | 0 正确  7 签名失败  8 格式错误 | |

### 4.8.4请求登录

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT ReqCertLogin(keystore, szApp) | |
| 功能描述 | 用指定的key登录服务器 | |
| 参数1 | keystore | [IN] 传入原文base64数据 |
| 参数类型 | [in] IDispatch\* | |
| 参数2 | szApp | 暂时没用到传入""即可 |
| 参数类型 | [in] BSTR | |
| 返回值 | 0 登录成功  其它 登录失败 | |

### 4.8.5请求验证签名

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT ReqVerifySig(sig, szSrc, nFmt, szCert) | |
| 功能描述 | 对传入的签名值进行验签 | |
| 参数1 | sig | [IN] 传入签名值base64字串 |
| 参数类型 | [in] BSTR | |
| 参数2 | szSrc | [IN] 传入原文base64字串 |
| 参数类型 | [in] BSTR | |
| 参数3 | nFmt | [IN] 暂时没用到传入0 |
| 参数类型 | [in] VOID | |
| 参数4 | szCert | [IN]传入证书 |
| 参数类型 | [in] BSTR | |
| 返回值 | 0 成功  其它 失败 | |

### 4.8.6 获取签名值

|  |  |
| --- | --- |
| 函数原型 | BSTR GetLastSvrSig(） |
| 功能描述 | 获取最近一次签名值 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 签名值的base64字串 |

### 4.8.7 获取证书

|  |  |
| --- | --- |
| 函数原型 | BSTR GetLastSvrCert (） |
| 功能描述 | 获取最近一次使用的证书 |
| 返回值 | 证书的base64字串 |

### 4.8.8 获取错误信息

|  |  |
| --- | --- |
| 函数原型 | BSTR GetLastErrText(） |
| 功能描述 | 获取最近一次的错误信息 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 错误信息字串 |

### 4.8.9 获取令牌

|  |  |
| --- | --- |
| 函数原型 | BSTR GetToken (） |
| 功能描述 | 获取最近一次的令牌字串 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 令牌字串 |

### 4.8.10 上传签名记录

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT ReqUploadMedRecord(szApp, appid, docid, docname, textinfo, signdata, signcert, signdate) | |
| 功能描述 | 上传签名记录 | |
| 参数1 | szApp | [IN] 传入 应用字串 |
| 参数类型 | [in] BSTR | |
| 参数2 | appid | [IN] 传入 应用id字串 |
| 参数类型 | [in] BSTR | |
| 参数3 | docid | [IN] 传入文档id字串 |
| 参数类型 | [in] BSTR | |
| 参数4 | docname | [IN] 传入 文档名字串 |
| 参数类型 | [in] BSTR | |
| 参数5 | textinfo | [IN] 传入 文本内容字串 |
| 参数类型 | [in] BSTR | |
| 参数6 | signdata | [IN] 传入 签名结果字串 |
| 参数类型 | [in] BSTR | |
| 参数7 | signcert | [IN] 传入 签名证书字串 |
| 参数类型 | [in] BSTR | |
| 参数8 | signdate | [IN] 传入 签名日期字串 |
| 参数类型 | [in] BSTR | |
| 返回值 | 0 成功  其它 失败 | |

### 4.8.11 获取存储序列号

|  |  |
| --- | --- |
| 函数原型 | BSTR GetSvrStorageSerial() |
| 功能描述 | 获取上传签名记录的存储序列号 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 存储序列号字串 |

### 4.8.12 获取存储id

|  |  |
| --- | --- |
| 函数原型 | BSTR GetSvrStorageId() |
| 功能描述 | 获取上传签名记录的存储id |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 存储id字串 |

### 4.8.13 获取存储时间

|  |  |
| --- | --- |
| 函数原型 | BSTR GetSvrStorageTime() |
| 功能描述 | 获取上传签名记录的存储时间 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 存储id字串 |

### 4.8.14 获取存储签名值

|  |  |
| --- | --- |
| 函数原型 | BSTR GetSvrStorageSig() |
| 功能描述 | 获取上传签名记录的存储签名值 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 存储签名值字串 |

### 4.8.15 获取存储证书

|  |  |
| --- | --- |
| 函数原型 | BSTR GetSvrStoreCert() |
| 功能描述 | 获取上传签名记录的存储证书 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 存储证书字串 |

### 4.8.16 获取Clicert

|  |  |
| --- | --- |
| 函数原型 | BSTR GetClicert() |
| 功能描述 | 获取上传签名记录的CliCert |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | CliCert书字串 |

### 4.8.17 获取Clisig

|  |  |
| --- | --- |
| 函数原型 | BSTR GetClisig() |
| 功能描述 | 获取上传签名记录的Clisig |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | Clisig字串 |

### 4.8.18 获取时间戳

|  |  |
| --- | --- |
| 函数原型 | BSTR GetSvrStorageTimestamp () |
| 功能描述 | 获取上传签名记录的时间戳 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 时间戳字串 |

