CFCA

华夏网银系统安全控件
使用手册

（版本：3.3.0.2）

中国金融认证中心

2021 年 1 月 2 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
3.3.0.1	创建文档	2017/08/31	马超	任新海
3.3.0.2	增加 SM3 接口，升级控件到最新版	2021/01/04	邓英灿	任新海
3.3.0.3	新增 Edge 扩展控件	2023/1/31	马峥	任新海

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

第一章 项目范围

1. 项目描述

该文档描述华夏网银系统应用级标准版安全控件密码保护的范围以及如何使用密码控件。

2. 项目背景

华夏网银系统应用级标准版安全控件是为最大限度的保护用户密码安全而开发的密码保护安全输入控件。

3. 项目目标

实现反键盘扫描，反消息捕获，反键盘钩子，反调试，软键盘和密码加密功能的 ActiveX 安全控件和 NPAPI 安全控件。COM 插件需支持 Windows 操作系统下的 IE6 以及以上版本浏览器版本。

第二章 环境

1. 操作系统

控件支持以下操作系统

- Windows XP x86
- Windows Vista (x86/x64)
- Windows 7 (x86/x64)
- Windows 8 (x86/x64)
- Windows 10 (x86/x64)
- Windows Server 2003(需更新到 KB968730 版本以上)
- Windows Server 2008 (x86/x64)

支持浏览器平台：

IE 6.0 及以上版本 IE 浏览器

Firefox v52 以下、Chrome v12-v45、Opera v12-v37 的非 IE 浏览器

第三章 安全控件的接口使用

1. 初始化参数说明

控件初始化参数信息包含如下：

1. ObjectID：控件的 ID，在控件回调 javascript 函数的时候用来确认是哪个控件调用了 javascript 函数。
2. MaxLength：密码的最大长度限制数。
3. MinLength：密码的最小长度限制数。
4. CipherType：算法类型，0：RSA， 1：SM2。
5. CapsLockTip：检测到大写锁定按键按下时是否使用气泡提示。默认提示。0：提示大写锁定，1：不提示。
6. BorderWidth：控件边框宽度，默认值为 1，设置为 0 则没有边框。
7. BorderColor：控件边框颜色设置参数，需要同时设置控件边框默认颜色与焦点在控件之上（即控件被选中时的颜色）。格式如下：“#CCEEFF|#FF0”。两个颜色均为标准 CSS 颜色格式，中间使用“|”分隔。前面的颜色为普通显示的颜色，后面的颜色为控件被选中时的颜色。不设置此参数时边框正常状态默认颜色为#D9D9D9，默认焦点在边框之上时颜色为#4D90FE。
8. BackgroundColor：控件背景色设置参数，需要同时设置控件默认颜色与焦点在控件之上（即控件被选中时的颜色）。格式如下：“#CF9|#BBFF66”。两个颜色均为标准 CSS 颜色格式，中间使用“|”分隔。前面的颜色为普通显示的颜色，后面的颜色为控件被选中时的颜色。
9. IntensityRegExp：输入密码复杂度判断正则表达式。
10. RestrictRegExp：允许输入字符集正则表达式。
11. ServerRandom：服务器端产生的随机数，BASE64 编码格式。

2. 对外提供的接口说明

HRESULT GetVersion(LONG *plVersion)

函数描述：

获得安全控件版本信息。

参数描述：

Long *plVersion：[OUT] 返回版本信息。

用法：

var version = SecEditBox.GetVersion ();

HRESULT Clear()

函数描述：

清除安全控件存储密码信息。

参数描述：

无。

用法：

SecEditBox.Clear ();

HRESULT GetValue(BSTR *pbstrEncryptedData)

函数描述：

获得安全控件输入密码加密结果。

参数描述：

BSTR *pbstrEncryptedData：[OUT] 返回输入密码加密结果。

用法：

var EncryptedPassword = SecEditBox.GetValue();

HRESULT GetLengthIntensity(VARIANT_BOOL* pbLengthIntensity)

函数描述：

判断输入的密码长度是否复合要求。

参数描述：

VARIANT_BOOL *pbLengthIntensity：[OUT] 返回输入的密码长度是否符合要求。False：不符合，True：符合。

用法：

var PasswordLengthIntensity = SecEditBox.GetLengthIntensity();

HRESULT GetComplexIntensity(VARIANT_BOOL* pbComplexIntensity)

函数描述：

判断输入的密码复杂度是否符合要求。

参数描述：

VARIANT_BOOL* pbComplexIntensity：[OUT] 返回输入的密码复杂度是否符合要求。False：不符合，True：符合。

用法：

var PasswordComplexIntensity = SecEditBox.GetComplexIntensity();

