移动数字证书

Windows 版用户手册

版本：M-4.0

适用硬件：M4

深圳证券数字证书认证中心

http://ca.szse.cn

目　　录

1.物品清单

包装盒内物品清单如下：

1. 移动数字证书
2. 用户手册
3. 合格证
4. 挂绳

2.软件安装

2.1 适用平台

移动数字证书支持下列操作系统：

- ✓ Windows 2000（32 位）
- ✓ Windows XP（32/64 位）
- ✓ Windows 2003（32/64 位）
- ✓ Windows 2008（32/64 位）
- ✓ Windows Vista（32/64 位）
- ✓ Windows 7（32/64 位）
- ✓ Windows8(32/64 位)
- ✓ Windows10(32/64 位)

2.2 注意事项

在开始安装移动数字证书相关软件之前，需保证满足以下要求（本手册中，“EKey”与“移动数字证书”意义相同）：

- ✓ 操作系统为产品支持的版本(请参见“2.1 适用平台”)。
- ✓ 浏览器版本为 Internet Explorer 6.0 或以上版本。
- ✓ 电脑上带有至少一个 USB 接口，并且在 CMOS 设置中将 USB 支持功能打开。
- ✓ 可选用 USB 延长线或 USB Hub。
- ✓ **在“明华 EKey 管理工具”安装完成之前，请确认已经拔下您电脑上的全部 EKey。**
- ✓ **在 win7、win8、win10 系统上安装驱动程序时，建议鼠标右键点击驱动程序，点击“以管理员身份运行(A)”安装驱动程序 SZSE_Install_Package.exe，否则根证书可能无法正确安装。**

2.3 安装过程

1、打开深交所官网明华驱动下载地址：http://ca.szse.cn/UpFiles/ca/EKey-M4.zip，下载驱动，驱动下载完成后，双击“SZSE_Install_Package.exe”安装程序。如果出现如图 2-1 所示窗口，请输入管理员的用户名和密码，点“确定”进入下一步；否则，将直接跳至第 2 步。

