StarKey™220 快速安装使用手册

感谢您使用北京捷德智能卡系统有限公司的产品：捷德 StarKey™系列安全智能钥匙和相关套件软件。您将在几分钟内了解和学会使用这种当今保障网络信息安全 USB 智能钥匙。

捷德公司的 StarKey™220 安全智能钥匙是在数字签名智能卡技术和 PKI 技术基础之上开发了一项创新产品。传统的智能卡被 USB Key 代替，微型处理器与 USB 控制器及连接器被嵌入一个壳体中，USB Key 是卡片功能的扩充，使用户不再需要读卡器。该产品及其套件软件可以支持目前互联网信息交换的主要应用：电子商务、网络银行、安全电子邮件、电子政务、网络安全登录、数字签名、信息加解密等等。

随后，您将跟随快速使用手册，安装捷德 StarKey™220 安全智能钥匙的驱动程序和中间件套件软件，使您感受到该产品的动能和特点。

计算机系统要求

在您安装 StarKey™220 的驱动和套件软件前，请检查您的计算机系统是否符合以下需求：

您的计算机操作系统必须是以下操作系统：

- Windows 2000
- Windows XP
- Windows 2003
- Vista

您的计算机同时具有 1 个以上的 USB 接口

- 注意： 如果您的计算机操作系统是 Windows 2000、 Windows XP 或 Windows 2003，Vista，请使用管理员登录该计算机进行安装操作。

