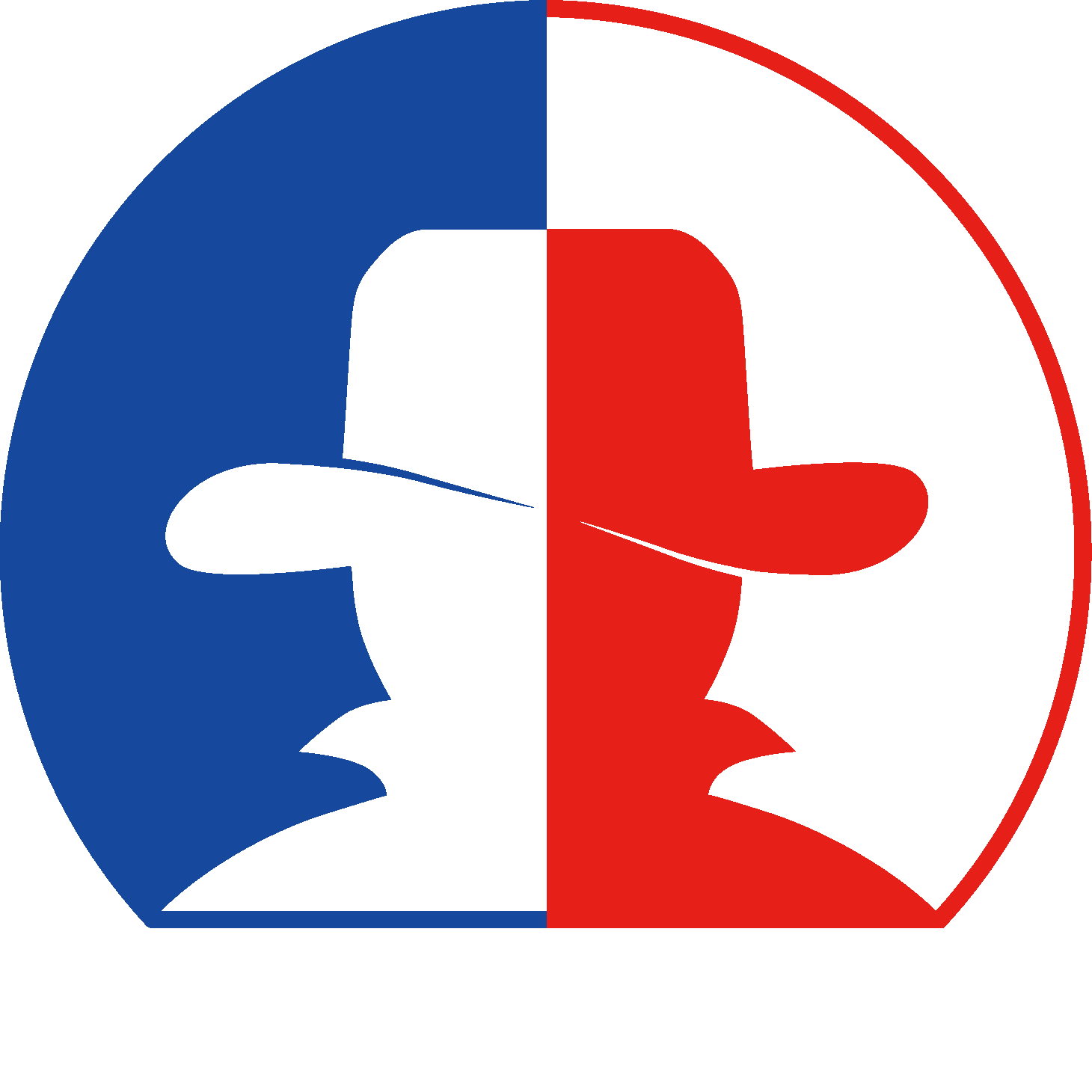
安全鼠标SFM-A03

用户手册V1.0







深圳奇甲安全信息技术有限公司

* 办公地址: 深圳宝安区翻身路38区华创达创客创新基地A507
* 公司网址: <https://www.ab2cd.com/>
* 电子邮箱: support@ab2cd.com

目录

[1 公司简介 3](#_Toc120179390)

[2 产品简介 3](#_Toc120179391)

[2.1 产品功能 3](#_Toc120179392)

[2.2 产品参数 4](#_Toc120179393)

[2.3 执行标准 5](#_Toc120179394)

[2.4 对外接口 5](#_Toc120179395)

[2.5 产品功能示意图 6](#_Toc120179396)

[2.6 产品应用逻辑框架图 7](#_Toc120179397)

[3 USB鼠标功能 7](#_Toc120179398)

[4 指纹生物识别 7](#_Toc120179399)

[4.1 指纹识别应用分类 7](#_Toc120179400)

[4.2 指纹录入要领和说明 8](#_Toc120179401)

[4.3 指纹录入提示 8](#_Toc120179402)

[4.4 解锁Windows功能 8](#_Toc120179403)

[4.5 本地验证功能 11](#_Toc120179404)

[5 口令管理功能 11](#_Toc120179405)

[5.1 软件安装和卸载 11](#_Toc120179406)

[5.2 首次使用 14](#_Toc120179407)

[5.3 添加用户和口令 16](#_Toc120179408)

[5.4 使用用户和口令 17](#_Toc120179409)

[5.5 修改PIN码 18](#_Toc120179410)

[5.6 增加/删除指纹 19](#_Toc120179411)

[5.7 备份/恢复口令 19](#_Toc120179412)

[6 USBKey应用 20](#_Toc120179413)

[6.1 USBKey介绍 20](#_Toc120179414)

[6.2 USBKey应用接口 21](#_Toc120179415)

[6.3 预置证书 22](#_Toc120179416)

[6.4 USBKey安全应用 22](#_Toc120179417)

[7 文件加密 25](#_Toc120179418)

[7.1 加密原理 25](#_Toc120179419)

[7.2 文件加密 25](#_Toc120179420)

[7.3 文件解密 26](#_Toc120179421)

[8 用户须知 26](#_Toc120179422)

[8.1 常见问题 26](#_Toc120179423)

[8.2 使用须知 27](#_Toc120179424)

[8.3 装箱清单 28](#_Toc120179425)

# 公司简介

深圳奇甲安全以物联网安全作为公司的核心业务，为物联网安全提供系统解决方案。以物联网安全作为技术输出，物联网平台作为技术配套，以安全设备作为长远规划的物联网安全高新企业。

以安全芯片应用于物联网终端设备为载体，以PKI作为技术支撑，配套后台加密服务器及其设备，为用户提供软/硬件防盗版、设备监管、数据采集、数据分析、安全预警、安全升级、隐私保护等安全服务，做到设备可信、数据可信、操作可信。