图 2-1

2. 弹出如图 2-2 所示窗口：

图 2-2

2、请确认已经拔下您电脑上的全部 EKey，点击“安装”，出现如图 2-2 所示窗口：

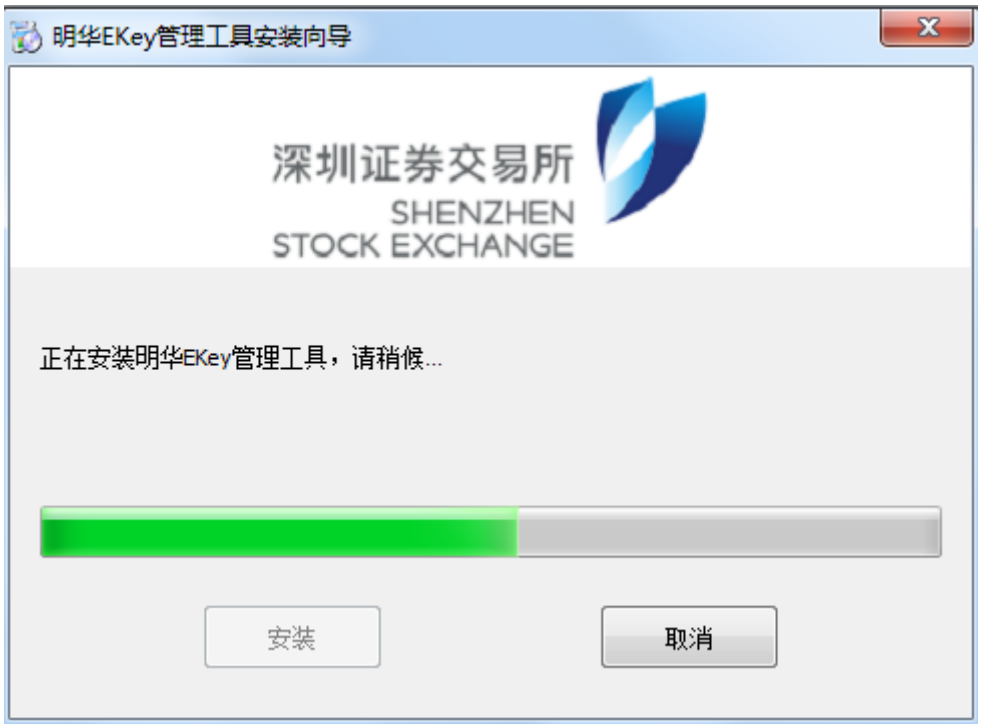

图 2-3

8、安装完成后，出现如图 2-3 所示窗口，点击“完成”，结束安装。

此时，桌面会生成“明华 EKey 管理工具”快捷方式；程序菜单会生成路径为“开始→所有程序→明华 EKey 管理工具→ 明华 EKey 管理工具”的菜单。

电脑每次开机时，都会自动运行“明华 EKey 管理工具”，无需手工启动。

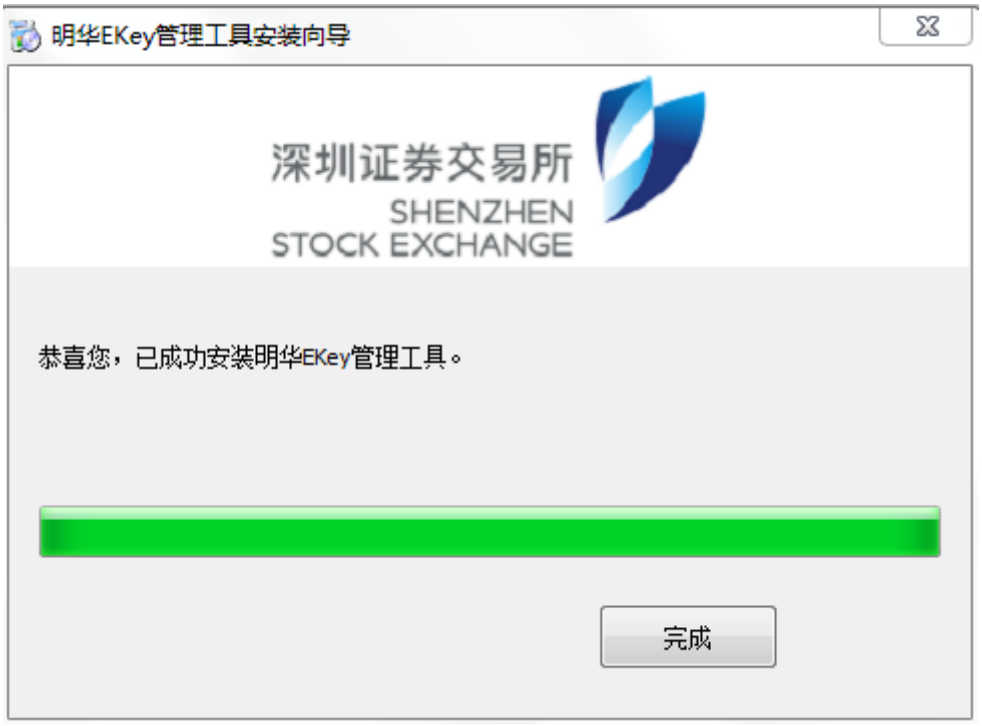

图 2-4

3. 证书使用

3.1 与电脑相连

可以使用以下两种方式：

1、拔下移动数字证书的帽盖，直接插在电脑的 USB 接口上，移动数字证书尾部的灯亮，表示移动数字证书与电脑的连接正常。

2、将 USB 延长线插在电脑的 USB 接口上，拔下移动数字证书的帽盖，将移动数字证书插在 USB 延长线上，移动数字证书尾部的灯亮，表示移动数字证书与电脑的连接正常。

3.2 证书状态查询

证书状态查询需要插入移动数字证书，并通过打开“明华 EKey 管理

工具”进行查看。“明华 EKey 管理工具”在操作系统启动后自动运行，管理工具的图标 显示在 Windows 窗口状态栏的右下角中。双击图标 可以打开管理工具主窗口。

