

# 恺迹信息科技有限公司



超小款



短款



长款7



长款Y



## *LiViKey*加密锁使用说明

上海恺迹信息科技有限公司

[www.ivikey.com](http://www.ivikey.com)

## 软件开发协议

ViKey 系列加密锁的所有产品，包括但不限于：开发工具包，磁盘，光盘，硬件设备和文档，以及未来的所有定单都受本协议的制约。

### 1. 许可使用

您可以将本软件合并、连接到您的计算机程序中，但其目的只是保护该程序。您可以以存档为目的的复制合理数量的拷贝。

### 2. 禁止使用

除在条款 1 中特别允许的之外，不得复制、反向工程、反汇编、反编译、修改、增加、改进软件、硬件和产品的其它部分。禁止对软件 and 产品的任何部分进行反向工程，或企图推导软件的源代码。禁止使用产品中的磁性或光学介质来传递、存储非本产品的原始程序或由我方提供的产品升级的任何数据。禁止将软件放在服务器上传播。

### 3. 有限担保

我方保证在自产品交给您之日起的 12 个月内，在正常的使用情况下，硬件和软件存储介质没有重大的工艺和材料上的缺陷。

### 4. 修理限度

当根据本协议提出索赔时，我方唯一的责任就是根据我方的选择，免费进行替换或维修。我方对更换后的任何产品部件都享有所有权。

保修索赔单必须在担保期内写好，在发生故障 14 天内连同令人信服的证据交给我方。当将产品返还给我方或我方的授权代理商时，须预付运费和保险。

除了在本协议中保证的担保之外，我方不再提供特别的或隐含的担保，也不再对本协议中所描述的产品负责，包括它们的质量，性能和对某一特定目的的适应性。

### 5. 责任限度

不管因为什么原因，不管是因合同中的规定还是由于刑事的原因，包括疏忽的原因，而使您及任何一方受到了损失，由我方产品所造成的损失或该产品是起诉的原因或与起诉有间接关系，我方对您及任何一方所承担的全部责任不超出您购买该产品所支付的货款。在任何情况下，我方对于由于您不履行责任所导致的损失，或对于数据、利润、储蓄或其它的后续的和偶然的损失，即使我方被建议有这种损失的可能性，或您根据第 3 方的索赔而提出的任何索赔均不负责任。

### 6. 协议终止

当您不能遵守本协议所规定的条款时，将终止您的许可和本协议。但条款 2, 3, 4, 5 将继续有效。

# 产品列表

ViKey 系列加密锁	
ViKeyAPP	实用型加密锁
ViKeySTD	标准型加密锁
ViKeyNET	网络型加密锁
ViKeyPRO	专业型加密锁
ViKeyWEB	身份认证型加密锁
ViKeyTime	时间型加密锁
更多产品信息，请登录 <a href="http://www.ivikey.com">www.ivikey.com</a> 网站或直接联系我们 TEL:18917081416	

加密锁功能简介 .....	5
1、产品概述 .....	6
1.1 功能特点 .....	6
1.2 开发接口提供 .....	7
1.3 开发例子提供 .....	7
1.4 操作系统支持 .....	7
2、产品属性介绍 .....	8
2.1 硬件 ID (HID) .....	8
2.3 用户密码 .....	8
2.4 管理员密码 .....	8
2.5 密码尝试次数 .....	9
2.6 操作权限 .....	9
3、产品出厂默认设置 .....	10
4、快速入门 .....	11
4.1 演示例子的使用 .....	11
4.2 如何使用加密锁来保护软件 .....	12
5、开发流程 .....	14
5.1 API 接口调用方式 .....	14
5.2 API 调用操作流程 .....	15
6、联系我们 .....	16

## 加密锁功能简介

**加密锁**——又称为加密狗，是一种插在计算机并行口/USB 接口上的软硬件结合的加密产品。加密锁一般都有几十、几百或几千字节的用户数据存储空间(非易失性存储器)，通常需要正确校验用户密码后才能对它进行读写操作，且密码校验失败次数是有限制的。

