

ROCKEY SMART 软件跨平台保护方案

飞天ROCKEY SMART是我公司最新推出的一款高强度智能卡加密锁。具有高度的安全性、并提供跨平台软件保护整体解决方案。通过它，开发商可以方便的实现产品的租赁、试用、按模块销售等多种销售模式，彻底杜绝软件盗版。下面我们简要介绍一下它的特点以及如何利用它为我们提供高强度的加密保护。

一、ROCKEY SMART 具有以下的特点

硬件上的安全性

ROCKEY SMART型加密锁是以智能卡硬件为核心。智能卡芯片都具有很高的集成度，与普通低档的单片机不同，只有已通过国际安全机构检测和认证(EAL 4+和IT SEC认证)的专业安全芯片制造商才能提供智能卡芯片。智能卡芯片是经过安全性设计的芯片，物理能够有效抵御电子探测攻击(SPA和DPA)和物理攻击(SiShell)，其在硬件设计阶段就提供了完善的安全保护措施。它通过芯片厂商开发，通过产生额外的噪声和干扰信号，或通过增加滤波电路来消除噪声，再加上若干保护层，采用特殊的材料(对电子束敏感的材料)等，使监测芯片内执行的指令序列不可能实现。同时智能卡芯片提供了硬件随机数发生器，在CPU的控制下，每次芯片与外界数据传输中，产生的随机数可以保证数据不会重复。智能卡硬件以其可靠的安全保障性能广泛应用于军事、金融、保险等国民生计的重要领域。ROCKEY SMART使用了最新一代的智能卡硬件，在物理安全的基础上还提供了强大的运算和数据处理能力，为我们实现各种复杂的安全协议提供了坚实的基础。

软件上的安全性

ROCKEY SMART集成了COS和虚拟机技术，COS提供了文件管理、安全管理、内层管理、输入输出管理等各种功能，通过COS提供的功能，可以保证数据的安全存储、数据的安全访问等各种应用。虚拟机技术提供了一种CPU的指令集支持和基于此指令集的开发接口及开发环境。通过虚拟机的支持，用户的核心算法和数据可以转移到智能卡内部，并在智能卡内部运行，在智能卡操作系统的管理下，形成

一个与计算机平行的小型计算机系统，并通过USB接口同计算机交换数据。保证在可靠解决方案和一定的算法复杂度的前提下，程序被破解的可能性等于零。

产品的易用性

ROCKEY SMART的易用性主要体现在两方面

1. 用户算法的开发上

ROCKEY SMART的虚拟机提供了C语言为标准开发语言，并且提供了文件操作、各种双精度浮点数学运算、RSA、DES标准加解密等丰富的开发接口函数库。为用户移植核心算法提供方便。

2. 产品的维护上

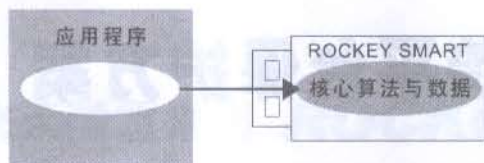
为了增加产品的整体稳定性和维护方便，ROCKEY SMART我们使用标准的系统类驱动。从而保证和系统有更好的兼容性。开发商也可以避免对第三方产品驱动的维护。

集先进技术于一身，拥有无限的延展性

ROCKEY SMART以文件系统为核心，并根据用户管理方面的需求，加入了很多管理上的先进技术(例如：一次一密的远程升级方案)。我们把加密领域的各种要求分解为加密锁最基本的功能，用户可以从这些最基本的功能构建出各种复杂的保护方案，并同时拥有最大的灵活性。

二、ROCKEY SMART 的高强度加密保护

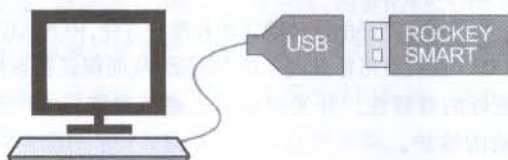
ROCKEY SMART通过COS强大的文件系统管理和安全机制、虚拟机提供的丰富的开发接口和ROCKEY SMART快速的数据交互速率，为用户实行高强度加密保护提供了保证。采用ROCKEY SMART保护软件，您可以将程序的一部分写入到ROCKEY SMART中而不必在主机上保留这一部分程序的副本，程序运行时也不会出现在计算机的内存中出现，这就杜绝了程序被跟踪调试和转储的可能。写到加密锁中的程序称为外置程序，它们存储于电可擦可编程只读存储器(EEPROM)中。一个加密锁中可以写入多个外置程序，且外置程序之间可以有调用关系，然而主程序一次只能激活一个外置程序。很明显，软件离开了加密锁就不可能正常工作。



ROCKEY SMART 保护软件示意图

当客户使用带有ROCKEY SMART保护的软件时,只需把加密锁当成一般的USB设备插在USB接口上就可以正常使用该软件了。

当主程序执行到一个外置程序时,会向ROCKEY SMART 发送调用的命令,并且传递相应的参数。ROCKEY SMART响应主程序的命令,执行相应的程序,把结果返回给主程序。继续等待,直到接收到下一个命令。



