农校对接平台证书应用工具包
接口使用手册

中国金融认证中心

2013 年 **12** 月 **19** 日

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. 文档描述

该文档主要描述接口的定义以及使用，帮助使用者了解接口的调用方式。由于工具包组件的主要用于网页调用，因此示例代码中以 javascript 语言编写。

2. 功能描述

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)

2.3 控件 ID

X86: clsid:4AB61763-2A77-4044-966B-4589F676E8A9

X64: clsid:054AFC85-2FEA-488F-8BE4-824EBF55907A

2.4 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。

2.5 示例代码

见 Demo