软件开发者可以通过接口函数和加密锁之间进行数据交换（即对加密锁进行读写操作），来检查产品配套的加密锁是否插在并行口/USB 接口上，如果没有插入或中途拔出了，则立即终止软件运行，或者使软件错误运行。软件开发者还可以在不同时间段，比如 1 月、2 月……，读取加密锁（用户数据存储空间的）不同位置的数据，并判断数据是否正确，然后控制软件是否正常运行；软件还可以根据数据的不同，来识别不同的操作员，然后相应的开放/禁止软件的某些功能。或者把程序的一小部分代码或运行参数写到加密锁上，运行前再从加密锁读出，并放到内存的相应位置上，如果没有相应的加密锁，程序将无法正确运行。或者直接用加密锁附带的工具加密自己的EXE 文件（俗称“包壳”），如果没插相应的加密锁，则软件将不能正常执行。软件开发者可以在软件中设置多处软件“锁”，利用加密锁作为钥匙来打开这些“锁”，这样就使用加密锁来保护了开发者的软件成果。

# 1、产品概述

ViKey系列加密锁(又称为加密狗)是专门针对广大软件开发公司而设计的一款基于USB 接口的高性能、低价格的加密锁。该加密锁使用简单、操作方便,非常适用于软件加密保护、关键数据保存、安全系统身份认证领域,包括网站系统、OA 办公系统、信息查询系统、教学软件或其它行业软件等等。

ViKey系列加密锁无需安装驱动程序,内置数据存储区(分为用户数据存储区和管理员数据存储区);数据存储区支持写次数10 万次以上,读取次数不限;内置32 bit位全球唯一硬件ID,方便查询各个加密锁的使用情况或用于软件加密处理;自定义两个8位密码,加强解密难度(密码校验次数默认为10 次);如果尝试错误密码超过设定的密码尝试次数,加密锁将自动锁定,以后无法登陆,防止了他人对加密锁的暴力破解。具有防复制功能;具有智能防跟踪功能;通信格式采用密文格式进行通信;支持多个设备在同一台计算机上使用。

ViKey 系列加密锁是完全基于智能卡技术开发,芯片集成了其所有器件(包括CPU、RAM、EEPROM 以及 USB 通讯模块),极大地提高了产品的安全性和稳定性。每个芯片上都具有 32 bit 位全球唯一的序列号(即硬件 ID)。

## 1.1 功能特点

无需安装驱动程序;

提供32 bit位全球唯一硬件ID;

支持在同一台 PC 上插入多把加密锁;

单操作员管理机制(普通用户);

双密码增强密钥;

密码校验默认次数为 10 次(管理员可修改);

提供 最大2K字节用户数据存储空间;

提供 最大2K字节管理员数据存储空间;

设备与程序之间采用密文通信;

设备具有反跟踪功能;

设备上的数据采用 3DES、MD5 加密,即使剖开芯片也是读不到加密数据;

设备具有防复制功能;

工作电流 23mA/5V (典型值,指示灯为点亮状态)。

## 1.2 开发接口提供

LIB 静态库方式;

DLL 动态库方式;

COM 组件方式;

Active 控件方式;

外壳加密方式。

注：开发接口方式在不断增加中，请到我们网站 <http://www.ivikey.com> 查看最新支持的开发接口类别。

## 1.3 开发例子提供

应用程序：VC++、JAVA、Delphi、BCB、C#、VB、PB、FoxPro、VB.NET、BC++、VFP、QT、Excel、Python、Power Builder、易语言、HTML、ActiveX、LabView、ACCESS、ASP、ASP.NET、JSP、PHP等

网站网页：ASP、ASP.net、PHP、JSP

注：开发例子在不断增加中，请到我们网站<http://www.iViKey.com> 查看最新例子。如果没有你需要的例子，请您联系我们的技术工程师，免费为您增加。

## 1.4 操作系统支持

支持 Windows 全系列

如 Windows 98SE/Me/2000/XP/Server 2003/Vista/Win7/Win8/Win10/Win11;