安装捷德 StarKey™220

1. 建议：关闭所有运行的应用程序和窗口。

2. 将捷德 StarKey™220 的配套光盘放入您计算机的光盘驱动器。在光盘驱动器目录下，运行 Setup.exe 程序。如图 1。

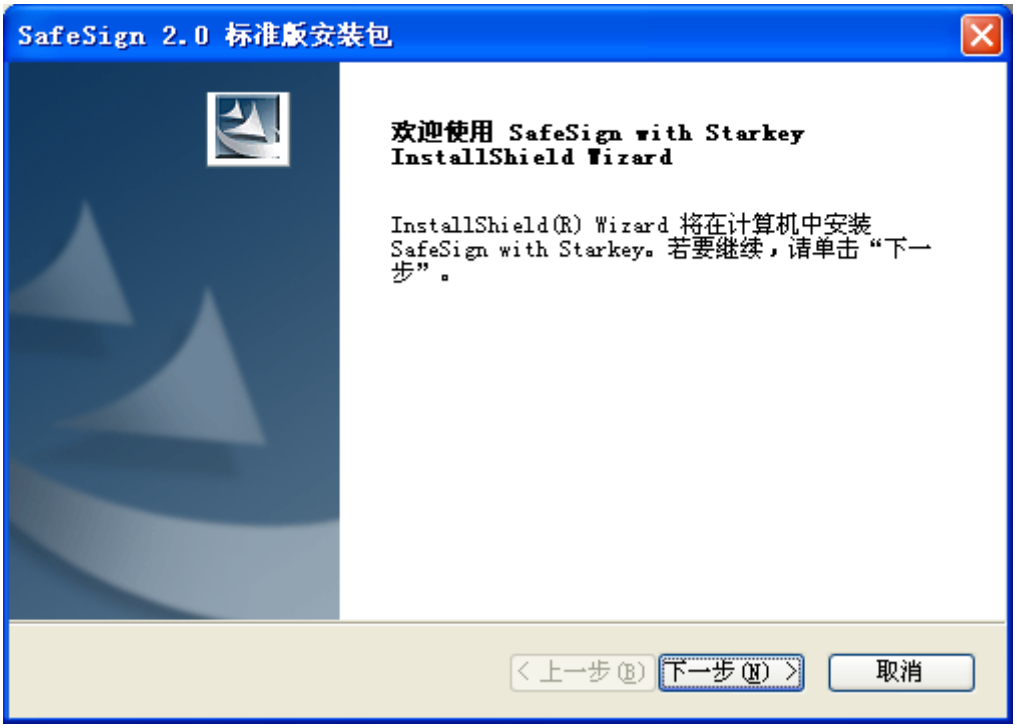

图 1

3. 点击“下一步”后，出现选择安装目录界面，如图 2

图 2

4. 点击“下一步”安装程序会自动安装 StarKey™220 产品的驱动、配套中间件软件和管理工具。如图 3。

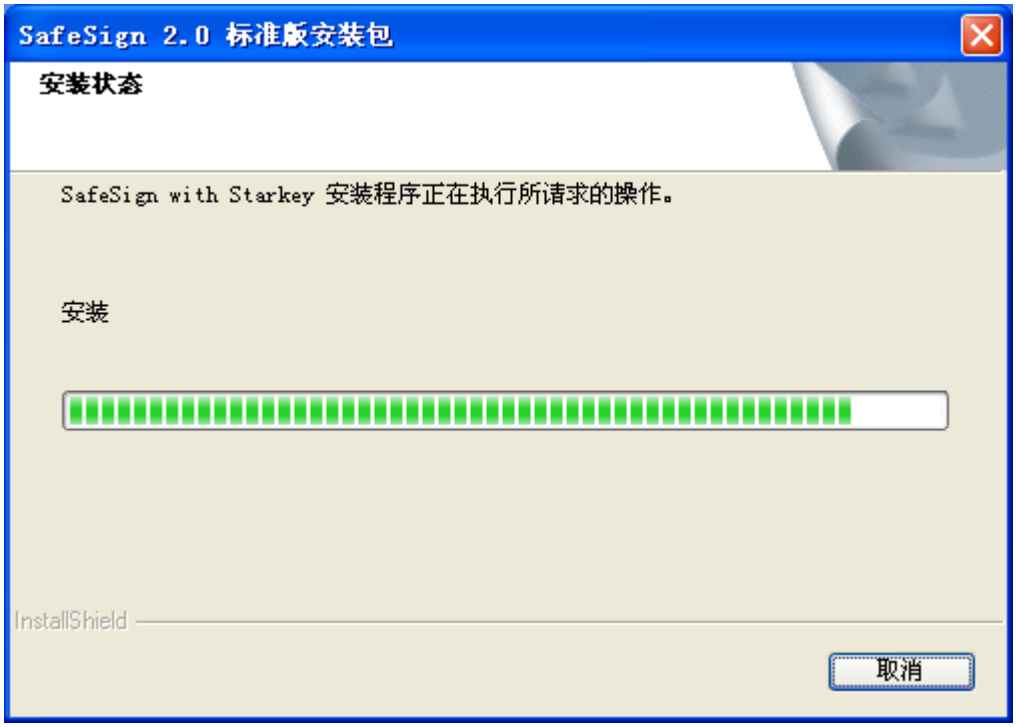