## 4.9 EFile

该组件实现对EFile文件格式的操作，可支持如下功能：

1. 支持单次/多次加密
2. 支持单次/多次签名
3. 支持单次/多次加密 后 单次/多次签名
4. 不支持签名后再加密，由于原文不再可见，因此无法在实现解密前验签
5. 不能在加密后生成EFile文件后，再使用EFile文件Open再进行加密，因为此时密文已经灭失掉，只有持有这几个加密证书ukey才能进行解密，但是可以进行验签操作。

|  |  |
| --- | --- |
| 函数名称 | 函数功能 |
| OpenStream | 打开一个普通文件 |
| Open | 打开一个EFile文件或一个普通文件 |
| Version | 文件格式版本号 |
| IsEFile | 判断是否为EFile文件 |
| SaveAsEFile | 保存EFile文件 |
| ComposeEFile | 生成EFile文件的Base64编码结构 |
|  |  |
| GetSourceEFile | 获取EFile文件中的原文件 |
| SaveSourceEFile | 把解密后的原文件保存 |
| IsSourceEncrypted | 返回是否EFile中原文件已经被加密 |
| GetSignCertCount | 内部的签名证书数量 |
| GetSignCert | 获取第nlndex个签名证书 |
| GetEncCertCount | EFile加密证书数量 |
| GetTSSign | 获取第nlndex个签名对应时间戳数据 |
| GetTSTime | 获取时间戳时间 |
| GetSign | 获取第nlndex个签名证书对应的签名结果 |
| GetEncCert | 获取第nlndex加密证书 |
| GetFileSize | 获取EFile文件长度 |
| Close | 关闭文件释放所有变量 |
| Sign | 使用keystore对EFile数据进行签名 |
| Enc | 加密数据 |
| Verify | 使用keystore对第nlndex个cert进行验签 |
| Dec | 使用keystore对数据进行解密 |

### 4.9.1打开一个普通文件

|  |  |  |
| --- | --- | --- |
| 函数原型 | BOOL OpenStream (szFileB64,bEfl) | |
| 功能描述 | 打开一个普通文件 | |
| 参数1 | [in] szFileB64 | [in]文件的base64 |
| 参数类型 | BSTR | |
| 参数2 | [in]bEfl | [in]为1的情况下原文件按照非EFile处理  [in]为0的情况下原文件按照EFile处理 |
| 参数类型 | INT | |
| 返回值 | 文件打开是否成功 0：成功； 其他：失败 | |

### 4.9.2打开一个EFile文件或一个普通文件

|  |  |  |
| --- | --- | --- |
| 函数原型 | BOOL Open (szFileName,bEfl) | |
| 功能描述 | 打开一个普通文件 | |
| 参数1 | [in]szFileName | [in]文件的路径 |
| 参数类型 | BSTR | |
| 参数2 | [in]bEfl | [in]为1的情况下原文件按照非EFile处理  [in]为0的情况下原文件按照EFile处理 |
| 参数类型 | INT | |
| 返回值 | 文件打开是否成功 0：成功； 其他：失败 | |
| 函数说明 | szFileName为空则弹出FileDialog,szFileName可为URL（目前不支持连接） | |

### 4.9.3文件格式版本号

|  |  |
| --- | --- |
| 函数原型 | LPCTSTR Version () |
| 功能描述 | 文件格式版本号 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 文件格式版本号 |

### 4.9.4判断是否为EFile文件

|  |  |
| --- | --- |
| 函数原型 | BOOL IsEFile () |
| 功能描述 | 判断是否为EFile文件 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 判断是否为EFile文件 true:是EFile文件 false：不是EFile文件 |

### 4.9.5保存EFile文件

|  |  |  |
| --- | --- | --- |
| 函数原型 | BOOL SaveAsEFile (szFileName) | |
| 功能描述 | 保存EFile文件 | |
| 参数 | [in]szFileName | [in]文件保存的路径 |
| 参数类型 | BSTR | |
| 返回值 | 保存EFile文件 true：保存成功 false：保存失败 | |

### 4.9.6生成的EFile文件的Base64编码结构

|  |  |
| --- | --- |
| 函数原型 | BSTR ComposeEFile () |
| 功能描述 | 生成的EFile文件的Base64编码结构 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 生成的EFile文件的Base64编码结构 |

### 4.9.7获取EFile文件中的原文件

|  |  |
| --- | --- |
| 函数原型 | BSTR GetSourceEFile () |
| 功能描述 | 获取EFile文件中的原文件 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 获取EFile文件中的原文件 |

### 4.9.8把解密后的原文件保存

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT SaveSourceEFile (szFileName) | |
| 功能描述 | 把解密后的原文件保存 | |
| 参数 | [in] szFileName | [in]文件路径 |
| 参数类型 | BSTR | |
| 返回值 | 0：保存成功；1：保存失败 | |

### 4.9.9返回是否EFile中原文件已经被加密

|  |  |
| --- | --- |
| 函数原型 | BOOL IsSourceEncrypted () |
| 功能描述 | 判断原文件是否已被加密 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | true：原文件已经被加密；false：原文件未被加密 |