奇甲安全将持续深耕物联网安全应用行业，为广大客服提供系统的，稳定的，成熟的，先进的物联网安全产品。

公司创新性研发身份认证类安全产品，包括安全鼠标，指纹Dongle，安全模组等系列化产品。

# 产品简介

* 1. 产品功能

SFM-A03产品是由奇甲安全研发，将鼠标功能，指纹解锁，口令管理，USBKey，文件加密功能五合一身份认证通用安全产品。

鼠标采用USB接口方式，即插即用，无需安装驱动即可使用鼠标功能。如果使用其它系统或者其它功能，通过扫描鼠标下方二维码方式进入网页下载对应驱动。

指纹解锁功能符合Windows Hello指纹标准，首次插入鼠标后，将自动从微软官网下载指纹驱动，然后按照Windows账户管理相关页面录入指纹，录入成功之后，则可以实现电脑开机时快速登录以及屏幕锁定时指纹解锁功能。

口令管理功能是本安全鼠标特有便捷实用功能，用户可以通过鼠标保存若干条用户口令和密码，在任何输入口令和密码登录各个系统和软件时通过点击鼠标中键，弹出用户口令和密码，并按照当前软件/网页自动排序（一般为第一条），仅需选择即可完成登录操作，用户无需记录用户名和密码。

在安全鼠标内载一颗安全芯片，内嵌了一个标准USBKey功能，用户通过验证指纹确认使用者身份，根据应用需求加载不同的证书，通过PKI体系实现身份识别/身份认证工作，可用于电子签章，登录管理，权限管理，软件保护等安全应用。

同时，内嵌的安全芯片为高速USB2.0芯片，通过安全芯片密码运算模块实现对文件的高速加密/解密，配合PC端文件管理工具，通过指纹确认用户身份，即可实现文件解密。加密的文件必须本人指纹才能使用，不能离开鼠标脱密。

* 1. 产品参数

|  |  |
| --- | --- |
| 内容 | 产品参数 |
| 整机 | |
| 工作温度 | 5℃～50℃ |
| 存储温度 | -20℃～60℃ |
| 工作电压 | DC 4.75V-5.25V |
| 待机功耗 | ≤1mA |
| 运行功耗 | ≤100mA |
| 通讯方式 | USB2.0兼容USB1.1 |
| 系统支持 | 指纹Windows 10 系统 |
| 芯片组 | |
| 安全芯片 | ACH512QFN64 |
| USB HUB | Fe1.1s |
| Fingerprint sensor | CS9511 |
| USB Mouse sensor | OM50E |
| 鼠标 | |
| 鼠标类型 | 有线鼠标 |
| 人体工学 | 左右手对称设计 |
| 按键个数 | 3键（左键，右键，中键） |
| DPI | （支持1000/1200） |
| 回报率 | 1/125秒 |
| 产品定位 | 办公商务/个性时尚 |
| 指纹 | |
| 指纹尺寸 | 96X96 pix |
| 指纹数量 | 4枚 |
| 拒假率(FAR) | ≤1/50000(0.0002%) |
| 拒真率(FRR) | ≤1.26% |
| 密码运算 | |
| 支持算法 | SM1/SM2/SM3/SM4/RSA2048/ECC256/AES128/TDES/HMAC |
| 支持应用个数 | 4 |
| 支持PKI证书 | 8 |
| 支持口令存储 | 128个 |
| SM2产生秘钥对速率 | >100次/秒 |
| SM2签名速率 | >100次/秒 |
| SM2验签速率 | >100次/秒 |
| SM4加密速率 | >50MBps |
| 口令管理 | |
| 保存口令个数 | 大于200个（标准版）、10000个（管理员版） |
| 软件辨识匹配度 | 80% |

* 1. 执行标准

|  |  |
| --- | --- |
| 标准名称 | 内容 |
| 国际标准 | CE  FCC  ROHS |
| 国家标准 |  |
| 行业标准 |  |
| 通讯协议 |  |
| 认证标准 |  |
| EMC标准 |  |

* 1. 对外接口
* 硬件接口

|  |  |  |  |
| --- | --- | --- | --- |
| 接口名称 | 接口数量 | 符合规范 | 功能描述 |
| USB | 1 | USB2.0 | 数据传输 |
| 按键 | 3 | 无 | 3键（左键，右键，中键） |
| 滚轮 | 1 | 无 | 滚动 |
| 灯带 | 1 | 无 | 红、绿、蓝 |
| 指纹 | 1 | Windows Hello | 唤醒、解锁Windows、本地身份验证 |

* 软件接口

软件接口支持C++、JAVA语言开发对接。

|  |  |  |
| --- | --- | --- |
| 接口名称 | 符合规范 | 功能描述 |
| CSP | CSP | 微软颁发，在Windows操作系统上通行 |
| PKCS | PKCS#11 | Linux密码管理应用接口规范 |
| SKF | SKF | 中国密码协会接口规范 |

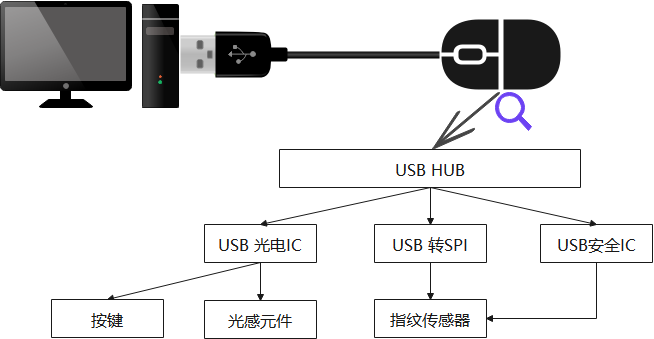
* 1. 产品功能示意图



通过USB与PC端相连，鼠标采用对称设计，左右按键和中键，滚轮采用导光材料，在鼠标左侧有指纹输入，后端镭雕公司Logo，并通过呼吸灯将Logo和灯带展示出来，同时显示安全鼠标工作状态。



* 1. 产品应用逻辑框架图



安全鼠标插入PC端后，将显示4个设备：鼠标指针设备（USB 鼠标），生物识别设备（指纹），HID1设备（USBKey）, HID2设备（口令管理）。

# USB鼠标功能

本安全鼠标之鼠标采用对称设计，通用3键（左右中）功能+滚轮设计，DPI为：1000/1200（具体因硬件版本不同而有区别），DPI不能调整；回报率1/125秒，设计简洁，美观大方，经久耐用，符合人体工程学要求，人性化设计，适合办公要求，是一款体验优异的鼠标。