支持嵌入式 Windows CE (即 WINCE)、Windows Embed XP;

支持 Linux32/64;

支持 Arm32/64;

支持 Mac OS。

## 2、产品属性介绍

### 2.1 硬件 ID (HID)

硬件ID是一个32bit位的一个编号，由加密锁在制作过程中固化在加密芯片中的一组硬件编号(不可修改)。每一个加密锁的设备编号都是不相同的，即全球唯一。该编号可以用作跟踪各个加密设备使用情况，如防代理商窜货等等功能；也可以用来作为加密算法中的一个加密条件，增强产品的安全性。

### 2.3 用户密码

用户密码是8位的字母或数字。

用户密码是保障普通用户权限的一个密码。如果校验的密码不正确，加密锁的操作权限只能进行各种匿名权限操作。如果校验正确，则加密锁将把权限提升用户权限。用户权限可以修改用户密码、读写数据及各种匿名权限操作等。。

### 2.4 管理员密码

管理员密码是8位的字母或数字。

管理员密码是保障管理员权限的一个密码，由于这个密码权限非常高级，一般应掌握在开发商核心管理人员手中。如果校验的密码不正确，加密锁的操作权限只能进行各种匿名权限操作。如果校验正确，则加密锁将把权限提升管理员权限，可以进行全部操作，如设置产品名称、软件 ID、修改普通用户密码，设置密码校验次数、读写数据等。



## 2.5 密码尝试次数

密码尝试次数是校验密码时连续错误的最大次数，每校验错误一次则加密锁会对校验次数自动减一，当减至0 次时则对该密码锁死(即不再允许校验此密码)；如果在未锁死之前校验密码正确，则加密锁会自动恢复校验次数为到原设置值。 如果超过了密码尝试次数，加密锁立刻被锁定 之后即便是输入正确的密码也不会激活加密锁。该机制类似于银行卡密码机制，有效防止黑客暴力破解加密锁。

例如，设置用户密码校验次为3 次，如果连续执行3 次校验用户密码错误，则加密锁就把用户密码锁死。如果用户在第2 或第3 次时校验密码正确，则把密码校验次数又恢复到3 次。

对于 ViKey 加密锁，其用户密码尝试次数出厂设置为 **10** 次，如果普通用户密码锁死，可用管理员登陆后将该次数修改为非 0，则解锁。但是如果管理员密码被锁死，只能退回我们，给予修改。

## 2.6 操作权限

用户权限是加密锁对不同用户的权力分配/操作限制，ViKey系列加密锁包含三种权限，如下所示

### 匿名权限

### 普通用户权限

### 管理员权限

加密锁插入计算机后在不登陆或者登陆失败的情况下处于匿名权限状态；

当校验用户密码正确时 (**VikeyUserLogon**)，加密锁将把权限提升为用户权限。如果校验失败，加密锁将返回到匿名权限状态。

当校验管理员密码正确时 (**VikeyAdminLogon**)，加密锁将把权限提升为管理员权限。如果校验失败，加密锁将返回到匿名权限状态。

在《ViKey加密锁-API开发手册.pdf》的API 函数说明中，每一个API 函数都会指明其用户权限类别，即表示在什么用户权限下可调用此API 函数。

### 3、产品出厂默认设置

- 用户密码: “111111”            每个密码为 8 位
- 管理员密码: “000000”        每个密码为 8 位
- 用户密码尝试次数: “10”      范围 0~255
- 管理员密码尝试次数: “10” 范围 0~255
- 软件 ID: “1234ABCD”        长度为 8 位
- ViKeyWeb 的 MD5Key: “FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF”。 32 字节
- 存储空间的内容全为 0;
- ViKeyTime 加密锁的时间默认是北京时间

## 4、快速入门

如果您是第一次使用ViKey系列加密锁，请先阅读本手册的第1~3章的内容，以便于对此产品及相关术语有所了解。

本章内容分为两部分，第一部分是介绍使用ViKey系列加密锁的Demo(即演示例子)来进行各种操作，可以使您对ViKey系列加密锁有基本的、直观的认识；第二部分介绍如何使用加密锁来保护软件，帮助您对使用加密锁来加密软件的基本原理和思路有所了解。

### 4.1 演示例子的使用

#### (1) 获得软件开发包

ViKey 系列加密锁软件开发包参考如图 4.1 所示，用户可以通过官网([www.ivikey.com](http://www.ivikey.com)) ->下载中心下载



#### (2) 将加密锁插入到 PC

将 ViKey 系列加密锁插入到 PC 机的 USB 接口，参考如图 4.2 所示，此时 ViKey 系列加密锁的指示灯会点亮。



### (3) 观看操作视频教程

打开SDK开发包，然后进入“1-[文档及视频教程]”目录，进入“视频教程”目录。双击运行“ViKey帮助工具.exe”，将会出现如图4.3所示的主界面。



观看视频教程，按照视频教程操作就可以了

## 4.2 如何使用加密锁来保护软件

使用加密锁来保护软件(即对软件进行加密)，主要是保护软件不被非法复制和使用，非授权访问或操作。使用加密锁对软件进行加密的形式是多种多样的，但最基本的原理是软件开发商编写的程序通过API接口函数和加密锁之间进行数据交换（即对加密锁进行读写操作），检查产品配套的加密锁是否插在USB接口上，如果没有插入或中途拔出了，则立即终止软件运行，或者以错误的方式运行，示意图如图4.15所示。由于加密锁具有各种功能特性，如硬件ID、软件ID、用户权限(密码)管理、用户数据存储区、密文通信、防反跟踪功能等等，使它具有不可复制性，所以软件也就具有不可复制性。

另外，软件保护的强度不仅仅依赖加密锁本身，很大程度也和软件开发者如何使用加密锁相关，所以软件开发者要充分利用加密锁的功能，在软件中设置多处不同形式的“锁”，利用加密锁作为钥匙来打开这些“锁”。

### (1) 加密锁的基本用法

加密锁一般都有几十、几百或几千字节的用户数据存储空间(非易失性存储器)，通常需要正确校验用户密码后才能对它进行读写操作。软件开发者可以在不同时间段，比如1月、2月、3月……，读取加密锁用户数据存储空间的不同位置的数据(这此数据是由软件开发商预先写进去的)，并判断数据是否正确，然后控制软件是否正常运行。

软件开发者可以让软件根据加密锁的存储数据的不同，来识别不同的操作员，然后相

应的开放/禁止软件的某些功能。通过使用加密锁来替换传统的用户名和密码，保证了系统的登录安全。

软件开发者可以把程序的一小部分代码或运行参数写到加密锁上，运行前再从加密锁读出，并放到内存的相应位置上，如果没有相应的加密锁，程序将无法正确运行。软件开发者可以使用硬件ID(即HID)和数据进行运算，再根据运算结果来控制程序是否运行。

以上介绍的都是调用API来加密软件的方式，这需要结合软件的源程序来进行。另外，还可以直接用加密锁附带的工具来加密EXE文件（即外壳加密），如果没插相应的加密锁，则软件将不能正常执行。

说明: ViKey系列加密锁中只有ViKeyWeb不支持外壳加密。

## (2) 提高软件的加密强度

对于调用API来加密软件的方式，软件开发者可以在程序设计上做一些处理，以提高软件的加密强度，参考如下：

- 在程序的各个部分插入校验算法的代码，不要简单的、统一的调用同一个函数来校验，这样就增加程序代码的复杂度
- 在程序的各个部分插入校验算法的代码，不要简单的、统一的调用同一个函数来校验，这样就增加程序代码的复杂度
- 校验代码插入程序中的地方越多，破解难度越大，软件就越安全
- 充分利用加密锁的功能，利用不同的时间、存储空间，尽量使用多种不同的校验方式。这样的话，只要破解者没有枚举/探测完所有的访问方式和校验方式，软件就不会被真正破解
- 可以对加密锁进行一些随机性的、无关的操作，如读写没有用到存储空间
- 重要的字符串在程序中尽量不要以明文出现(比如要通过 2 个数组相“异或”才得到)
- 用户密码和硬件 ID 不要以字符串形式出现，应使用多个数组来分开保存，甚至可以通过 2 个数组相“异或”才得到
- 最好使用动态密码，即每个加密锁的用户密码与它的 HID 有关联
- 最好能检查 EXE 或 DLL 文件的完整性