图 3

5. 安装完成之前，安装程序会提示用户安装根证书，只要点击“是”即可

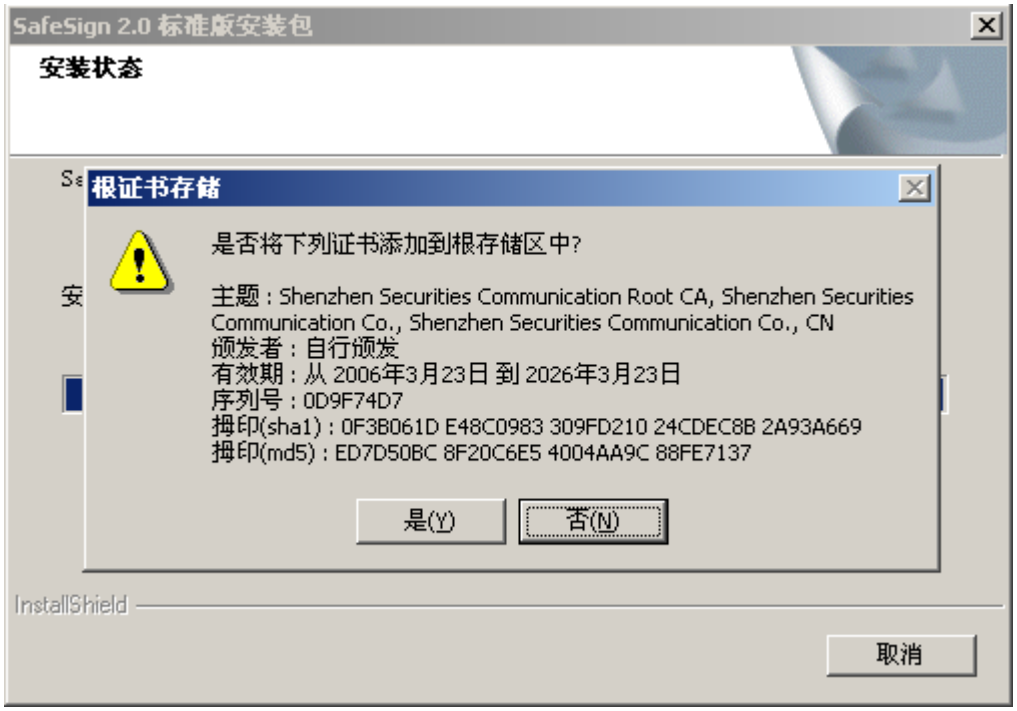

图 5

6. 相关软件安装完毕，请将您的 StarKey™220 插入计算机的 USB 接口，完成安装。

StarKey™220 管理工具说明（用户版）

使用前请注意：

1. 您作为 StarKey™220 的最终用户，在您使用之前，可能需要将您的 StarKey™220 进行初始化，初始化的工作通常由您的管理员为您完成，也可能由为您服务的专业公司为您完成。（使用 StarKey™220 管理员版的管理工具）