鼠标采用符合Windows/Linux标准HID鼠标设计，无需安装任何驱动，适应能力强，能自动匹配目前几乎所有操作系统。

# 指纹生物识别

* 1. 指纹识别应用分类

人体指纹信息包含了人体独一无二的特征，通过指纹确认用户身份是非常便捷有效的手段。在本安全鼠标中，有两种应用模式：

一种是将指纹图像信息采集送到上位机，上位机通过指纹识别算法与之前采集的指纹进行比对，比对成功之后，可以登录系统，解锁屏幕等获取使用上位机资源权限。

一种是将将指纹信息本地存储比对，即在安全鼠标内部存储运算，对比成功之后，将获得使用USBKey，使用口令管理工具，文件加密密钥等权限。

* 1. 指纹录入要领和说明

1. 手指要按下，抬起为一次录入或者验证过程，长时间不按下或者长时间不抬起可能会造成用户超时；
2. 按下指纹的时候，不要太轻，不能抖动，来回摩擦。
3. 录入指纹时，为了获取更多的有效特征，需要录入10次，每次录入时，稍微变换一下指纹方向或者位置。这样，验证时无论手指任何角度录入都有机会进行匹配，增大验证成功的概率；
4. 有的手指，由于工作运动磨损等原因，指纹特征不明显，录入和比对会比较困难，尤其是老人或者长期使用某个手指的劳动者。如遇此情况，请更换手指或者重复多次录入；
5. 指纹验证具有自我自动学习功能，会自动将当前识别成功的指纹特征合并至录入的数据库中，将越用越快。
   1. 指纹录入提示

用户使用指纹功能时，安全鼠标尾部LED配合用户录入过程，并提示指纹录入状态，LED提示只对口令管理/USBKey使用有效，对鼠标使用不具意义。（部分产品有此功能）

其具体含义如下：

|  |  |  |
| --- | --- | --- |
| 状态 | LED灯显示 | 说明 |
| 闲时 | 红黄蓝交替缓慢点亮 | 约5分钟后自动熄灭，进入休眠模式 |
| USBKey工作 | 黄灯闪烁 | USBKey通讯时即表明USBKey忙 |
| 指纹按下 | 红黄绿快速流水灯 | 等待指纹弹起 |
| 指纹弹起并成功 | 绿灯闪烁3秒后常亮 | Windows取指纹成功/本地验证指纹成功 |
| 指纹弹起并失败 | 红灯闪烁3秒后全灭 | Windows取指纹失败/本地验证指纹失败 |
| 系统故障 | 红黄绿同时爆闪 | 出现系统性，严重错误，如：锁定 |

* 1. 解锁Windows功能

Windows10之后的版本，自带Windows Hello功能，通过指纹生物识别信息能在开机是快速登陆Windows系统，以及屏幕锁定后解锁Windows功能。

* 驱动安装

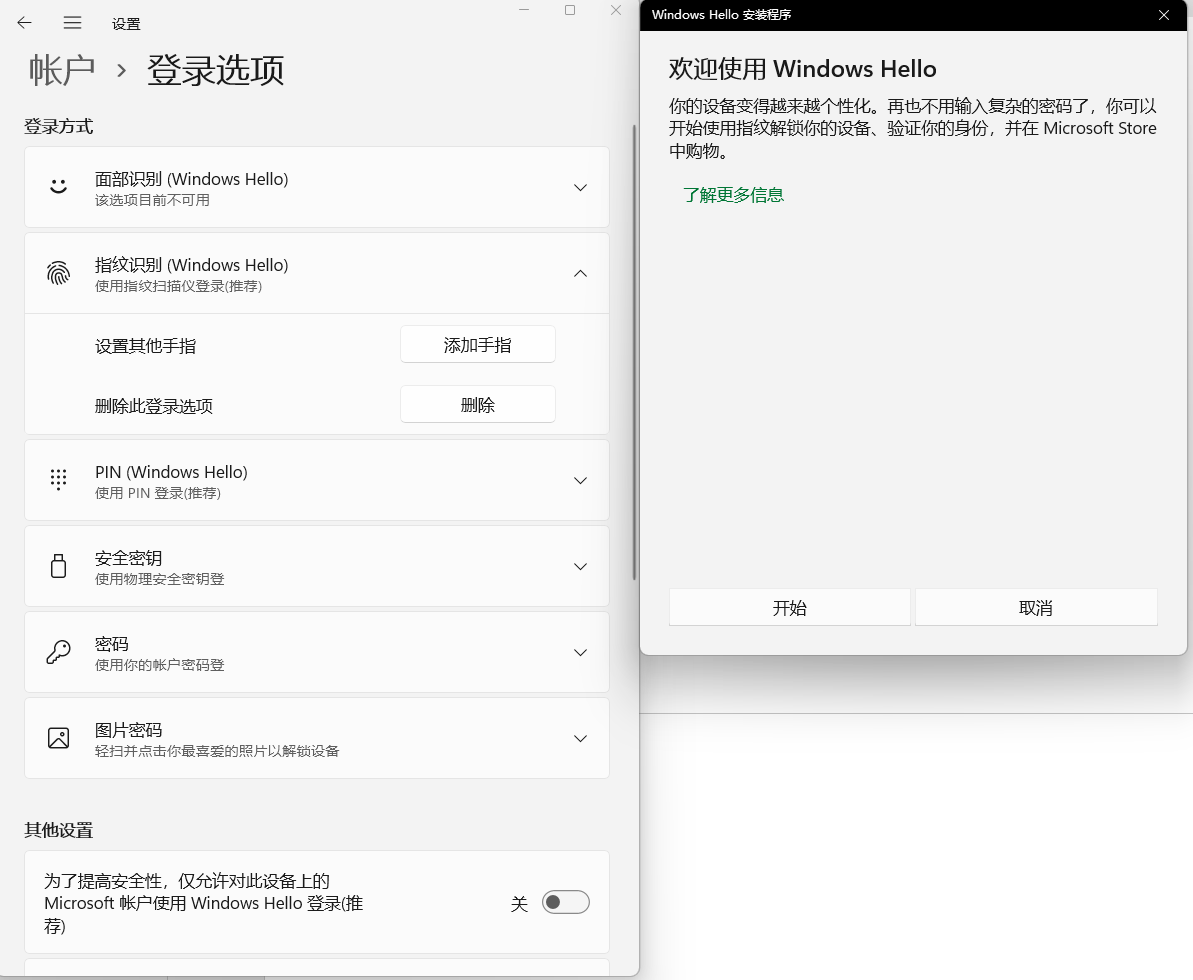
当首次插入USB鼠标时，如果电脑处在联网状态，并打开Windows更新功能，则系统将自动从微软官网下载经微软授权签名的指纹驱动程序；如果电脑没有联网或者没有设置为自动更新，则需要扫描鼠标下方二维码或者手动方式输入web网址（<http://www.ab2cd.com/upload/20220506091921f.rar>)下载驱动并手动安装。

