

一、适用平台

EKey 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）、Windows 8（32/64 位）、Windows 10（32/64 位）。

二、安装说明

在“深交所 EKey (M5) 管理工具”安装前，请确认已经拔下电脑上的全部 EKey。

1. 打开深交所官网 CA 服务地址：

<http://www.szse.cn/marketServices/message/ca/index.html>，进入资料下载，下载驱动程序（M5 型号），双击“SZSE_Install_Package.exe”安装程序；

2. 确认已经拔下电脑上的全部 EKey，点击“安装”；

3. 安装完成后，点击“完成”，结束安装。

三、修改密码

“深交所 EKey (M5) 管理工具”在操作系统启动后会自动运行，管理工具的图标  显示在 Windows 窗口状态栏的右下角。双击图标  可打开管理工具主窗口。

1. 将 EKey 插在电脑的 USB 接口上，EKey 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。

3. 输入原用户密码、新用户密码，密码可为 4~16 位字符

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。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。**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。**

四、注意事项

1. 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）：

1) 操作系统为产品支持的版本(请参见“一、适用平台”)。

2) 浏览器版本为 Internet Explorer 6.0 或以上版本。

3) 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。

4) 可选用 USB 延长线或 USB Hub。

5) 在“深交所 EKey (M5) 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。

6) 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. 第一次使用 EKey 时，请立即修改用户密码，不要使用默认密码。

3. 请牢记您的 EKey 密码，不要透露给其他人。用户反复尝试 EKey 的用户密码，超过 5 次会被锁定。

4. 请妥善保管好您的 EKey，勿借给他人使用。每次使用完 EKey 后，请从电脑上拔下来，并

及时收妥。如有遗失，请立即与 EKey 颁发机构联系。

5. 详细的使用说明请访问 <http://www.szse.cn/marketServices/message/ca/index.html>。

五、常见问题

1. EKey 的初始密码是什么？

EKey 的初始密码默认为“111111”。

2. EKey 上的灯闪烁，是否说明 EKey 在工作？

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

六：硬件规格

硬件型号	SJK1944-G	
型号代码	M5:	支持 RSA1024/2048、SM2 算法
用户的存储空间	128KB	
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°C ~ 70°C	
存放温度	-25°C ~ +85°C	
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 1.1/2.0/3.0 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	M5:	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	M5:	支持 RSA1024/2048、SM2 算法
RSA1024 公私钥对产生时间	≤ 1000 ms（平均时间）	
RSA1024 解密/签名运算时间	≤ 64 ms	
RSA1024 加密/验证运算时间	≤ 12 ms	
RSA2048 公私钥对产生时间	M5:	≤ :7500ms（平均时间）
RSA2048 解密/签名运算时间	M5:	≤ 200 ms
RSA2048 加密/验证运算时间	M5:	≤ 60 ms
SM2 解密/签名运算时间	M5:	≤ 100 ms
SM2 加密/验证运算时间	M5:	≤ 180 ms

密码算法：对称加密算法	支持 DES/3DES 算法（硬件）、SSF33、SM4 算法
DES/3DES 加密/解密速度	$\geq 100\text{Kbps}$
SM4 加密/解密速度	$\geq 500\text{Kbps}$
国密 SSF33 加密/解密速度	$\geq 270\text{Kbps}$
DES/3DES 算法持续工作可用性	$\geq 99.99\%$
SM4 算法持续工作可用性	$\geq 99.99\%$
RSA 算法持续工作可用性	$\geq 99.99\%$
SM2 算法持续工作可用性	$\geq 99.99\%$
通电持续工作可用性	$\geq 99.99\%$