

农校对接平台证书应用工具包 软件需求说明书

中国金融认证中心

2013 年 12 月 19 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	初稿：在标准版 3.2.0.7 版中精简版接口基础上增加如下接口： 1) 获取当前控件版本号； 2) 获取选定签名证书序列号； 3) 获取选定签名证书有效时间	2013/12/19	张欣欣	李达、范文露
3.1	导入证书链时，不需导入 863CA	2013/12/19	张欣欣	

目 录

1. 项目范围.....	1
1.1 项目描述.....	1
1.2 项目背景.....	1
1.3 项目目标.....	1
2. 环境.....	1
2.1 语言显示.....	1
2.2 操作系统.....	1
3 接口描述.....	1
GetVersion.....	2
SelectSignCertificate.....	2
GetCSPNameofSignCert	2
GetSelectedCertContent	3
GetSelectedCertSN	3
GetSelectedCertVaildTime	3
SignMessage.....	4
GetLastErrorDesc.....	4
4 安装证书链.....	5

1. 项目范围

1.1 项目描述

中国金融认证中心以 COM 组件的形式，为其他应用程序提供签名验证等功能的工具包程序。

1.2 项目背景

中国金融认证中心自主开发，提供具有电子签名，电子签名验证功能的控件。

1.3 项目目标

保证在所列出的操作系统平台及浏览器下能够正常运行及技术支持。

2. 环境

2.1 语言显示

页面语言环境支持：美国英文，简体中文

2.2 操作系统

- 32 位操作系统

Window XP、Windows Vista、Windows 7、WinServer2003、WinServer2008

- 64 位操作系统

Windows Vista、Windows 7、WinServer2003、WinServer2008

- IE 浏览器

IE6、IE7、IE8、IE9、IE10

(注：由于目前 IE10 只能开启 32 位模式，故目前只能调用 32 位控件)

3 接口描述

GetVersion

HRESULT GetVersion (BSTR* pbstrVersion)

描述:

获取当前控件版本号。

参数:

BSTR* pbstrVersion[OUT, RETVAL] –当前控件版本号

SelectSignCertificate

HRESULT SelectSignCertificate (
 BSTR bstrSubjectDNFilter,
 BSTR bstrIssueDNFilter,
 BSTR* pbstrSubjectDN)

描述:

从 windows 的证书库中, 按照过滤条件(Subject DN or IssuerDN)选择带私钥的签名证书。

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* pbstrSubjectDN[OUT, RETVAL] -返回被选出证书的主题 DN

GetCSPNameofSignCert

HRESULT GetCSPNameofSignCert (BSTR* pbstrCSPName)

描述:

在选择签名私钥证书后，获得签名证书所属 CSP 的名称

参数:

BSTR* pbstrCSPName [OUT, RETVAL] -返回签名证书所属的 CSP 的名称

GetSelectedCertContent

HRESULT GetSelectedCertContent (BSTR* pbstrCertificate)

描述:

在选择签名证书后，获取公钥证书内容（Base64编码）。该函数必须在调用完 SelectSignCertificate()、SelectSignCertificateByPFXFile()之后调用。

参数:

BSTR* pbstrCertificate [OUT, RETVAL] - Base64 编码的公钥证书内容。

GetSelectedCertSN

HRESULT GetSelectedCertSN (BSTR* pbstrCertSN)

描述:

在选择签名私钥证书后，获得签名证书序列号。

参数:

BSTR* pbstrCertSN [OUT, RETVAL] 证书序列号。

GetSelectedCertVaildTime

HRESULT GetSelectedCertVaildTime (BSTR* pbstrCertTime)

描述:

在选择签名私钥证书后，获得签名证书的结束时间。

参数:

BSTR* pbstrCertTime [OUT, RETVAL] 证书结束时间。

SignMessage

HRESULT SignMessage (
 BSTR bstrSourceMsg,
 BSTR bstrAlgorithm,
 BSTR *pbstrSignature)

描述:

根据指定的算法(支持 SHA-1, SHA256,MD-5[取决于证书对应的 CSP 是否支持])对字符串（UTF-8）进行 PKCS#7 签名（带原文）。

参数:

BSTR bstrSourceMsg[IN]-待签名的字符串，UTF-16 LE 编码格式字符串。（IE 默认是 UTF-16 LE 的编码字符串，签名之前内部会将其转换为 UTF-8 编码）

BSTR bstrAlgorithm[IN]-签名算法。SHA-1，SHA-256，MD-5

BSTR* pbstrSignature[OUT, RETVAL] -PKCS#7 签名(带原文)，Base64 编码格式字符串（UTF-16 LE 编码）

GetLastErrorDesc

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

4 安装证书链

导入 CFCA 在用的生产及测试所用的 RSA 证书链(但不包含 863CA 对应证书链)。