### 4.9.10内部的签名证书数量

|  |  |
| --- | --- |
| 函数原型 | INT GetSignCertCount () |
| 功能描述 | 获取内部的签名证书数量 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | 内部的签名证书数量 |

### 4.9.11获取第nlndex个签名证书

|  |  |  |
| --- | --- | --- |
| 函数原型 | LPCTSTR GetSignCert (nlndex) | |
| 功能描述 | 获取第nlndex个签名证书 | |
| 参数 | [in] nlndex | [in]证书索引号 |
| 参数类型 | INT | |
| 返回值 | 获取第nlndex个的签名证书 | |

### 4.9.12 EFile加密证书数量

|  |  |
| --- | --- |
| 函数原型 | INT GetEncCertCount () |
| 功能描述 | 获取EFile加密证书数量 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | EFile加密证书数量 |

### 4.9.13获取第nlndex个签名对应时间戳数据

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetTSSign (nlndex) | |
| 功能描述 | 获取第nlndex个签名对应时间戳数据 | |
| 参数 | [in] nlndex | 签名索引号 |
| 参数类型 | INT | |
| 返回值 | 第nlndex个签名结果 | |
| 函数说明 | 该函数获取第nlndex签名，对应时间戳数据（验证或者解析该数据请使用JHTSA控件） | |

### 4.9.14获取时间戳时间

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetTSTime (nlndex) | |
| 功能描述 | 获取时间戳时间 | |
| 参数 | [in] nlndex | 时间戳索引号 |
| 参数类型 | INT | |
| 返回值 | 第nlndex个时间戳时间 | |

### 4.9.15获取第nlndex个签名证书对应的签名结果

|  |  |  |
| --- | --- | --- |
| 函数原型 | BSTR GetSign (nlndex) | |
| 功能描述 | 获取第nlndex个签名证书对应的签名结果 | |
| 参数 | [in] nlndex | 签名证书索引号 |
| 参数类型 | INT | |
| 返回值 | 第nlndex个签名证书对应的签名结果 | |

### 4.9.16获取第nlndex加密证书

|  |  |  |
| --- | --- | --- |
| 函数原型 | LPCTSTR GetEncCert (nlndex) | |
| 功能描述 | 获取第nlndex加密证书 | |
| 参数 | [in] nlndex | 加密证书索引号 |
| 参数类型 | INT | |
| 返回值 | 第nlndex加密证书 | |

### 4.9.17获取EFile文件长度

|  |  |
| --- | --- |
| 函数原型 | INT GetFileSize () |
| 功能描述 | 获取EFile文件长度 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | EFile文件长度 |

### 4.9.18关闭文件释放所有变量

|  |  |
| --- | --- |
| 函数原型 | BOOL Close () |
| 功能描述 | 关闭文件释放所有变量 |
| 参数 | 无 |
| 参数类型 | 无 |
| 返回值 | true：成功关闭文件释放所有变量； false：关闭文件释放所有变量失败 |

### 4.9.19使用keystore对EFile数据进行签名

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT Sign (keystore,szTsaUrl) | |
| 功能描述 | 使用keystore对EFile数据进行签名 | |
| 参数1 | [in] keystore | [in]所选证书对应的keystore |
| 参数类型 | IDispath | |
| 参数2 | [in] szTsaUrl | [in]时间戳服务器地址 |
| 参数类型 | BSTR | |
| 返回值 | 0:签名成功；1：签名失败 | |
| 函数说明 | 使用时间戳服务器（目前不支持时间戳） | |

### 4.9.20加密数据

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT Enc (szEncCert,szTsaUrl) | |
| 功能描述 | 加密数据 | |
| 参数1 | [in] szEncCert | [in]加密证书 |
| 参数类型 | BSTR | |
| 参数2 | [in] szTsaUrl | [in]时间戳服务器地址 |
| 参数类型 | BSTR | |
| 返回值 | 0:加密成功；1：加密失败 | |
| 函数说明 | 使用时间戳服务器（如果要加密的话，目前不支持加密部分的签名时间戳，并且咱们使用的加密证书通常是别人的而不是插在你电脑上的ukey里的） | |

### 4.9.21使用keystore对第nlndex个cert进行验签

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT Verify (keystore,nlndex) | |
| 功能描述 | 加密数据 | |
| 参数1 | [in] keystore | [in] 所选证书对应的keystore |
| 参数类型 | IDispath | |
| 参数2 | [in] nlndex | [in]证书索引号 |
| 参数类型 | INT | |
| 返回值 | 0:验签成功；1：验签失败 | |
| 函数说明 | Keystore只要初始化连接PC机上插着的LNCA发放的支持算法ukey即可，不需要ukey必须包含正确的签名证书 | |

### 4.9.22使用keystore对数据进行解密

|  |  |  |
| --- | --- | --- |
| 函数原型 | INT Dec (keystore) | |
| 功能描述 | 使用keystore对数据进行解密 | |
| 参数 | [in] keystore | [in] 所选证书对应的keystore |
| 参数类型 | IDispath | |
| 返回值 | 0:解密成功；1：解密失败 | |

请参看提供的例子理解和使用这些组件。