驱动下载二维码（进入之后选择Windows指纹驱动）：



* 初始化指纹

首次使用Windows Hello生物（指纹）识别需要初始化指纹，按照步骤依次进入：设置->账户->登录选项(Windows Hello)->指纹识别->添加手指，录入指纹信息，如下图所示。Windows指纹登录没有个数限制，用户可以录入多个指纹对应同一个Windows账户。



点击开始，输入当前用户口令之后，开始录入指纹。

为获取更多的指纹特征，需要多次录入并获取指纹侧面指纹信息，所以需要按照提示多次录入，直到显示“一切就绪”为止。

录入成功之后，即可实现登录Windows和解锁Windows功能应用。

* 1. 本地验证功能

本地验证指纹功能与解锁Windows功能没有任何关系，本地验证指纹功能仅限安全鼠标内部生物识别使用，所以，首次使用时同样需要录入指纹功能。本地最多能保存4枚指纹空间，4个指纹可以表示同一个用户，具有相同的使用安全鼠标资源权限。

使用本地验证需要用户手动安装“奇甲安全鼠标”管理工具。从官网下载驱动程序按照指引安装完成后，打开软件，首次使用时使用默认口令：111111登录管理工具，按照提示录入指纹信息。具体见“奇甲安全鼠标管理工具”章节详细说明。

# 口令管理功能

* 1. 软件安装和卸载
* 工具下载

口令管理工具需要安装管理软件，软件下载地址为：

(<http://www.ab2cd.com/upload/20220506092625f.zip>)：

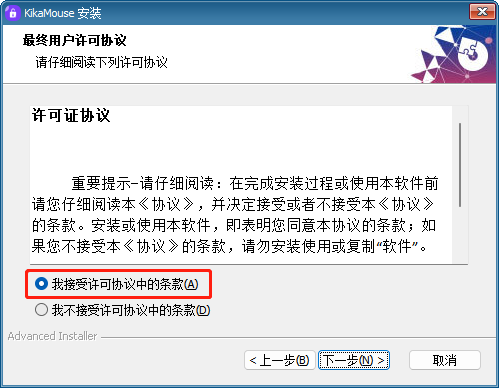


（扫描进入之后选择“安全鼠标管理工具”）：

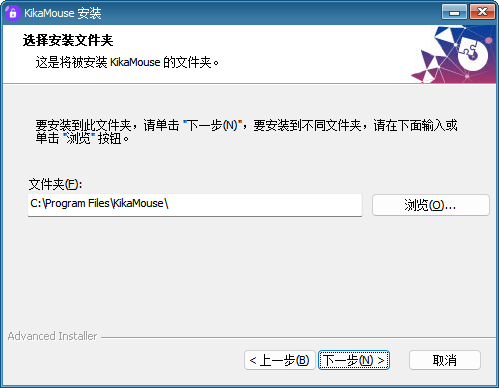
* 软件安装



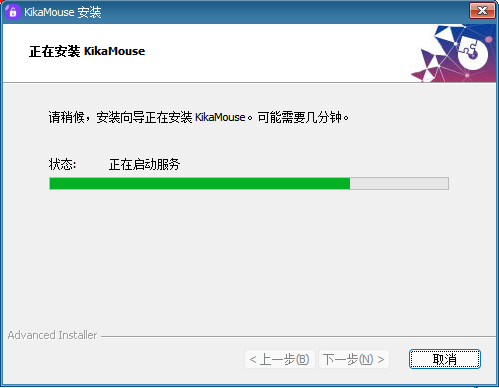
点击安装包进入安装界面



接受许可协议



选择安装目录



开始安装

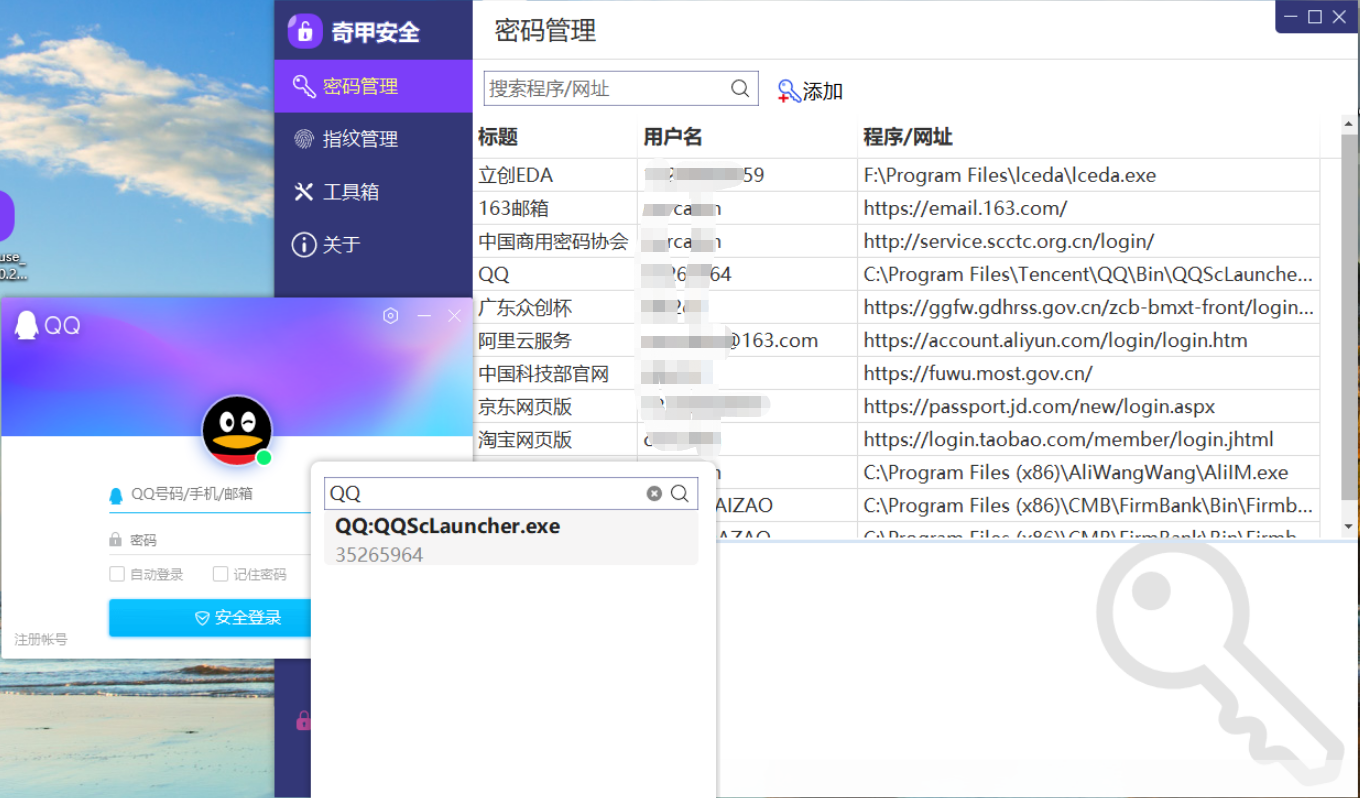


安装完成

按照安装软件指引，直至软件安装成功。安全鼠标口令管理工具分为两部分，一部分为用户界面（奇甲安全鼠标）需要用户主动打开，一部分为后台程序（KikaMouseSvc）为自动长期驻留Windows服务中，并建议开机启动。