HRESULT GetClientRandom (BSTR *pbstrClientRandom)

函数描述：

获得客户端随机数值。

参数描述：

BSTR *pbstrClientRandom：[OUT] 返回客户端随机数值，该数据使用加密公钥进行加密，并用 Base64 编码后的结果。

用法：

var ClientRandom = SecEditBox. GetClientRandom ();

HRESULT GetPasswordStrength(LONG *plPasswordStrength)

函数描述：

获得输入密码强度信息。

参数描述：

LONG *plStrength：[OUT] 返回密码强度。1 －弱，2 －中，3 －强。

关于密码强度的定义：数字、小写字母、大写字母或符号，只有其中的一种，强度为弱；有其中的两种，强度为中；三种或者以上的，强度为强。

用法：

var PasswordStrength = SecEditBox.GetPasswordStrength();

HRESULT IsWeakPassword (VARIANT_BOOL *pbIsWeakPassword)

函数描述：

获得输入密码是否为弱密码库中的密码。

参数描述：

VARIANT * pbIsWeakPassword：[OUT] 返回弱密码库的判断结果。true - 弱密码库的密码，false －非弱密码库的密码。

关于弱密码库的定义：弱密码库一般指键盘上连续按键组成的密码。

用法：

var IsWeakPassword = SecEditBox.IsWeakPassword ();

HRESULT GetNetInfo(BSTR *pbstrNetInfo)

函数描述：

获得用户网卡信息。

参数描述：

BSTR *pbstrNetInfo：[OUT] 返回用户 MAC 地址和 IP 地址。

用法：

var NetInfo = SecEditBox.GetNetInfo ();

HRESULT SM3HashData(BSTR bstrIn, BSTR bstrRand, BSTR bstrCert, BSTR *pbstrOut)

函数描述：

对原文及随机数据进行哈希计算，哈希原文为：“原文” + “随机数”；若

随机数为 NULL 或随机数长度为 0，则哈希原文为：“原文”。

若 Base64 编码公钥证书为 NULL，则计算不带 Z 值的哈希；否则为带 Z 值的。。

参数描述：

BSTR * bstrIn[IN]：原文；

BSTR * bstrRand[IN]：随机数；

BSTR * bstrCert[IN]：Base64 编码的 SM2 公钥证书（不含头尾），可以为 NULL；

BSTR * pbstrOut[OUT]：接收 SM3 哈希结果的 Buffer，为 Base64 编码。

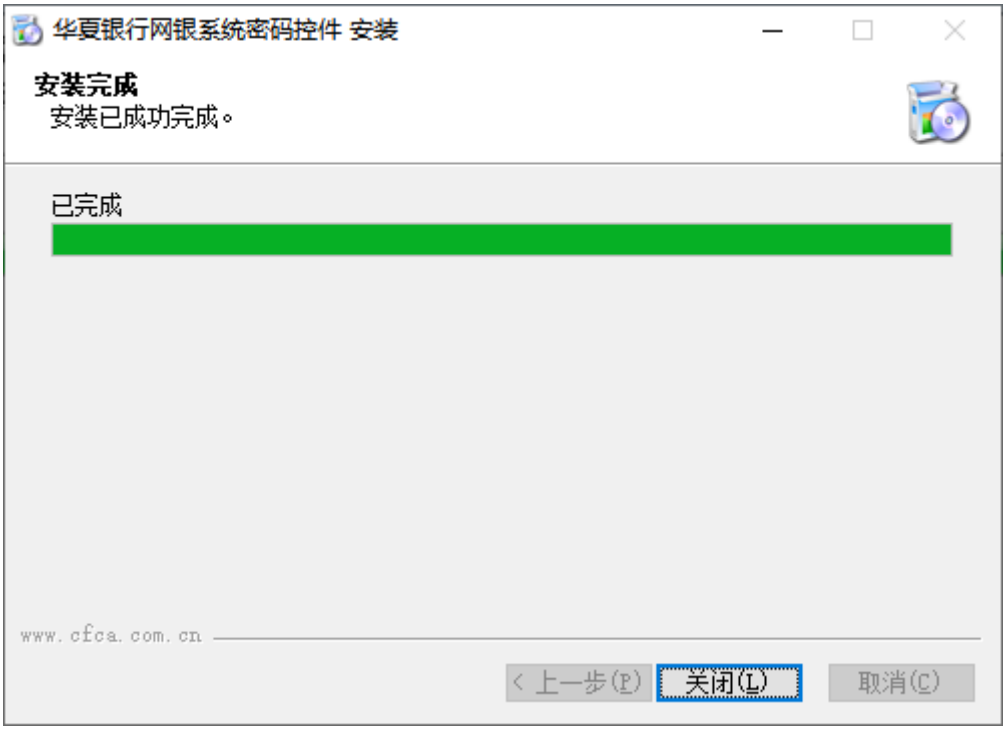
用法：

var SM3Hash= SecEditBox. SM3HashData(“input”,”123456”,””);