2. 初始化完成后，您的 StarKey™220 将有一个初始的用户密码 111111。请您使用管理工具修改您的初始用户密码。

管理工具使用说明：

1. 确认驱动软件安装完毕，StarKey™220 已经插入 USB 接口。

2. 打开“开始”-“程序”-“SafeSign2.0 标准版”-“智能卡管理工具”，进入 StarKey™220 管理工具-SafeSign。如图 5。

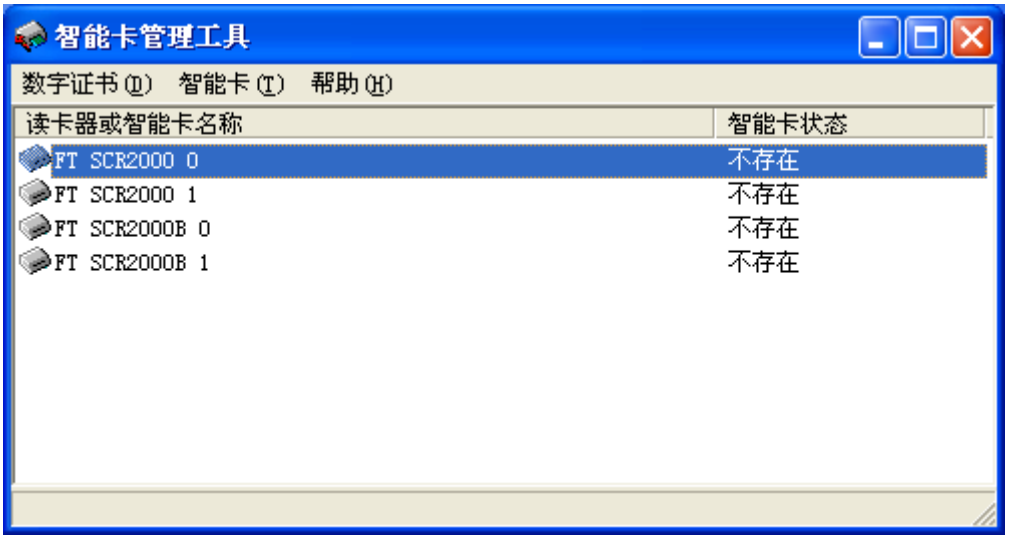

图 4

3. 您可以在 StarKey™220 管理工具中进行如下操作：

a) 在“数字证书”菜单中，可以“查看数字证书”、“导入数字证书”等。如图 5。

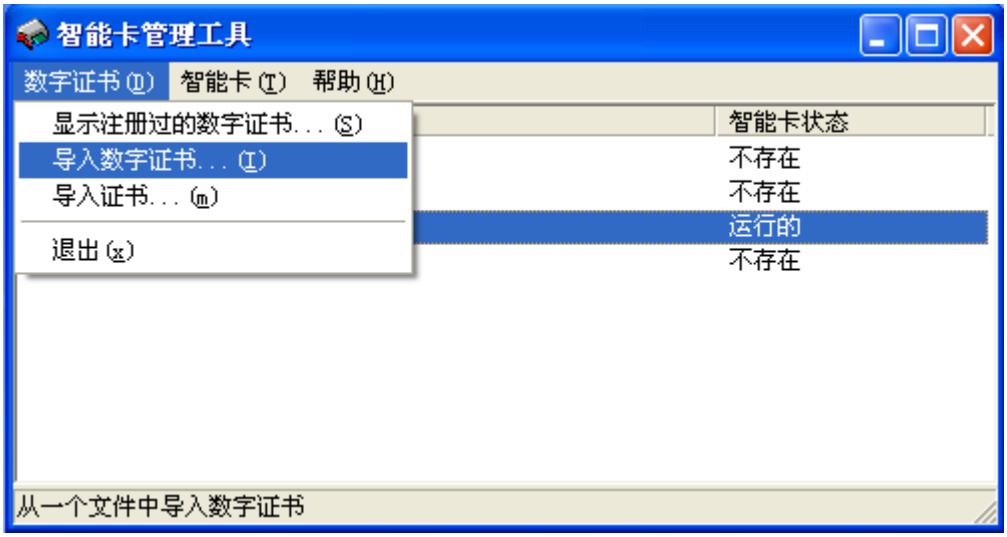

图 5

在“数字证书”菜单中，点击“导入数字证书”和“导入证书”即会出现导入相应内容的菜单，如图 6 图 7。