* 打开软件

可以通过点击桌面图标KikaMouse进入管理页面，也可以在任何口令输入控件上，点击鼠标中键，点击“密码管理”进入页面，如图：

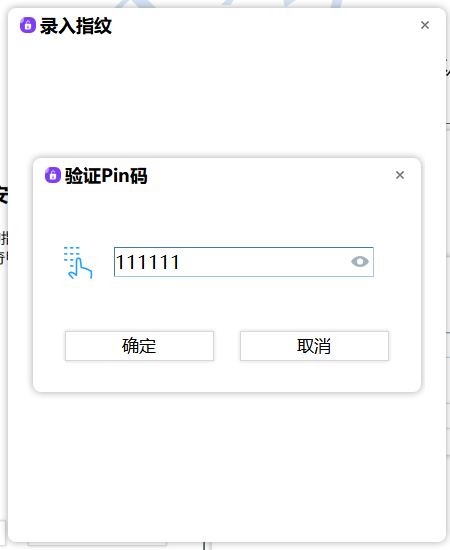
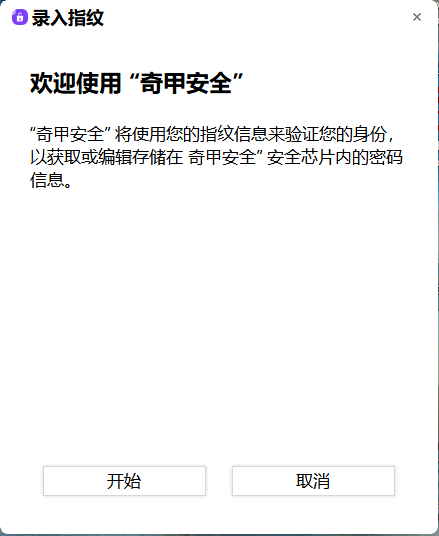


* 软件卸载

可以使用Windows软件卸载工具或者第三方工具卸载奇甲安全鼠标工具。

* 1. 首次使用

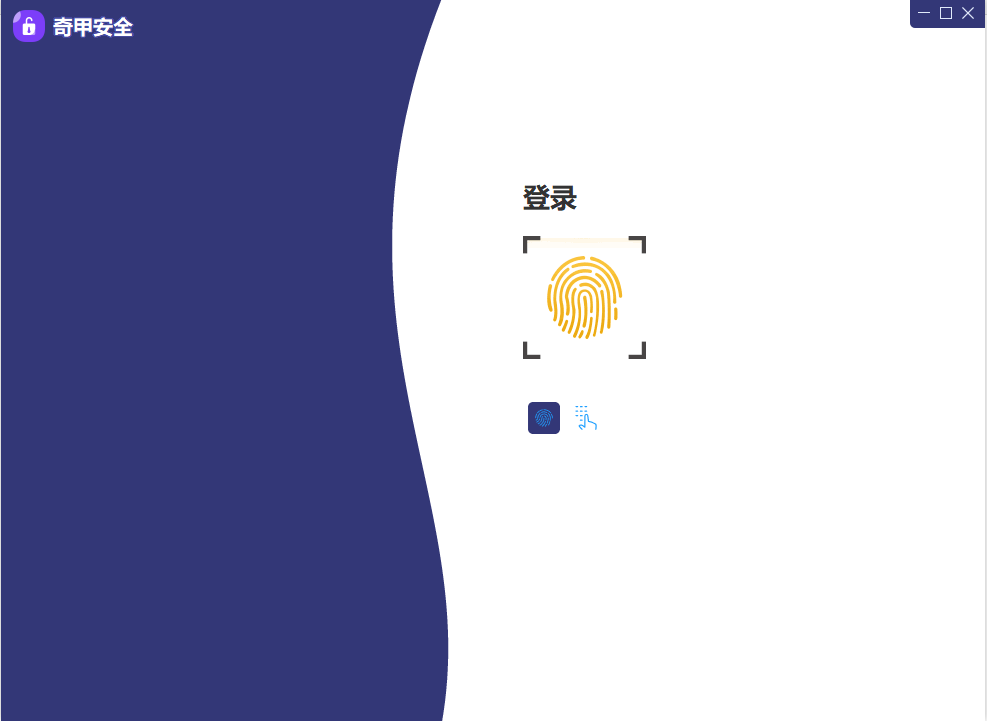
首次使用时，安全鼠标内没有任何指纹信息，需要通过默认口令“111111”进入，如图所示：



输入口令之后，要求用户录入指纹：



录入成功之后，用户可以通过指纹方式登录（也可以通过管理员口令登录）：

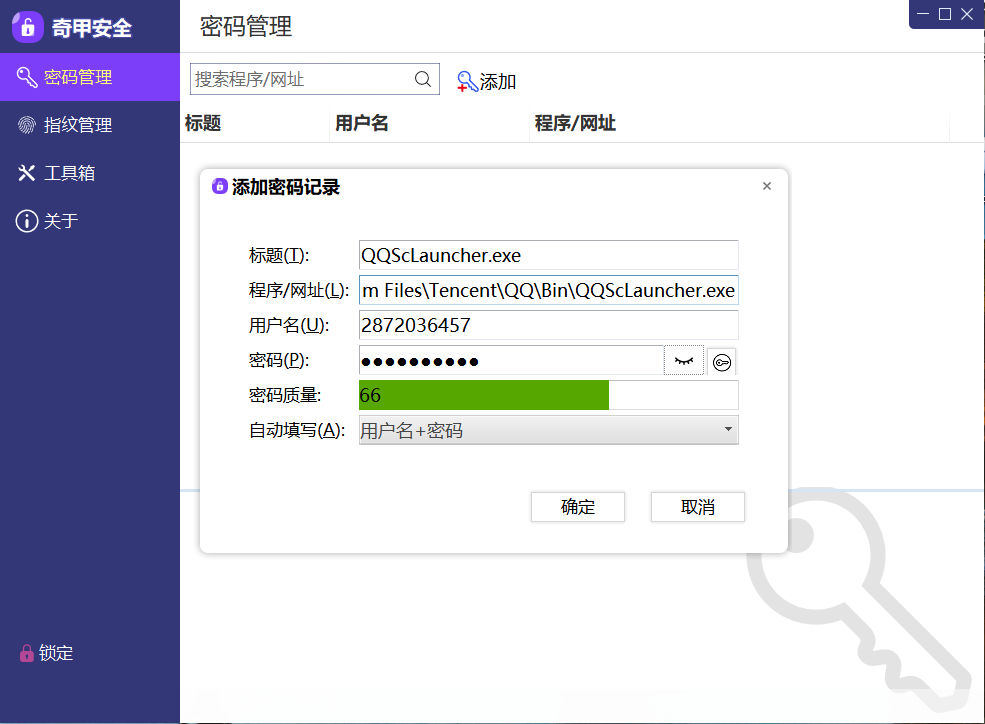


登录成功之后，进入口令管理列表页面：



* 1. 添加用户和口令

进入管理页面后，选择记录管理，点击添加【或者直接将软件快捷方式拉入到管理页面】，并按照格式填写新增记录的网址/软件名称，用户名，密码。并选择使用口令管理自动填入模式（后续会根据用户选择的软件自适应匹配），目前包括两种模式：用户名和密码，密码（用户名默认填充）。也可以点击🔑按钮，自动生成随机密码。