第四章 插件安装

1. 安装

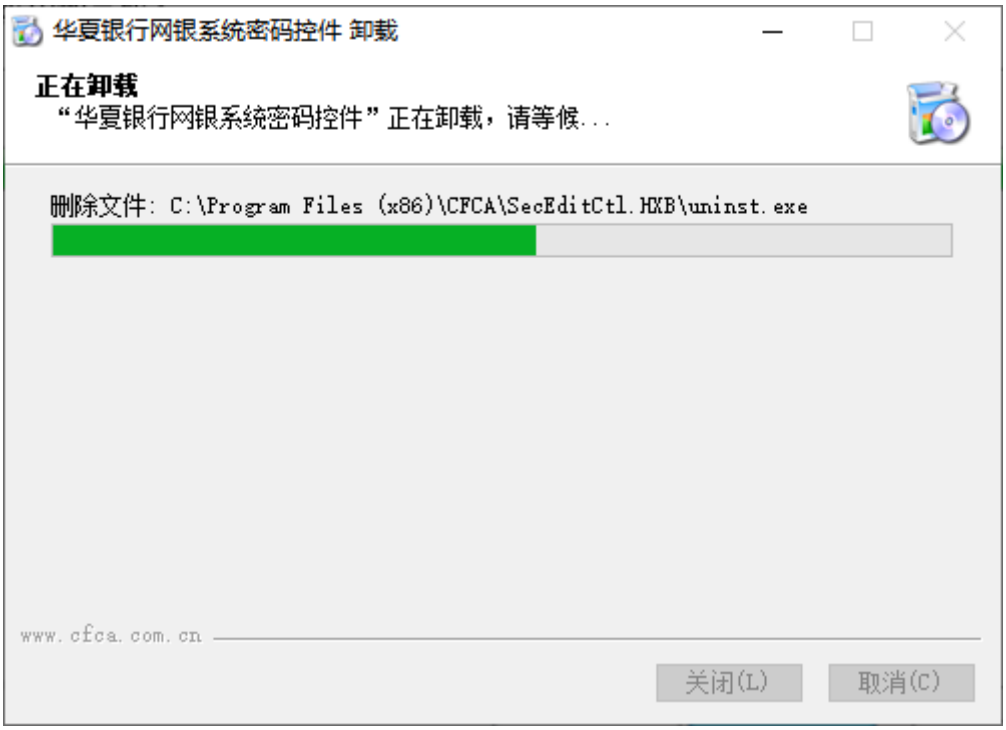
双击 SecEditCtlAllSetup.HXB.exe 安装程序进行安装。安装包支持 IE 平台 32 位和 64 位系统组件、非 IE 平台 32 位系统组件、Edge 扩展部分的安装。