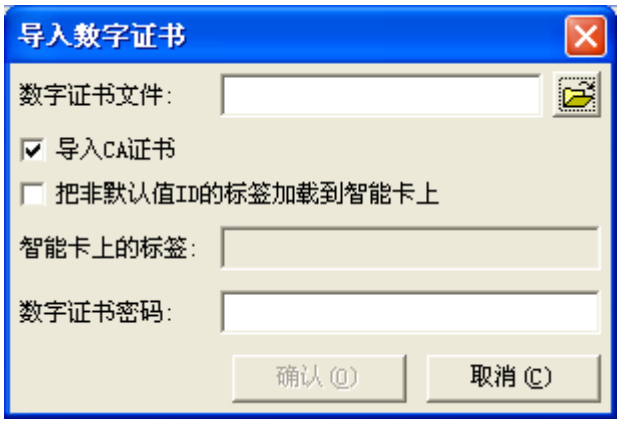

图 6

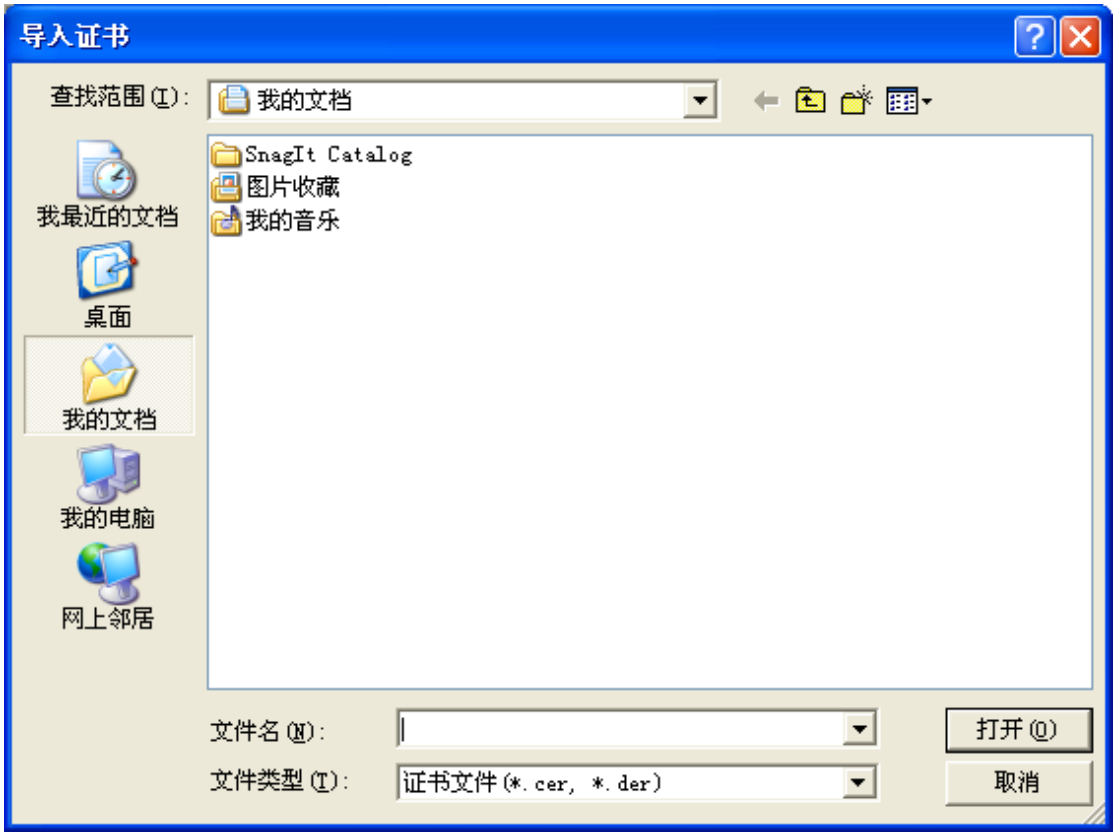

图 7

b) 在“智能卡”菜单中，可以“修改用户密码 PIN”、“查看智能卡对象”、“显示智能卡信息”等操作。如图 8。

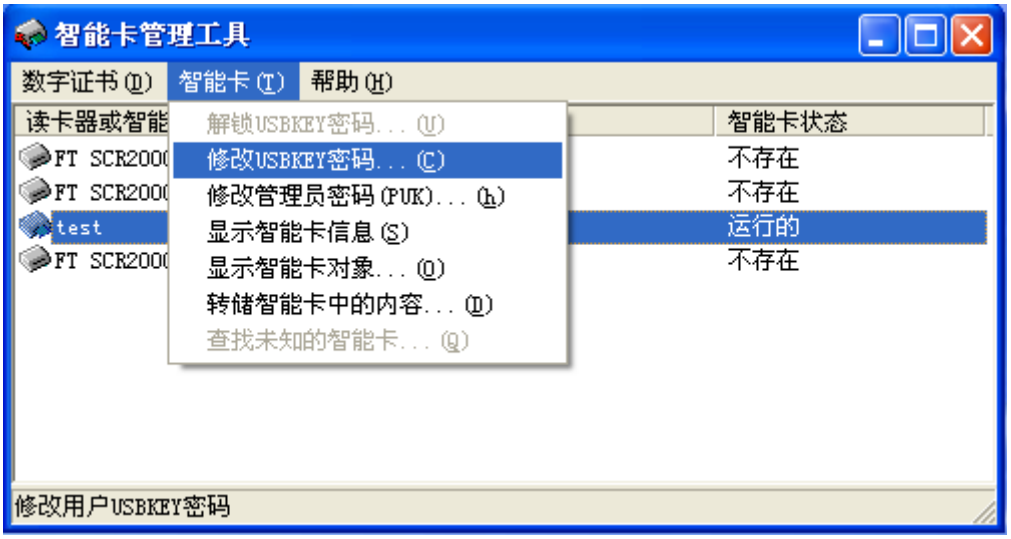

图 8

在“智能卡”菜单中，点击“修改 USBKEY 密码”即可对 KEY 的密码进行修改，在相应位置添入新旧密码点击“确认”即可，修改成功会有相应提示，如图 9 图 10。

PS：USBKEY 的初始密码为 6 个 1，建议收到 USBKEY 后及时进行更改，如果忘记密码用户会有 14 次的尝试密码机会，否则 USBKEY 会被锁死，此时请与颁发者联系。