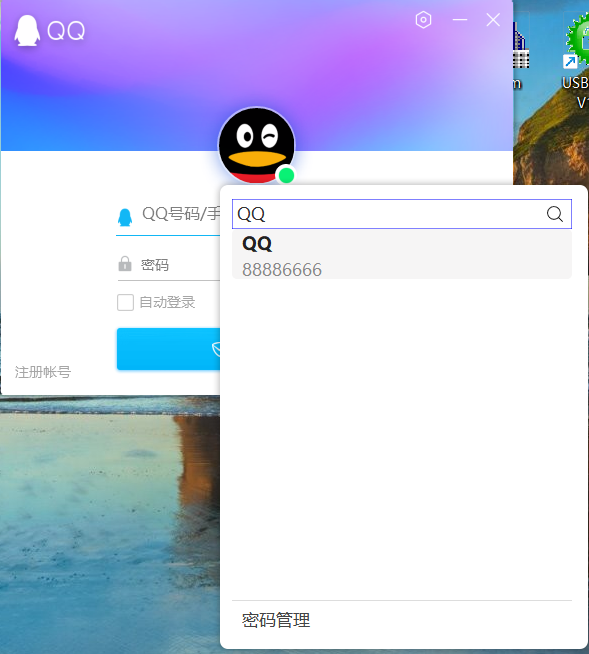


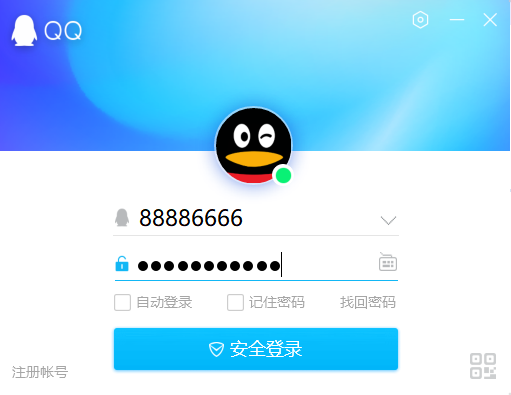
标准版最多可以添加200条以上记录，双击记录可以将记录详情重新展示，也可以点击删除该条记录。



* 1. 使用用户和口令

打开管理工具，单击选择对应记录，点击网页/软件超级链接，如果是本地软件将自动打开应用，如果为网页则直接使用默认浏览器打开对应网站。

如打开QQ，鼠标在用户名闪烁，点击鼠标中键，将弹出密码管理控件，并按照当前软件自动匹配，通常为第一个记录，单击记录选择，将自动将用户名（QQ序列号），密码自动填入。

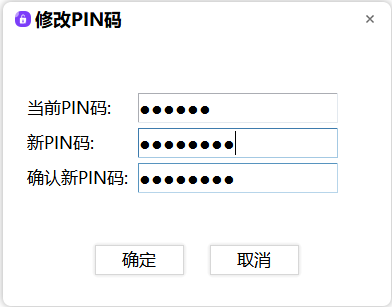
用户只需点击登录即可实现安全登录。

类似的，登录网页账号，点击网页/软件超级链接，打开网页，将光标停留在用户名出，点击鼠标中键，弹出密码管理控件，选择对应网页，将自动填充用户名和密码。

* 1. 修改PIN码

安全鼠标默认登录密码为“111111”，建议用户拿到鼠标后第一时间修改密码，使用密码的权限与指纹的权限完全一致。

用户输入口令最多5次错误，5次之后，口令将被锁定，只能通过指纹方式解锁恢复。如果指纹没有录入/失效，口令被锁，安全鼠标口令管理功能将永远锁定。



* 1. 增加/删除指纹

本安全鼠标标准版本地最多支持4枚指纹，用户可以根据自己需要增加和删除指纹，具体录入过程参考首次使用。



* 1. 备份/恢复口令

用户可以将保存在安全鼠标中的口令，通过加密的方式备份在本地，以防鼠标损坏更换时方便重新导入到安全鼠标中。

系统不会自动备份，一段时间后，建议用户主动备份当前用户口令，备份的文件采用用户口令加密保存，导入时需要输入相同的口令予以解密才能导入到安全鼠标中。

在口令备份时，为防范远程攻击，必须要求用户输入口令同时验证指纹才能备份（待开发）。

作为后续高级应用，我们将口令加密备份至云端，可以满足移动设备多方面应用，待开发。



# USBKey应用

* 1. USBKey介绍

一般意义上的USBKey是一种USB接口的硬件加密设备。它使用MCU用于处理简单的业务逻辑，包含加密算法实现密码学快速运算，并具有一定的存储空间，用于存储用户关键秘密数据如秘钥。在USBKey内置嵌入式操作系统COS，实现对文件管理，权限管理以及密码学运算。