2. 卸载

从默认安装目录找到卸载程序，点击卸载 uninst.exe 完成卸载。

默认安装目录为“C:\Program Files (x86)\CFCA\SecEditCtl.HXB”。



第五章 接口说明

在加载插件的同时通过参数指定插件的属性，Javascript 接口调用参数调用示例：

```
if (window.navigator.cpuClass == "x86") {

                document.getElementById("FakeSecEditBox1").innerHTML =
"<object id=\"SecEditBox1\" codebase=\"SecEditCtl.HXB.x86.cab\"
classid=\"clsid:6B8935F2-AF81-45e8-850B-2100FE454E31\" width=\"240\"
height=\"29\"><param name=\"ObjectID\" value=\"SecEditBox1\"><param
name=\"MinLength\" value=\"4\"/><param name=\"MaxLength\" value=\"12\"/><param
name=\"CipherType\" value=\"0\"><param name=\"CapsLockTip\"
value=\"0\"><param name=\"BorderWidth\" value=\"3\"><param
name=\"BorderColor\" value=\"#CCEEFF|#FF0\"><param name=\"BackgroundColor\"
value=\"#0F0|#0D0\"><param name=\"IntensityRegExp\"
value=\"(^[!-~]*[A-Za-z]+[!-~]*[0-9]+[!-~]*$)|(^[!-~]*[0-9]+[!-~]*[A-Za-z]+[!-~]*$)\"/><para
m name=\"RestrictRegExp\" value=\"([!-~]+)\"><param name=\"ServerRandom\"
value=\"MDEyMzQ1Njc4OWFiY2RlZg==\"/></object>";

                document.getElementById("FakeSecEditBox2").innerHTML =
"<object id=\"SecEditBox2\" codebase=\"SecEditCtl.HXB.x86.cab\"
classid=\"clsid:6B8935F2-AF81-45e8-850B-2100FE454E31\" width=\"240\"
height=\"29\"><param name=\"ObjectID\" value=\"SecEditBox2\"><param
name=\"MinLength\" value=\"4\"/><param name=\"MaxLength\" value=\"12\"/><param
name=\"CipherType\" value=\"1\"><param name=\"CapsLockTip\"
value=\"0\"><param name=\"BorderWidth\" value=\"3\"><param
name=\"BorderColor\" value=\"#CCEEFF|#FF0\"><param name=\"BackgroundColor\"
value=\"#0F0|#0D0\"><param name=\"IntensityRegExp\"
value=\"(^[!-~]*[A-Za-z]+[!-~]*[0-9]+[!-~]*$)|(^[!-~]*[0-9]+[!-~]*[A-Za-z]+[!-~]*$)\"/><para
m name=\"RestrictRegExp\" value=\"([!-~]+)\"><param name=\"ServerRandom\"
value=\"MDEyMzQ1Njc4OWFiY2RlZg==\"/></object>";

                }

                else {

                document.getElementById("FakeSecEditBox1").innerHTML =
"<object id=\"SecEditBox1\" codebase=\"SecEditCtl.HXB.x64.cab\"
classid=\"clsid:23D904EC-B7B8-4F44-8B6B-387615554938\" width=\"240\"
height=\"29\"><param name=\"ObjectID\" value=\"SecEditBox1\"><param
```

name=\"MinLength\" value=\"4\"/><param name=\"MaxLength\" value=\"12\"/><param name=\"CipherType\" value=\"0\"><param name=\"CapsLockTip\" value=\"0\"><param name=\"BorderWidth\" value=\"3\"><param name=\"BorderColor\" value=\"#CCEEFF|#FF0\"><param name=\"BackgroundColor\" value=\"#0F0|#0D0\"><param name=\"IntensityRegExp\" value=\"(^[!-~]*[A-Za-z]+[!-~]*[0-9]+[!-~]*$)|(^[!-~]*[0-9]+[!-~]*[A-Za-z]+[!-~]*$)\"/><param name=\"RestrictRegExp\" value=\"([!-~]+)\"><param name=\"ServerRandom\" value=\"MDEyMzQ1Njc4OWFiY2RlZg==\"/></object>";

document.getElementById("FakeSecEditBox2").innerHTML = "<object id=\"SecEditBox2\" codebase=\"SecEditCtl.HXB.x64.cab\" classid=\"clsid:23D904EC-B7B8-4F44-8B6B-387615554938\" width=\"240\" height=\"29\"><param name=\"ObjectID\" value=\"SecEditBox2\"><param name=\"MinLength\" value=\"4\"/><param name=\"MaxLength\" value=\"12\"/><param name=\"CipherType\" value=\"1\"><param name=\"CapsLockTip\" value=\"0\"><param name=\"BorderWidth\" value=\"3\"><param name=\"BorderColor\" value=\"#CCEEFF|#FF0\"><param name=\"BackgroundColor\" value=\"#0F0|#0D0\"><param name=\"IntensityRegExp\" value=\"(^[!-~]*[A-Za-z]+[!-~]*[0-9]+[!-~]*$)|(^[!-~]*[0-9]+[!-~]*[A-Za-z]+[!-~]*$)\"/><param name=\"RestrictRegExp\" value=\"([!-~]+)\"><param name=\"ServerRandom\" value=\"MDEyMzQ1Njc4OWFiY2RlZg==\"/></object>";

}

}

else {

document.getElementById("FakeSecEditBox1").innerHTML = "<object id=\"SecEditBox1\" type=\"application/npSecEditCtl.HXB.x86\" width=\"240\" height=\"29\"><param name=\"MinLength\" value=\"4\"/><param name=\"ObjectID\" value=\"SecEditBox1\"><param name=\"MaxLength\" value=\"12\"/><param name=\"CipherType\" value=\"0\"><param name=\"CapsLockTip\" value=\"0\"><param name=\"BorderWidth\" value=\"3\"><param name=\"BorderColor\" value=\"#CCEEFF|#FF0\"><param name=\"BackgroundColor\" value=\"#0F0|#0D0\"><param name=\"IntensityRegExp\" value=\"(^[!-~]*[A-Za-z]+[!-~]*[0-9]+[!-~]*$)|(^[!-~]*[0-9]+[!-~]*[A-Za-z]+[!-~]*$)\"/><param name=\"RestrictRegExp\" value=\"([!-~]+)\"><param name=\"ServerRandom\" value=\"MDEyMzQ1Njc4OWFiY2RlZg==\"/></object>";

```
document.getElementById("FakeSecEditBox2").innerHTML = "<object id=\"SecEditBox2\" type=\"application/npSecEditCtl.HXB.x86\" width=\"240\" height=\"29\"><param name=\"ObjectID\" value=\"SecEditBox2\"><param name=\"MinLength\" value=\"4\"/><param name=\"MaxLength\" value=\"12\"/><param name=\"CipherType\" value=\"1\"><param name=\"CapsLockTip\" value=\"0\"><param name=\"BorderWidth\" value=\"3\"><param name=\"BorderColor\" value=\"#CCEEFF|#FF0\"><param name=\"BackgroundColor\" value=\"#0F0|#0D0\"><param name=\"IntensityRegExp\" value=\"(^[!-~]*[A-Za-z]+[!-~]*[0-9]+[!-~]*$)|(^[!-~]*[0-9]+[!-~]*[A-Za-z]+[!-~]*$)\"/><param name=\"RestrictRegExp\" value=\"([!-~]+)\"><param name=\"ServerRandom\" value=\"MDEyMzQ1Njc4OWFiY2RlZg==\"/></object>";
}
```

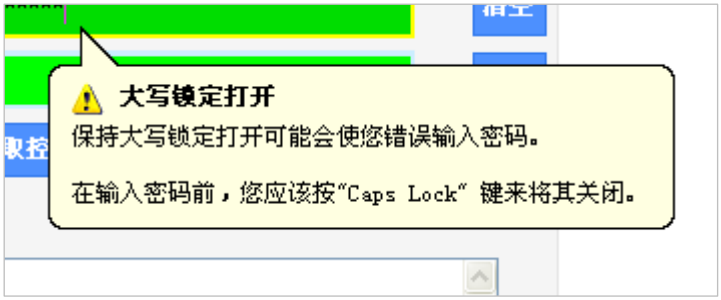
获取密码长度匹配结果、密码字符的正则表达式匹配结果、加密后的密码以及客户端随机数：

```
Version = SecEditBox.GetVersion();
PasswordLengthIntensity = SecEditBox.GetLengthIntensity();
PasswordComplexIntensity = SecEditBox.GetComplexIntensity();
EncryptedPassword = SecEditBox.GetValue();
ClientRandom = SecEditBox.GetClientRandom();
PasswordStrength= SecEditBox. GetPasswordStrength ();
```

第六章 Demo 使用说明

1. 客户端 HTML 页面操作

浏览器界面密码输入大写锁定打开提示：



浏览器界面加密信息显示：

2. 服务器 JAVA 程序调用

java 程序调用示例：

RSA 解密

java -jar Decrypt.jar rsa1024_11111111.pfx 11111111 JWofy7/epOGxiG5/3kyV/2xnX7NKv/t65Z2iO6/fnXNpe48sRjQIgRC2XOmUwZqZnaII6

Xp7kTK1Yx8gAGcUJIONhB+amFqb6V8P/4Ah9npxD26P4Vs91Ln/m6XFrkRYimHnS LoJahIFFBmiu3Zrcu3Pz4vK9xIIGK9aE3XKEM0= MDEyMzQ1Njc4OWFiY2RlZg== YC5ApZQgzwYXGtTMeilNqA== 1

Parameters explain:

para 1-pfx path

para 2-pfx password

para 3-RSA Encrypted Data(RandomKey which is got from client)

para 4-ServerRandomKey

para 5-3DES Encrypted Data(Value property returns this data from client)

para 6-CipherType

SM2 解密

java -jar Decrypt.jar SM2_TEST_PRIKEY.key 0 bIEzvfPMCfqXl9EgBGdzeTf3mZHvUxI7rKnYvB/vUFy9wLquJ78jF3RHyH47k3bCHG Kq2OZJwAt5bnhmdNrQGKte6FmRHSAYaNzs7qkW77UxB3OYxpfHJLpJ0S684rhjiZd wjhhytnroPUVSGnI1/w== MDEyMzQ1Njc4OWFiY2RlZg== D147Sryb8jvCdvXuOvjuTw== 0

Parameters explain:

para 1-pfx path

para 2-pfx password

para 3-SM2 Encrypted Data(RandomKey which is got from client)

para 4-ServerRandomKey

para 5-SM4 Encrypted Data(Value property returns this data from client)

para 6-CipherType