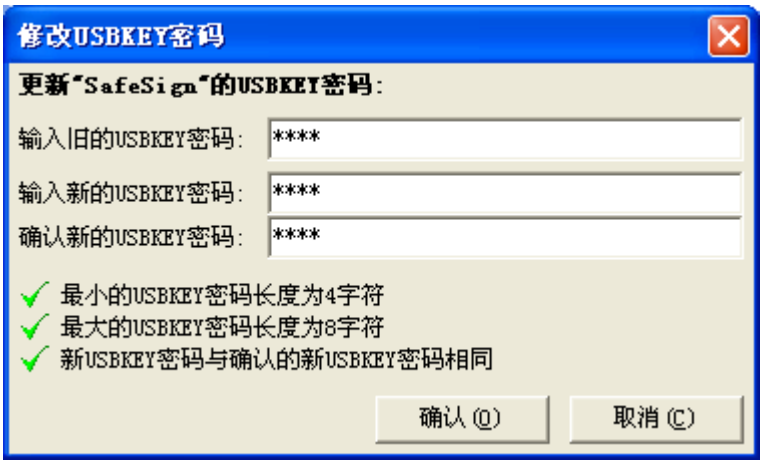

图 9

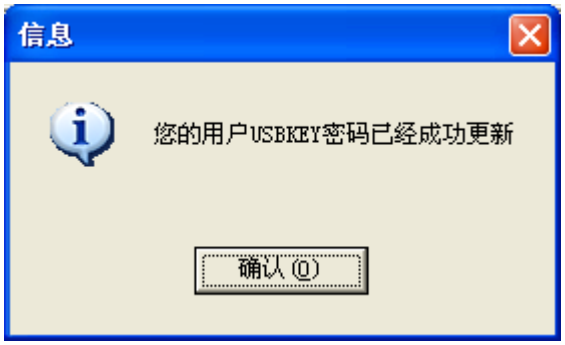

图 10

在“智能卡”菜单中，点击“显示智能卡信息”可以查看智能卡现在的使用情况以及密码状态，如图 11。

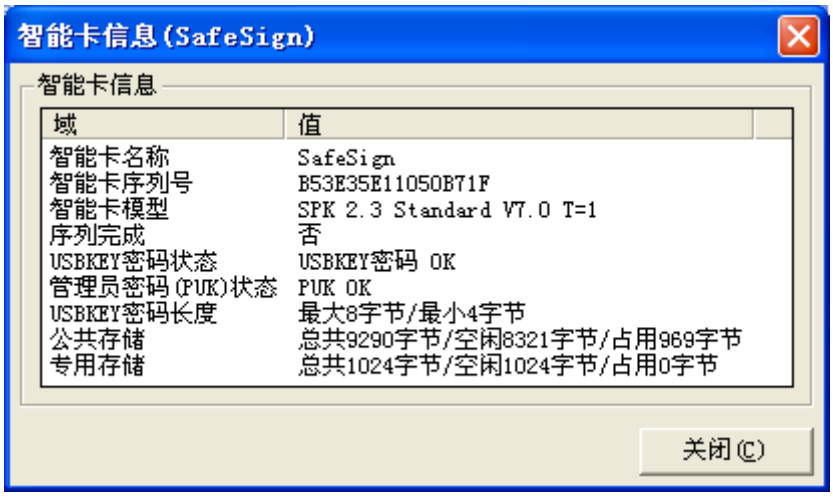

图 11

在“智能卡”菜单中，点击“显示智能卡对象”可以查看智能卡中存贮的对象信息，如图 12。（图中内容只是范例，应用中的对象信息和数量都会不同）

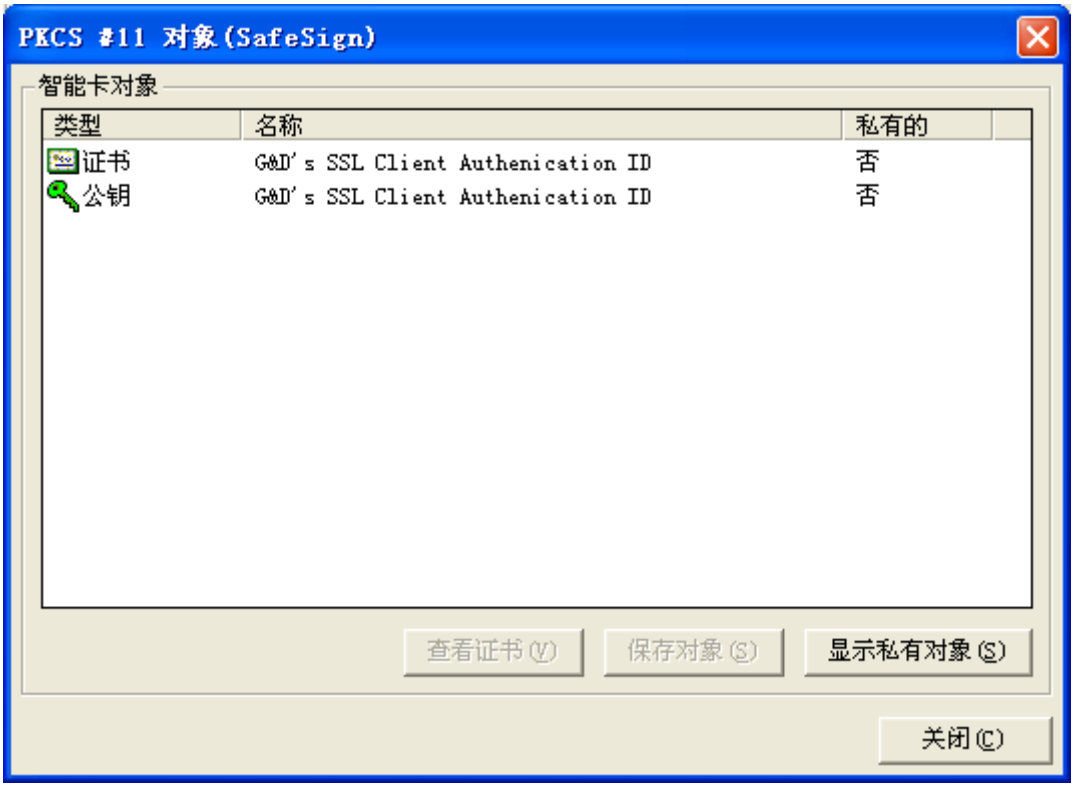

图 12

双击证书，或者选择“查看证书”可以查看到智能卡种存储证书的信息，如图 13，在这个界面上可以查看到证书的主题名，颁发者和有效日期等信息。

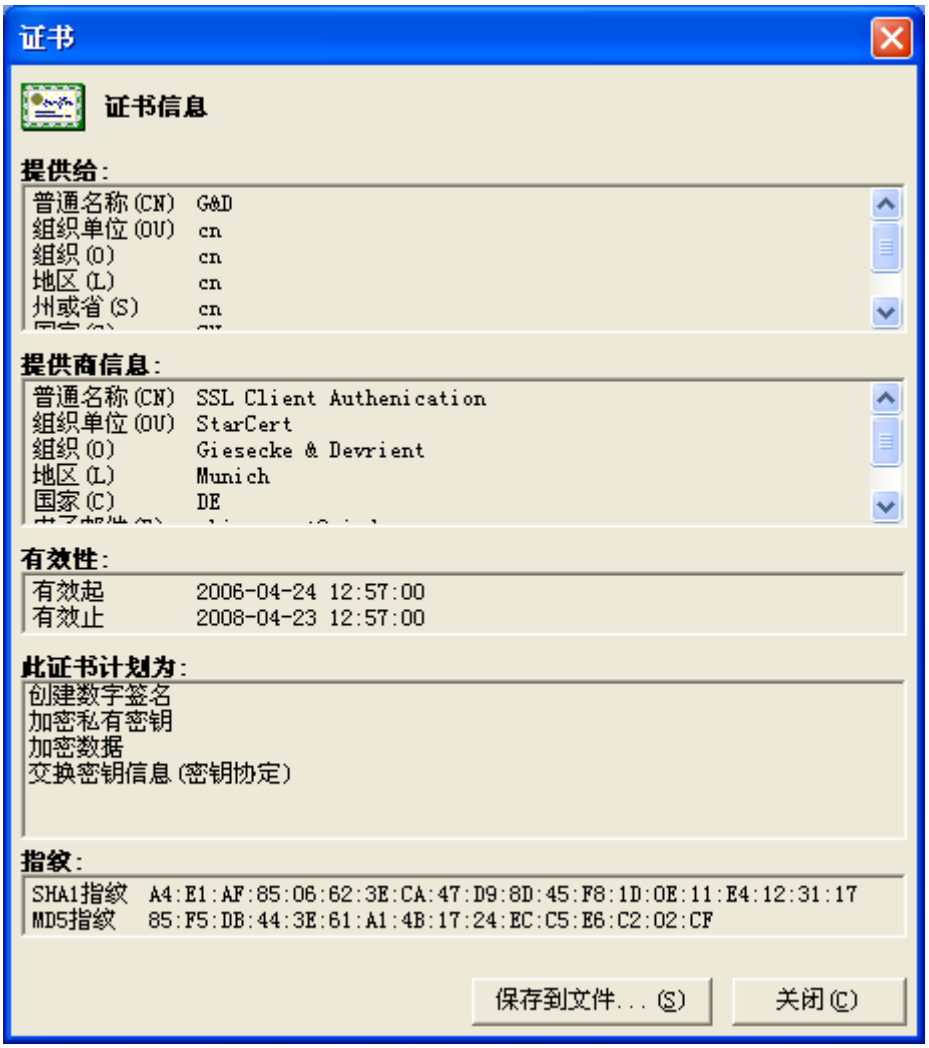
证书
证书信息
提供给:
普通名称(CN) G&D
组织单位(OU) cn
组织(O) cn
地区(L) cn
州或省(S) cn
提供商信息:
普通名称(CN) SSL Client Authenication
组织单位(OU) StarCert
组织(O) Giesecke & Devrient
地区(L) Munich
国家(C) DE
有效性:
有效起 2006-04-24 12:57:00
有效止 2008-04-23 12:57:00
此证书计划为:
创建数字签名
加密私有密钥
加密数据
交换密钥信息(密钥协定)
指纹:
SHA1指纹 A4:E1:AF:85:06:62:3E:CA:47:D9:8D:45:F8:1D:0E:11:E4:12:31:17
MD5指纹 85:F5:DB:44:3E:61:A1:4B:17:24:EC:C5:E6:C2:02:CF
保存到文件...(S)
关闭(C)

图 13

StarKey™220 特性和技术参数

StarKey™220 拥有以下特性:

- ✧ 最新的智能卡CPU处理器
- ✧ 96K bytes ROM空间
- ✧ 4K bytes RAM空间
- ✧ 32 K 比特 EEPROM 空间供客户使用
- ✧ 卡内生成长达1024比特的RSA密钥
- ✧ 支持USB1.1标准
- ✧ 随技数生成符合FIPS140-2安全标准
- ✧ 私有密钥操作：签名及解密
- ✧ 非对称认证
- ✧ 数字签名应用平台
- ✧ RSA 签名及验证长达1024比特密钥长度， 符合ISO/IEC 7816-8标准
- ✧ 支持PKCS#11
- ✧ 支持Microsoft CryptoAPI 的 CSP
- ✧ 与ISO/IEC and EMV `96 兼容
- ✧ 安全报文
- ✧ 卡内进行DES, DES-3 和SHA-1 算法

因为必须的算法都是在硬件内部进行的，所以密钥是安全的。

- ➢ 生成硬件密钥对速度更快

  RSA 密钥对是在 StarKey™220 硬件内部生成的。生成 1024 比特密钥对只需大约 4 秒钟，用于生成密钥的主密钥是芯片上的随机数生成器生成的。

- ➢ 硬件随机数生成器

  StarKey™220 使用真正的随机数生成器生成密钥对和报文认证码（MAC）。随技数生成符合 FIPS140-2 安全标准。

- ➢ 多级访问

  StarKey™220 文件系统中有 16 个安全级别。文件系统使用户能够定义一个或多个用于密钥管理的安全权限，用户可以根据需求定义复杂的安全关系。

- ➢ 安全存储空间

  StarKey™220 使用拥有芯片内部处理器，用于固件和数据存储。这种设计非常安全，因为数据和低级别指令集永不离开 StarKey™220。

- ➢ SafeSign 中间件特性
  - ✧ 支持多种语言。
  - ✧ PKCS#11, PKCS#12, PKCS#15
  - ✧ 支持Microsoft CryptoAPI （CSP）

- ✧ Microsoft Windows 2000/XP 登录
- ✧ 安全电子邮件客户如Microsoft Outlook (Express, 98, 2000), Netscape Messenger, Novell Groupwise 6, Baltimore MailSecure
- ✧ 安全电子邮件插件Secure eMail plug-ins for Lotus Notes from Utimaco, Secude, SSE, Baltimore
- ✧ 浏览器SSL认证， 如 MS Internet Explorer, Netscape Navigator
- ✧ Baltimore PKI, Entrust PKI, RSA Keon PKI, VeriSign PKI 或GlobalSign PKI 应用支持通过 PKCS#11 or MS CryptoAPI
- ✧ Microsoft, NCP, Cisco, Checkpoint 的VPN客户
- ✧ SSH 安全外壳客户
- ✧ PGP, RSA SecurID, Celo eSigner, Lotus Notes Rnext

➢ 驱动

- ✧ 微软认证WHQL
- ✧ Windows 98/ME/2000/XP/2003

StarKey™220 系统结构

我们提供标准的 PC/SC API. 开发人员可以使用标准的 Microsoft Win32 PC/SC 函数集来开发 StarKey™220。

StarKey™220 系统结构由四层组成: 硬件, Kernel 驱动, 用户界面 和应用层

➢ 硬件层

硬件层在系统的最底层，它包括 StarKey™220 硬件电路，固件程序和连接线。

➢ Kernel 驱动层

KERNEL 驱动层处理 PC 与硬件层之间的数据交互，StarKey™220 通过上层应用访问需求，是标准的 PC/SC 驱动界面。上层应用可以通过标准的 Win32 PC/SC 函数集访问 StarKey™220。

➢ 用户界面层

这一层有两个附属层：下面一层负责基本 APDU 指令和其他操作的传输，上面一层用于 PKI 应用。

在下面一层的应用界面为智能卡开发人员提供功能。开发人员可以直接发送 APRU 指令给 StarKey™220 进行硬件操作，也可以使用标准的 Win32 PC/SC 函数集来开发 StarKey™220 应用。如果 Win32 界面不提供所需的功能，开发人员可以使用私有界面。

位于上面一层的界面是 PKCS#11 API 和 MS CryptoAPI 界面。 该界面由下层界面支持，与现有应用兼容，并可以进行开发。例如，一些应用要求用户通过 StarKey™220 以数字形式签署在浏览器中提交的内容。这些功能就需要使用上层界面。

➢ 应用层

位于应用层的程序包括 StarKey™220 通用和专有应用。捷德提供的界面是基于行业标准的，

多数开发人员都会逐渐熟悉。开发人员可以使用捷德提供的界面将他们的应用集成到 StarKey™220 上。

StarKey™220 技术标准

支持操作系统	Windows 98SE/ME/2000/XP/2003
尺寸	50 x 17 x 7 mm (1.97 x 0.67 x 0.28 英尺)
重量	5 克
耗电量	< 250 mW
运行温度	0 C ~ 70 C (32 F to 156 F)
储存温度	-40 C ~ 85 C (-40 F to 185 F)
湿度	非密集排列 0 to 100%
接口类型	USB type A (Universal Serial Bus)
外壳	高级模具、防水、聚碳料高强度外壳
RSA 1,024byte 密钥对生成速度	4s
RSA 1,024byte 密钥签名速度	180ms
RSA 1,024byte 密钥验证速度	60ms
3-DES 加密	31us
DES 加密	19us
数据存储时间	最少 10 年
存储单元擦写	最少 100,000 次