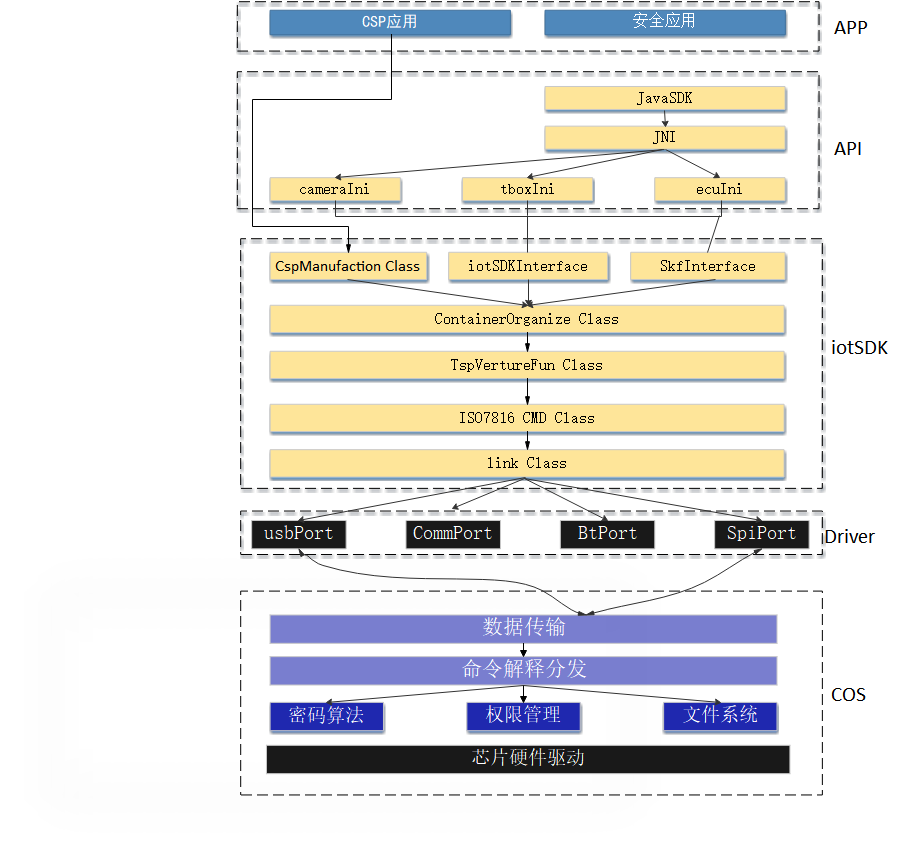
在USBKey中，通过PKI体系（公钥算法）内置用户私钥，对从USBKey发送数据时，使用私钥签名表明身份；从USBKey接收端，使用私钥解密数据。公钥作为公开信息，使用公钥进行加密和验签。由于用户私钥保存在安全芯片中，具有极高的安全等级，通过权限判断满足条件只能使用，理论上使用任何方式都无法读取，因此保证了用户认证的安全性。

在安全鼠标中内置了一颗EAL4+高速安全芯片，内置安全COS系统，并通过指纹方式验证用户授权，在办公系统中具有很强的应用场景。

本USBKey最多能装载8个应用，即8个本地证书，8个应用独立使用。

* 1. USBKey应用接口

USBKey作为应用非常广泛的一种设备，在诸多领域内取得应用。尤其是在安全要求较高的银行系统率先大规模使用，延伸到移动支付领域，政务办公系统等有它的存在。为简化应用，方便各个厂商，各个行业领域互联互通，ISO以及国内相继发布了行业标准，并统一了接口。



安全鼠标内置的USBKey在Windows端复合CSP接口规范，适用在Windows下所有CSP接口应用，如web安全访问网页https证书应用，用户远程登录身份识别应用，版权保护安全应用，等等。

如果当前系统为Linux系统则复合pkcs#11接口规范，同时符合国内智能安全设备接口SKF接口规范。同时，为了更加方便用户使用，安全鼠标还自定义了一套iotSDK接口适应于物联网方向应用接口。

在此标准接口之上，还按照各种要求定义了应用层接口，如有需要还提供了高层的JAVA, Python等接口，方便应用。

具体接口说明，参考其他技术文档。

* 1. 预置证书

在使用USBKey之前，都需要下载服务端认可的设备证书，如果是设备端向服务器端请求业务，只需服务器认证设备端单向认证即可。

在Windows预置证书，可以使用奇甲安全的CSP中间件，在USBKey中预置服务器认可的设备证书，预置证书有两种方式：

1. 在USBKey设备内产生秘钥对，读出公钥，并读出设备相关相关信息，组装成X.509证书请求格式，向CA服务器/证书颁发机构申请证书，CA机构对公钥及其设备信息签名后产生证书，并导入到USBKey中；
2. CA机构根据用户请求产生秘钥对，并对公钥及其设备信息签名，预先产生证书，使用口令对证书文件加密，形成\*.pfx文件，通过CSP导入到USBKey中形成证书；

第一种方式安全，私钥用于在USBKey中，没有外泄；

第二种方式可以批量产生秘钥，效率高；

* 1. USBKey安全应用
* 登录VPN

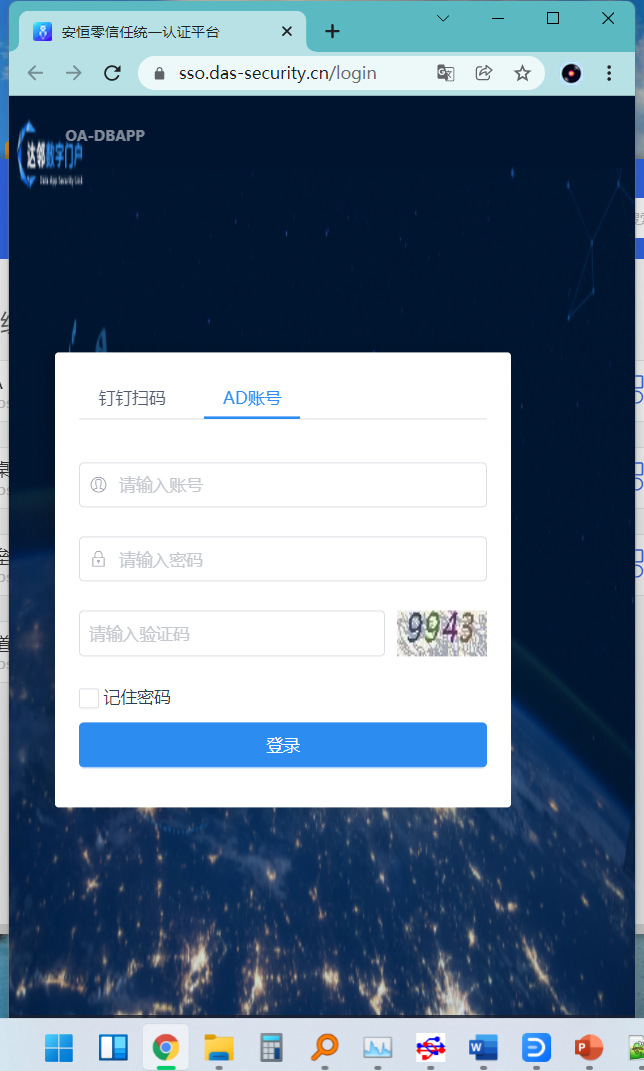
通过上述预置证书的方法，预置服务器认可的设备证书，登录VPN是使用USBKey设备私钥对认证消息签名，将消息发给服务器即可完成单向认证。

而使用USBKey的权限可以通过输入指纹方式验证，无需用户输入密码。通过指纹验证不仅可以验证用户身份，而且通过指纹验证必须在设备端人工操作，意味着必须物理存在，防范远程和假冒攻击，因此无需再通过第三方双因子验证，其安全级别以及便捷度均非常优越。