## 5、开发流程

本章内容将会介绍 ViKey系列加密锁的API 接口调用方式和基本操作流程，然后以 Visual Studio 2008 为开发平台，分别使用LIB 静态库方式和DLL 动态库方式举例，实现对ViKey系列加密锁的基本操作(没有涉及软件保护方面的设计)。例子程序中的代码简单明了，也没有使用任何特殊技巧，所以使用其它语言的软件开发人员都可以把它作为参考。说明：例子中所用到的API 函数的介绍，请参见《ViKey加密锁-API开发手册.doc》。

### 5.1 API 接口调用方式

ViKey系列加密锁提供有多种API 接口调用方式，具体如下：

#### LIB 静态库方式

该方式的好处是编译生成的 EXE 文件可独立运行，无需附带其它文件，也无需向系统注册相关文件。目前只支持**Visual C++** 和**Boland C++**两种开发语言。

使用 LIB 静态库的操作方法是：在开发软件时，把ViKey.LIB 及ViKey.H 文件复制到工程目录下，然后在工程设置中包含它们，这样就可以在程序中调用相应的API 函数了。

#### DLL 动态库方式

该方式是大多数编程语言都支持的一种开发方式，用户只需在程序中进行声明，然后再调用相应的API 函数即可，程序在运行时必须保证ViKey.DLL 文件在系统目录下或在此EXE文件的同一目录下。

#### COM 组件方式

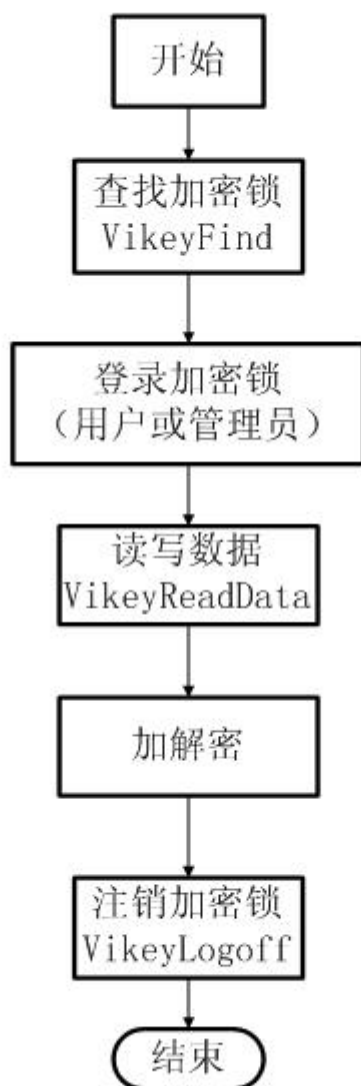
该方式也是绝大多数编程语言都支持的开发方式，**COM** 组件提供了相应的API 接口，程序运行时必须保证ViKey.DLL 组件已存在，并且已注册。

#### Active 控件方式

该方式也是绝大多数编程语言都支持的开发方式，**Active X** 控件提供了相应的API 接口，程序运行时必须保证ActiveX.Dll 控件已存在，并且已注册。

## 5.2 API 调用操作流程图

不管使用哪一种 API 接口调用方式，其操作流程都是相似的，参考如图 5.1 所示，具体代码请参考产品配套 SDK 开发包内的示例程序。图中的“设备”，指的是加密锁，后面的说明中也有这样的表述。



## 6、联系我们

### 用户反馈

我们非常欢迎用户对我们的产品的任何反馈，请与我们直接联系，我们会给您满意的答复。

官方淘宝店:<https://ivikey.taobao.com/>

电话：18917081416

QQ:3243647362



客服微信