当移动数字证书与电脑相连以后，打开“明华 EKey 管理工具”，显示如下图（如图 3-1 所示）所示信息，则移动数字证书处于正常状态。

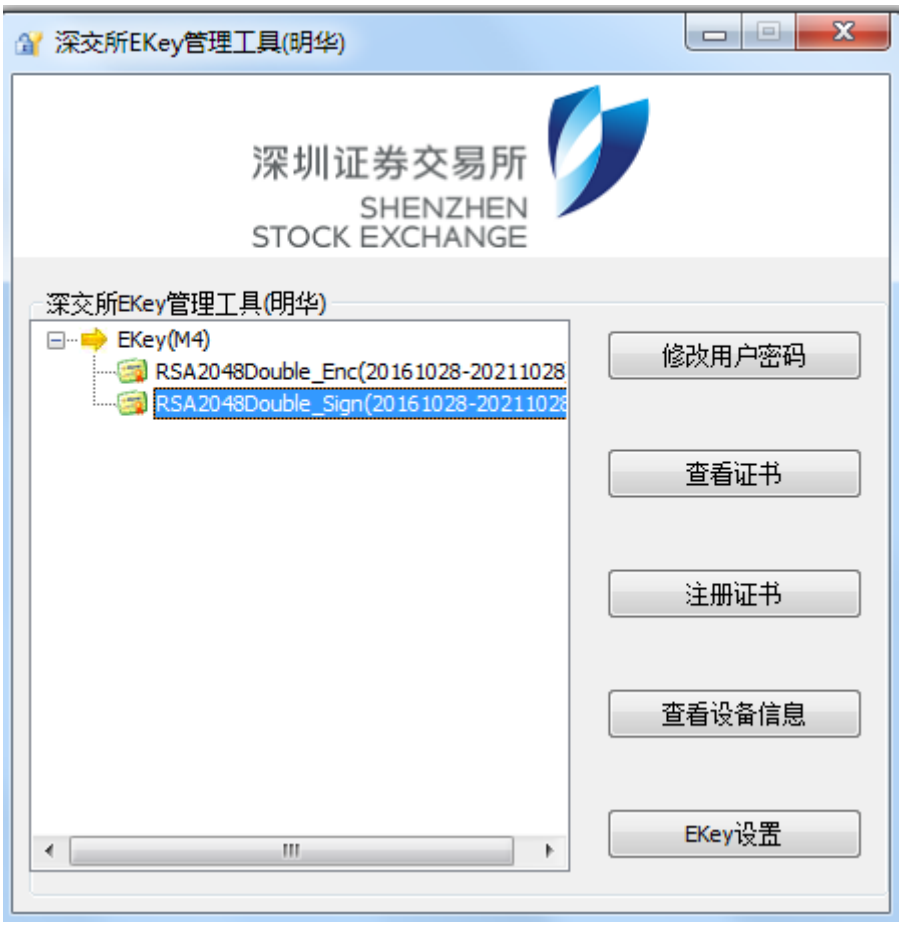

图 3-1

3.3 软件窗口简介

“明华 EKey 管理工具”包括“修改用户密码”、 “查看证书”、“注册证书”、“查看设备信息”、“EKey 设置”功能按钮，窗口如图 3-2 所示。

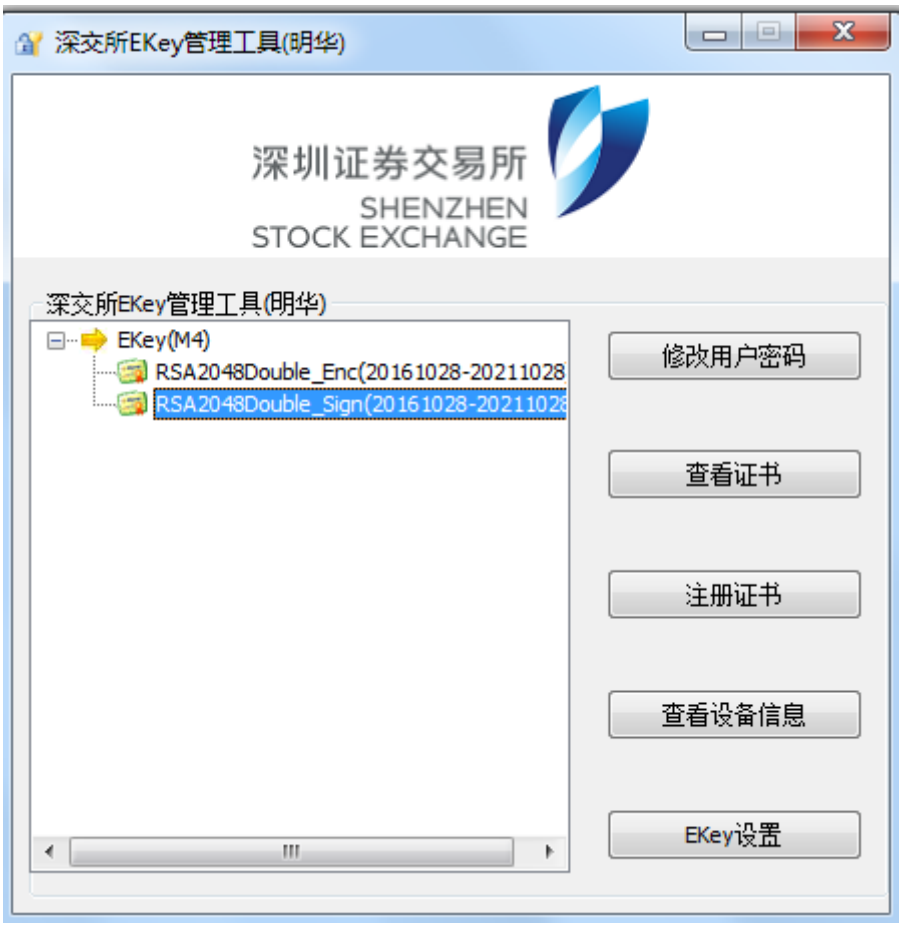

图 3-2

窗口分为两个部份：

1、设备清单：

显示与电脑相连的移动数字证书，及该移动数字证书是否已有证书等信息。

2、功能按钮：

“修改用户密码”：修改移动数字证书的用户密码。

“查看证书”：查看证书详细信息。

“注册证书”：将 EKey 里的证书注册到 Windows 系统证书存储区。

“查看设备信息”：查看电脑操作系统信息、IE 浏览器版本、管理工具版本、EKey 连接状态、EKey 类型、EKey 序列号、EKey 密码重试次

数。

“EKey 设置”：设置插入 EKey 时，是否自动打开指定网址（该网址可修改）；拔出移动数字证书时，是否显示关闭 IE 窗口提示框。

3.4 标准功能

3.4.1 修改用户密码

功能：将移动数字证书原用户密码修改为新密码，步骤如下：

1、将移动数字证书插在电脑的 USB 接口（或 USB 延长线接口）上，移动数字证书上的指示灯闪亮表示工作正常。

2、点击“修改用户密码”按钮，出现修改用户密码的窗口，如图 3-3 所示：

图 3-3

3、输入原密码、新密码，密码可为 4~16 位字符，如图 3-4 所示：

图 3-4

4、点击“确认”按钮。

如果原用户密码校验通过，则修改用户密码成功，新用户密码将取代原用户密码，如图 3-5 所示：

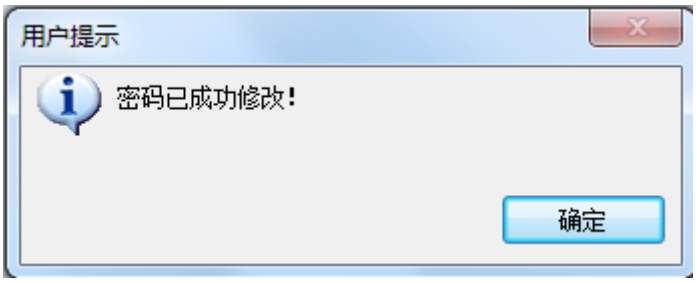

图 3-5

如果原用户密码校验出错，或两次输入的新用户密码不一致，则提示用户密码修改失败，如图 3-6 所示：

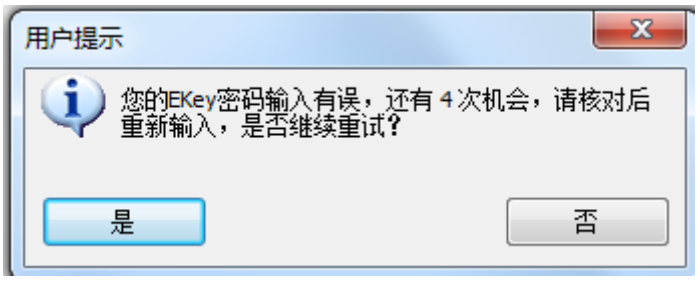

图 3-6

注意：当用户密码修改连续失败次数达到 5 次时，数字证书将被锁死。

3.4.2 查看证书

功能：查看移动数字证书中证书的详细内容。步骤如下：

1、将移动数字证书插在电脑的 USB 接口（或 USB 延长线接口）上，移动数字证书上的指示灯闪亮表示工作正常。

2、点击设备清单中的证书，窗口变为如图 3-7 所示：

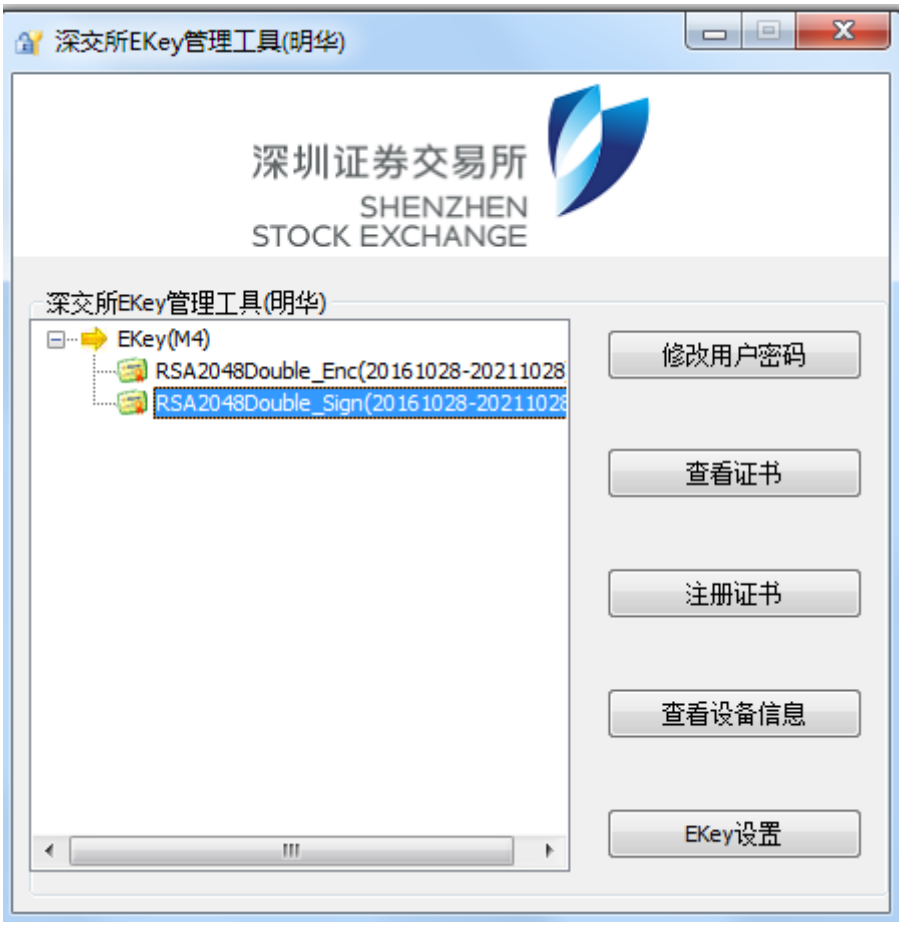

图 3-7

3、点击“查看证书”按钮，可以查看移动数字证书中该证书的详细内容，窗口如图 3-8 所示：

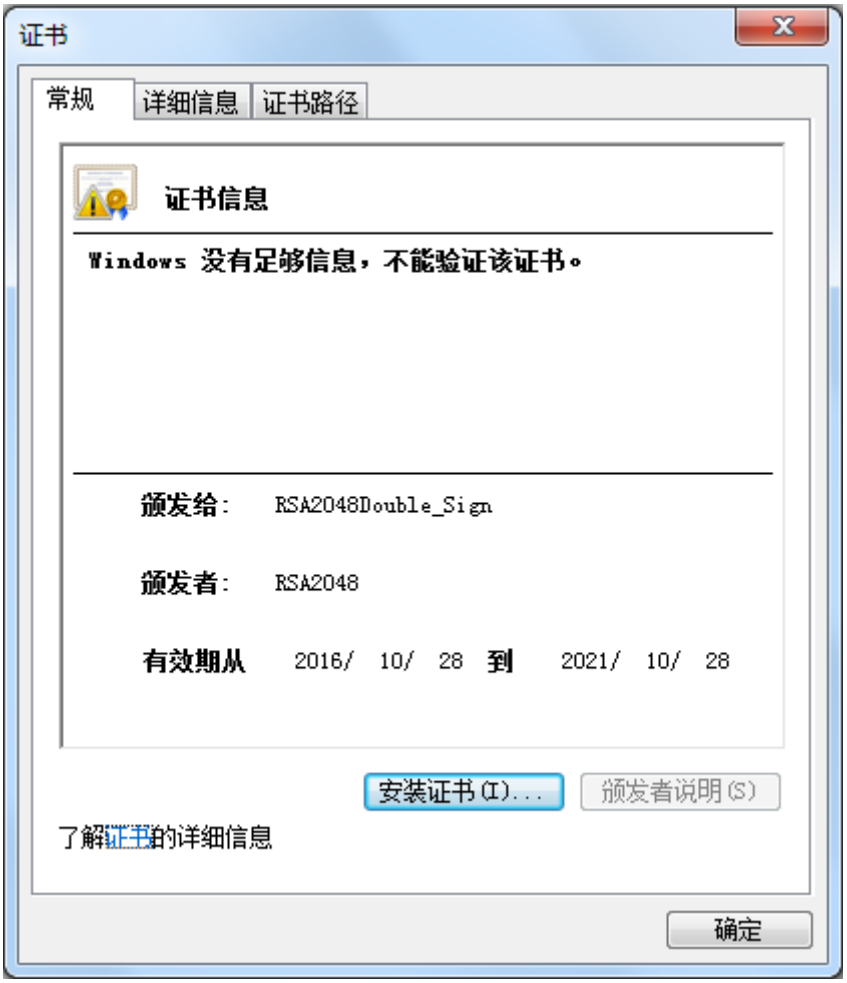

图 3-8

3.4.3 注册证书

功能：将移动数字证书中的某证书文件注册到电脑操作系统的证书存储区中。步骤如下：

1、将移动数字证书插在电脑的 USB 接口（或 USB 延长线接口）上，移动数字证书上的指示灯闪亮表示工作正常。

2、点击设备清单中的证书，选中需要注册的证书，如图 3-9 所示窗口：

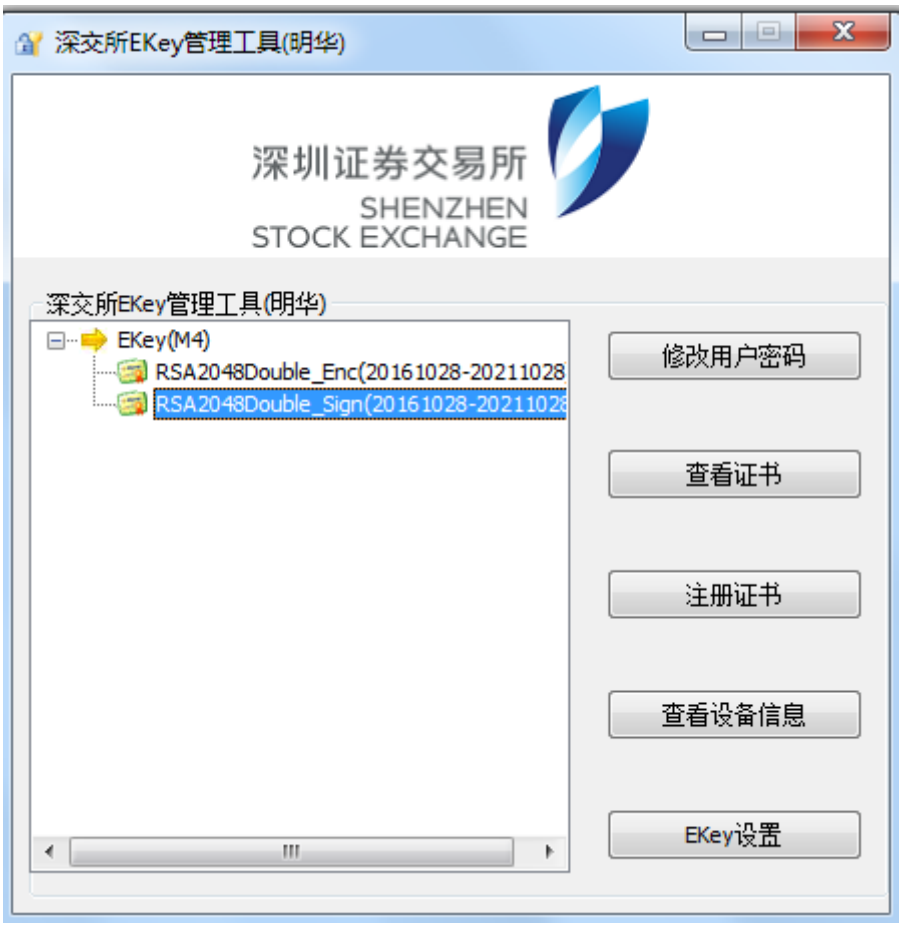

图 3-9

3、点击“注册”按钮，则弹出如图 3-10 所示窗口，证书成功注册到电脑操作系统证书存储区。

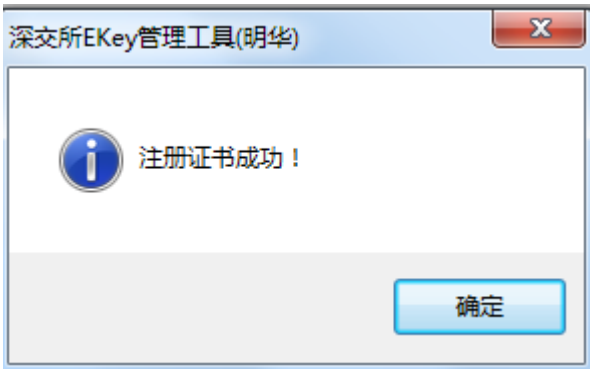

图 3-10

注意：证书存储区是电脑操作系统内部，用于保存证书、证书信任列表、证书吊销列表的系统区域。

4 **移动数字证书插好后，EKey 管理工具自动将移动数字证书中的所有**

证书注册到电脑操作系统的证书存储区中；移动数字证书拔下时，会自动将该移动数字证书中的所有证书从电脑操作系统的证书存储区中注销。

3.4.4 查看设备信息

功能：查看电脑操作系统信息、IE 浏览器版本、管理工具版本、EKey 连接状态、EKey 类型、EKey 序列号、EKey 密码重试次数。步骤如下：

1、将移动数字证书插在电脑的 USB 接口（或 USB 延长线接口）上，移动数字证书上的指示灯闪亮表示工作正常。

2、点击“查看设备信息”，显示设备相关信息，如下图 3-11 所示窗口：

图 3-11

3.4.5EKey 设置

功能：设置插入移动数字证书时，是否自动打开指定网址（该网址可修改）；拔出移动数字证书时，是否显示关闭 IE 窗口提示框。

3.4.5.1.自动打开网站

点击“EKey 设置”，出现如下图 3-12 所示窗口。

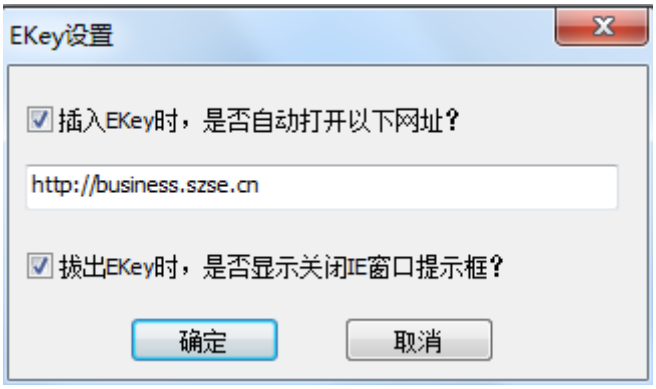

图 3-12

当勾上“插入 EKey 时，是否自动打开以下网站？”,则每次移动数字证书插入电脑时,将会自动打开 IE 浏览器并且打开设置的网站;相反，如果没有勾上，当移动数字证书插入电脑时，不会自动打开 IE 浏览器。

3.4.5.2 自动关闭 IE 窗口

点击“EKey 设置”，出现如下图 3-13 所示窗口。

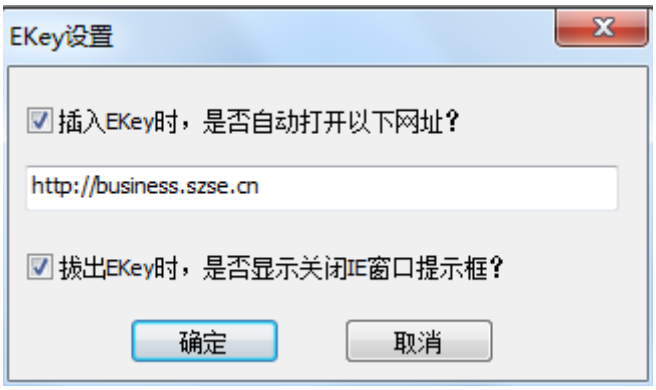

图 3-13

当勾上“拔出 EKey 时，是否显示关闭 IE 窗口提示框？”后（窗口设置如图 3-13 所示），则每次移动数字证书拔出电脑时，如果存在打开的 IE 浏览器窗口，将会自动弹出如图 3-14 所示窗口，提示是否关闭 IE 浏览器，点击“确定”按钮，将关闭所有打开的 IE 浏览器，点击“取消”按钮，则不会有任何操作；相反，如果没有勾上“拔出 EKey 时，是否显示关闭 IE 窗口提示框？”时，则不会出现如图 3-14 所示窗口。

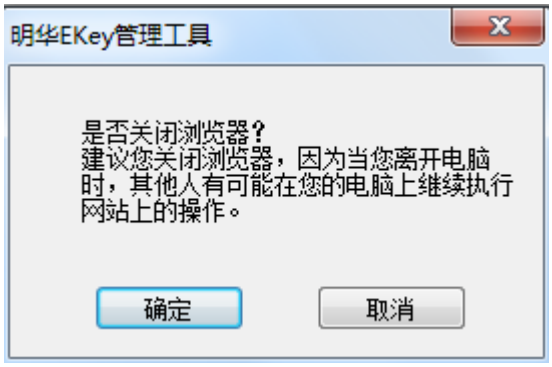

图 3-14

3.6 注意事项

- ✓ 第一次使用移动数字证书时，请立即修改用户密码，不要使用默认密码。
- ✓ 请牢记您的移动数字证书密码，不要透露给其他人。
- ✓ 每次使用完移动数字证书后，请从电脑上拔下来，并及时收妥。
- ✓ 请妥善保管好您的移动数字证书，勿借给他人使用；如有遗失，请立即与移动数字证书颁发机构联系。

4. 软件卸载

1、卸载菜单的路径为：开始→所有程序→明华 EKey 管理工具→卸载。点击“卸载”，出现如图 4-1 所示窗口：

图 4-1

2、点击“卸载”进行卸载，出现如图 4-2 所示窗口，点击“完成”按钮完成卸载。

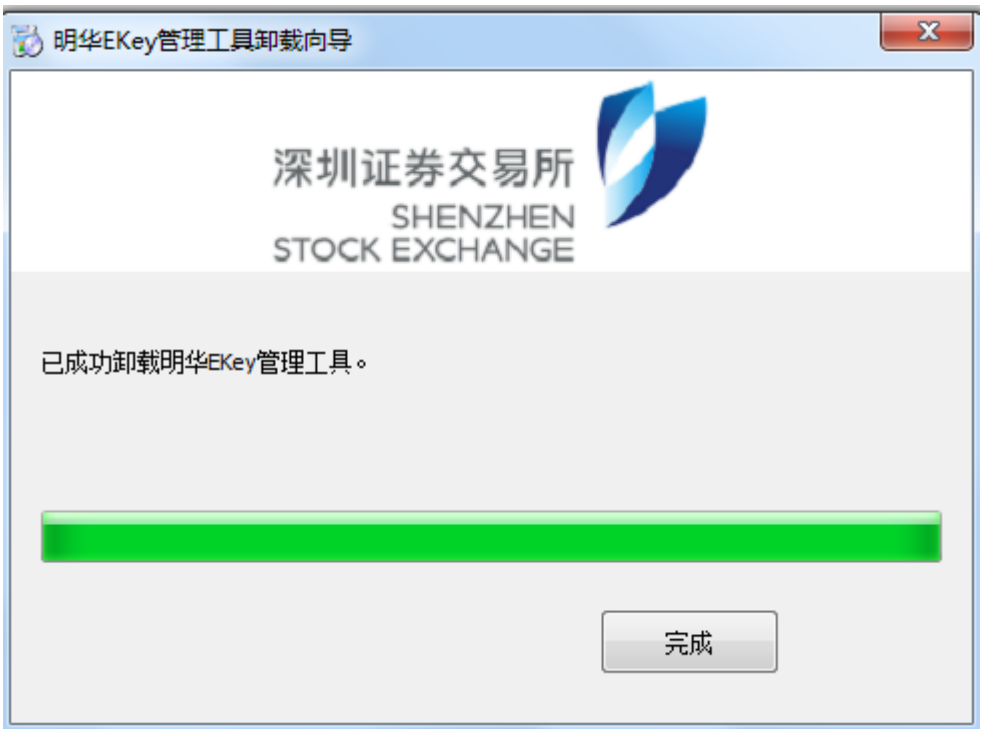

图 4-2

5. 常见问题

1. 什么是移动数字证书？为什么要使用移动数字证书？

移动数字证书是一种智能存储设备，可存储数字证书；证书硬件内有 CPU 芯片，可进行密码运算；外形小巧，可插在电脑的 USB 接口中使用。

数字证书如果存储在电脑硬盘中，则证书私钥很容易被复制、窃取，安全性差；数字证书如果存储在移动数字证书中，则证书私钥无法复制、导出，即使电脑中了木马病毒，也不会被窃取，安全性非常高。

2. 移动数字证书有什么优点？

（1）安全性高：

- 可有效防止黑客或他人盗取证书。证书一旦下载到移动数字

证书中，证书私钥无法复制、导出，因此黑客无法窃取。

- 移动数字证书有密码保护机机制，且密码连续输错次数超过 5 次，移动数字证书会自动锁死，必须要解锁后方可继续使用。
- 证书存放在移动数字证书中，不受电脑硬盘格式化、重装系统等的影响，可有效防止证书损毁和丢失。

（2）使用方便：

- 体积小，重量轻，可随身携带。
- 具有自动打开指定网站功能：每次移动数字证书插入电脑时，将会自动打开 IE 浏览器并且打开设置的网站，无需用户手工输入网址，使用方便、快捷。
- 具有自动提示关闭 IE 浏览器功能：每次移动数字证书拔出电脑时，如果存在打开的 IE 浏览器窗口，将会自动弹出提示是否关闭 IE 浏览器的窗口，无需用户手工关闭 IE 浏览器窗口，使用方便、快捷。

3. 移动数字证书的初始密码是什么？

移动数字证书的初始密码默认为“111111”。

4. 如何查看移动数字证书内证书？

可以通过移动数字证书的 EKey 管理工具查看，具体方法为：打开 EKey 管理工具，选择证书，点击“查看证书”按钮，就可以查看该证书的详细信息。

5. 移动数字证书是 U 盘吗？

不是。移动数字证书外观虽然和 U 盘差不多，都是插在电脑的 USB

接口中使用，但两者还是有很大区别：

（1）两者的作用不同。U 盘是用来存储数据的，因此容量都比较大，从几百 MB 到几 GB；而移动数字证书属于智能存储设备，主要用于存放数字证书，并可以进行密码运算，一般容量较小，只有几十 KB。