* 登录OA系统

目前安恒零信任统一认证平台是通过第三方软件重复认证或者账号密码方式登录OA系统的，其安全性及其便捷度都不及指纹USBKey方式验证。



* 公司权限审核

公司内部重要事务，将管理定义为多个角色，并对角色按照规则予以约定，多方确认后完成最终决策。对于此情况可以使用USBKey对操作予以确认，使用私钥对事件确认具有法律效力。

该场景适用于公司法律文件签署，财务人员审计，软件版本发布，发货清单确认等业务。

# 文件加密

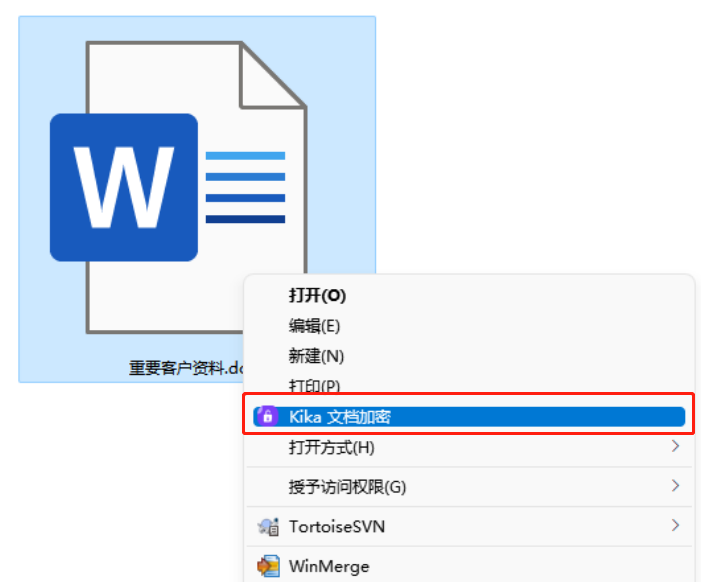
* 1. 加密原理

文件加密是USBKey一个典型应用，内置一组安全应用并产生非对称秘钥对，私钥永不离开硬件，公钥可读不写。文件加密时，读取设备中加密应用公钥，采用公钥配合随机数（保证一次一密）对文件加密；文件解密时，将加密的秘钥通过安全芯片内部私钥解密获得文件加密的秘钥，然后对文件进行解密。

不仅如此，加密管理软件除了对文件进行SM4/AES高强度对称加密之外，还先期对文件进行压缩再加密，极大的提升了用户空间，超强的文件加密安全要求——离开安全鼠标，加密的文件没有办法恢复。

* 1. 文件加密

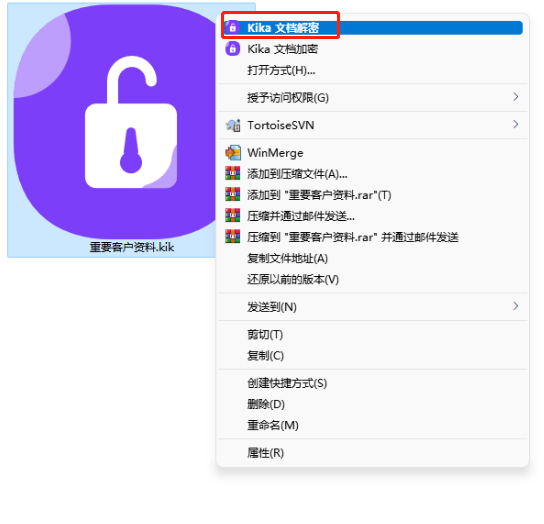
选择文件或者文件夹，点击右键，选择“Kika文档加密”，如图：



将生产一个同文件名，后缀为kik的文件。加密后，将继续保持原文档，由用户确定是否将原文文档删除，以保证安全性。

* 1. 文件解密

选择kik后缀的加密文件，点击右键，选择“Kika文档解密”，如图：



加密不需要任何权限，解密需要获得使用安全鼠标权限，将弹出登录页面，要求用户输入指纹或者口令（如果用户已经处在登录状态，则无需重复确认身份），如图：



口令确认后，将还原明文文件，获得之前加密的文件。

# 用户须知

* 1. 常见问题

1. 指纹识别原理是什么？

指纹识别技术是利用人类指纹的唯一性，通过采集[指纹图像](https://www.zhihu.com/search?q=%E6%8C%87%E7%BA%B9%E5%9B%BE%E5%83%8F&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra=%7B%22sourceType%22%3A%22answer%22%2C%22sourceId%22%3A1531364273%7D)进行比对来识别身份的一种技术。指纹识别需要先采集指纹并对指纹进行DSP图像处理从而生成细节清晰的指纹图像来进行对比给出结果。指纹识别芯片/传感器，就是内嵌的芯片产品，可以实现上述的指纹图像采集、特征提取、对比的芯片。

本方案选用的是电容压感式指纹传感器模块，采集的点整数为96X96pix。

1. 如果指纹识别受伤或者不方便怎么办？

本安全鼠标除了提供指纹方式验证身份之外，还允许使用口令/PIN码方式认证。

1. 如果安全鼠标丢了怎么办?

安全使用口令管理功能具有本地备份功能，能够将保存在安全鼠标中的口令通过安全的方式备份到PC端，并在需要的时候导入新设备。所以只要及时备份，就可以避免众多的口令丢失。

另外保存在USBKey中的秘钥由于安全性考量，禁止备份和导出。如果安全鼠标丢失，则需要重新申领设备，重新认证颁发证书即可。

1. PKI体系是什么？

公钥基础设施(Public Key Infrastructure, PKI)是典型的密码学应用技术。在 PKI系统中， 由证书认证机构(Certification Authority, CA)签发数字证书、绑定 PKI 用户的身份信息和公钥。PKI依赖方(Relying Party)预先存储有自己所信任的根 CA 自签名证书，用来验证与之通信的 PKI 用户的证书链，从而可信地获得该用户的公钥、用于各种安全服务。

由于安全鼠标内置安全芯片设计为标准USBKey，可以使用PKT体系对秘钥安全存储、管理、运算，实现身份认证，加密接等工作。

* 1. 使用须知

1. 指纹采集芯片应避免硬物划伤传感器表面；
2. 避免淋雨、过度灰尘、高湿环境；
3. 指纹采集传感器应该定期清洁，棉签或无尘布粘少许酒精或白酒擦拭；
4. 指纹手指采集，必须要经过手指按下-弹起为一完整过程；
5. 产品操作演示视频（请扫二维码）；



演示视频 更多资讯 奇甲公众号

* 1. 装箱清单

|  |  |  |  |
| --- | --- | --- | --- |
| SN | 物品名称 | 数量 | 单位 |
|  | 安全鼠标 | 1 | 个 |
|  | 检验凭证 | 1 | 张 |
|  | 包装盒 | 1 | 个 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |