

上海农商行村镇银行安全控件

软件说明书

（版本：3.3.0.1）

中国金融认证中心

2022年5月11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 |
| 3.3.0.1 | 创建文档 | 2022/5/11 | 邓英灿 | 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](#_Toc74821024)

[1. 项目描述 1](#_Toc74821025)

[2. 项目背景 1](#_Toc74821026)

[3. 项目目标 1](#_Toc74821027)

[第二章 环境 1](#_Toc74821028)

[1. 操作系统 1](#_Toc74821029)

[2. 信任站点 2](#_Toc74821030)

[第三章 控件功能描述 2](#_Toc74821031)

[1. 概述 2](#_Toc74821032)

[第四章 接口使用 4](#_Toc74821033)

[1. 安全控件初始化参数说明 4](#_Toc74821034)

[1.1 IE和非扩展方式的非IE浏览器 5](#_Toc74821035)

[1.2 扩展方式的浏览器 5](#_Toc74821036)

[2. 安全控件对外提供接口说明 6](#_Toc74821037)

# 项目范围

## 项目描述

该文档描述上海农商行村镇银行密码安全保护控件的需求说明。

## 项目背景

上海农商行村镇银行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。

## 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。以及Chrome、Firefox和Edge浏览器的部分版本。

# 环境

## 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

Edge（Chromium内核）

## 信任站点

<http://10.20.155.37>

[http://\*.srcbcz.com](http://*.srcbcz.comhttps://*.srcbcz.com)

[https://\*.srcbcz.com](http://*.srcbcz.comhttps://*.srcbcz.com)

# 控件功能描述

## 概述

上海农商行村镇银行密码控件RSA加密方式加密逻辑如下：

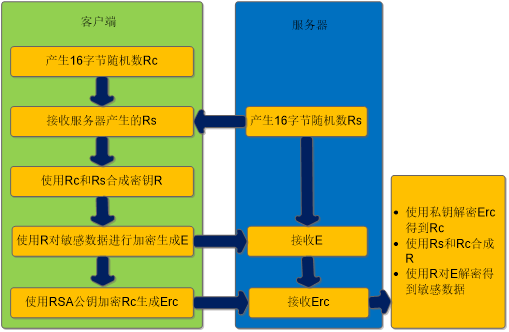


图 3‑1 客户端与服务器通信流程

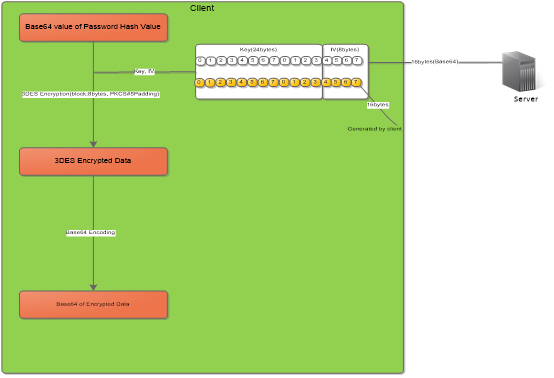


图 3‑2 客户端对敏感数据进行3DES加密流程

客户端产生16字节随机数Rc，服务器产生16字节随机数Rs。取Rs的前12字节在前以及Rc的前12字节在后，组成24字节的对称密钥R。取Rs的后4字节在前以及Rc的后4字节在后，组成8字节作为初始向量。以8字节为加密单位块长度、PKCS#5 填充模式对密码使用3DES加密。

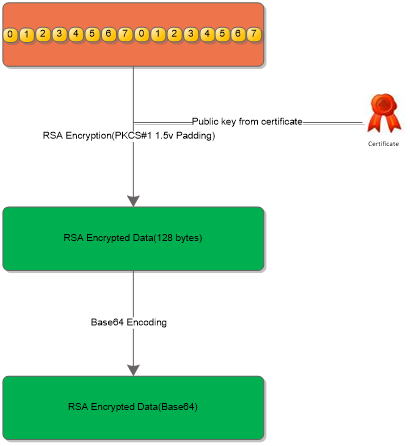


图 3‑3 客户端对对称密钥使用RSA公钥进行加密流程

使用RSA公钥对客户端产生的随机数Rc进行加密，再进行Base64编码后传给服务器。

SM2的普通加密方式与RSA加密方式相比稍有变动，区别如下：

针对输入密码进行的对称加密处理，客户端产生16字节随机数Rc，服务器产生16字节随机数Rs。取Rs的前8字节在前以及Rc的前8字节在后，组成16字节的对称密钥R。取Rs的后8字节在前以及Rc的后8字节在后，组成16字节作为初始向量。进行SM4的CBC的标准对称加密。

使用SM2公钥对客户端产生的随机数Rc进行加密，再进行Base64编码后传给服务器。

# 接口使用

## 安全控件初始化参数说明

### IE和非扩展方式的非IE浏览器

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。

### 扩展方式的浏览器

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. IntensityRegExp：输入密码复杂度判断正则表达式。
6. RestrictRegExp：允许输入字符集正则表达式。
7. ServerRandom：服务器端产生的随机数，BASE64编码格式。

扩展版本的控件在界面显示为 input type=\"password\" 类型，所以界面显示效果相关设置参考HTML中的 input password类型相关参数即可。

在扩展版本中，不支持CapsLockTip参数，但是控件提供了GetKeyState()函数，返回状态即为Caps Lock的状态。使用方式详见测试网页。

## 安全控件对外提供接口说明

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。0 - 弱密码，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。返回值为0说明密码为弱密码库中的密码。

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 ();



# 