（2）U 盘中的数据可随意进行读写、复制，而数字证书一旦存放在移动数字证书中，则证书私钥无法被复制、导出，可有效防止证书被他人复制窃取，安全性非常高。

（3）移动数字证书中有 CPU 芯片，可进行密码运算，而 U 盘无此功能。

6. 移动数字证书上的灯闪烁，是否说明移动数字证书在工作？

当您把移动数字证书插入电脑后，操作系统会识别硬件。识别后，移动数字证书上的灯应该是常亮的。如果移动数字证书上的灯不亮，说明系统未识别到硬件，您需要重新插入移动数字证书，或重新安装驱动程序，如果以上两种方法都无效，则可能为移动数字证书损坏。

当您在使用移动数字证书进行证书申请或数据提交等操作时，移动数字证书会进行加密、签名等工作。此时移动数字证书上的灯也会不断闪烁，表明移动数字证书在正常工作；不再闪烁时，表明工作完成。

7. 何种情况下，移动数字证书会被锁定？

用户反复尝试移动数字证书的用户密码，超过 5 次会被锁定。

6.软件版本

（1）安装程序（中文版）版本信息

版本号：6.2.2.6

产品名称：MingWah EKey Management Tools Setup

发布日期：2016-11-08

文件名称：SZSE_Install_Package(6.2.2.6).exe

（2）Setup (English) version information

Version No.: 6.2.2.6

Product Name:MingWah EKey Management Tools Setup

Release Date: 2016-11-08

File Name: SZSE_Install_Package(6.2.2.6).exe

7.硬件规格

硬件型号	SJK1577	
型号代码	M1：	支持 RSA 1024 算法
	M2：	支持 RSA 1024/2048 算法
	M3:	支持 RSA 1024/2048 算法
	M4	支持 RSA1024/2048、SM2 算法
用户的存储空间	64KB	
数据保存期限	≥ 10 年	
存储器重写次数	≥ 10 万次	

电源	2.7 ～ 5.5 V，支持低功耗模式	
工作时钟频率	4M ～ 12M Hz	
工作温度	0℃ ～ 70℃	
存放温度	-25℃ ～ +85℃	
工作湿度	0% ～ 90% （不冷凝）	
指示灯	具有 LED 灯，用于电源指示和通讯指示	
抗静电特性	ESD ＞ 4000V	
连接接口	USB A 型接口，符合 USB 1.1/2.0 标准规范	
传输速率	全速（≥ 12 Mbps）	
COS 体系	支持 ISO7816-4/5/6/8/9 标准规范	
支持算法	M1：	RSA 1024、DES/3DES、国密 SSF33 算法、SHA-1
	M2：	RSA 1024 、 RSA 2048 、 DES/3DES、国密 SSF33 算法、SHA-1
	M3:	RSA 1024 、 RSA 2048 、 DES/3DES、国密 SSF33 算法、SHA-1
	M4:	RSA 1024 、 RSA 2048 、 DES/3DES、SSF33、SM1、SM2、

		SM3 、 SM4 、 MD5 、 SHA-1 、 SHA256、SHA384、SHA512
支持中间件	CSP 中间件、PKCS#11 中间件、SKF 中间件	
硬件真随机数发生器	支持	
数据存取速度(读操作)	≥ 20 Kbps	
数据存取速度(写操作)	≥ 10 Kbps	
密码算法：非对称加密算法	M1：	支持 RSA 1024 算法
	M2：	支持 RSA 1024/2048 算法
	M3：	支持 RSA 1024/2048 算法
	M4:	支持 RSA1024/2048、SM2 算法
RSA1024 公私钥对产生时间	≤ 1200 ms （M4 平均时间）	
RSA1024 解密/签名运算时间	≤ 64 ms（M4 平均时间）	
RSA1024 加密/验证运算时间	≤ 12 ms（M4 平均时间）	
RSA2048 公私钥对产生时间	M2：	≤ 20000 ms （平均时间）
	M3：	≤ 20000 ms （平均时间）
	M4:	≤ 12000 ms（平均时间）
RSA2048 解密/签名运算时间	M2：	≤ 1000 ms
	M3：	≤ 1000 ms
	M4:	≤ 220 ms
RSA2048 加密/验证运算时间	M2：	≤ 160 ms

	M3：	≤ 160 ms
	M4:	≤ 60 ms
SM2 解密/签名运算时间	M4:	≤ 100 ms
SM2 加密/验证运算时间	M4	≤ 180 ms
密码算法：对称加密算法	支持 DES/3DES 算法（硬件）、国密 SSF33 算法、SM4 算法	
DES/3DES 加密/解密速度	≥ 100Kbps	
国密 SSF33 加密/解密速度	≥ 15Kbps	
SM4 加密/解密速度	≥ 270Kbps	
DES/3DES 算法持续工作可用性	≥ 99.99%	
SM4 算法持续工作可用性	≥ 99.99%	
RSA 算法持续工作可用性	≥ 99.99%	
SM2 算法持续工作可用性	≥ 99.99%	
通电持续工作可用性	≥ 99.99%	