使用带 ROCKEY SMART 的软件

1. ROCKEY SMART 的文件系统与安全机制

ROCKEY SMART 以文件系统的安全为依托,为用户的软件提供了非常完善的安全保障。下面先介绍一下文件系统的几个相关概念。

1.1 文件类别

文件类别(FCLA)是文件的分类标志,类别编码相同的文件一般会被假定为同一产品的文件。它以一个字节来表示,取值为(0x00~0xFF)加密锁内部的可执行文件受到类别码的限制,只能够读写和创建相同类别码的数据文件。关于类别有如下的规定:

1) 0xFF 表示“无类别”,这个类别的数据文件可以被任何类别的可执行文件访问,而这个类别的可执行文件只能访问类别为0xFF的数据文件。

2) 系统根目录的类别是“无类别”。

3) 在加密锁中,相同类别的文件构成一个相对独立的子系统,“无类别”数据文件是公共数据,“无类别”可执行文件是公共处理程序。

1.2 文件安全级别

除了类别以外,每个文件还有一个“安全级别”

来限制相同类别文件的访问控制,即安全级别是针对相同类别文件设置的。

在具体的实现中,安全级别占用一个字节的低四位(0x00-0x0F),与属性(占高四位)合成一个字节,分为16个不同的权限,其中0是最低级,15是最高级。

安全级别是更高层次的文件管理功能,如果用户不需要这么复杂的管理功能,把所有的文件安全级别都设定为0即可。

1.3 文件属性

属性有五种,分别是普通、内部使用、高于忽略、目录和可执行文件。一个目录或文件可以有多个属性。

“普通”属性没有任何的特殊性,如果不设置,就默认为此属性。

“可执行”属性指出文件是否为一个能在COS上运行的文件,这种文件必须放在加密锁的根目录下,而且只有在超级密码验证通过后才能创建和删除。

“目录”属性表示这是一个子目录,如果这个属性被设置,其它属性位会被忽略。

“高于忽略”属性只对加密锁内部的可执行文件有效,表示这个可执行文件只在系统安全级别低于可执行程序自身安全级别的情况下才运行,若系统安全级别已经高于或等于可执行文件自身的安全级别,这个文件就不执行。

“内部使用”如果是数据文件,表示这个文件只能由加密锁内部的可执行文件来访问,外部操作只有在超级密码验证通过后可以删除,但不可以读写。没有超级密码验证通过的时候根本不允许外部访问。如果是可执行文件,表示这个文件有隐含的属性,在列目录时,如果没有通过超级密码验证,有隐含属性的可执行文件就不会显示出来,这也是对可执行文件的一种保护。

使用API创建可执行文件与内部文件时,要求处于超级密码验证通过状态。

1.4 安全机制

ROCKEY SMART安全机制的核心在于“系统安全级别”,它和文件的安全级别一样,都是16级。“系统安全级别”与“文件安全级别”相配合以提供整个卡片的完全控制。具体来说,我们如果需要操作卡内的某些文件,就必须让“系统安全级别”高于或等于“文件安全级别”,而改变“系统安全级

别”的方法只有两个：一是校验“超级密码”，另一是通过在虚拟机上运行的可执行程序。

在COS的实现中安全机制分成三个部分分散在系统中，下面加以简介：

1) 全局的安全

我们使用一个8字节的“超级密码”作为全局的安全策略。超级密码是由ROCKEY SMART生产厂家提供给软件开发商，且可以由软件开发商自己修改或废除的一个口令字。当正确的超级密码送入卡内验证后，“系统安全级别”会设为最大值，卡内所有普通数据文件（不包括内部使用的）都可以读出到卡外或由卡外予以更新，而可执行文件只能被“选择/删除”。另外，如果想在卡内建立可执行文件，也必须先验证超级密码。当开发商把超级密码修改为全0以后，超级密码就不能够再被修改或验证。这相当于废除了超级密码，任何人再也无法获得超级用户的权限，请慎用。

2) 文件系统的安全

文件系统的安全包括两点内容，一是文件类别的应用，这主要为了将文件归于不同组，不同类别的文件其安全级别互相独立。另外文件类别也用于限制在虚拟机上运行的程序不能访问与其分属不同类别的数据文件。二是当可执行程序操作其它数据文件时，COS会检查可执行程序的安全级别是否高于或等于待操作的数据文件的安全级别。

3) COS的安全限制

当运行中的可执行程序如果需要改变“系统安全级别”时，COS会限制应用程序设置的安全级别不会超过它本身设定的安全级别。

2. ROCKEY SMART 的虚拟机开发

ROCKEY SMART提供了C语言支持，便于用户开发虚拟机程序。虚拟机系统为用户提供了丰富的开发接口函数。接口函数包括文件操作函数如文件的创建、读写等，数学函数如双精度浮点的余弦、开方等各种数学运算、安全管理函数如改变系统安全级别、数据处理函数如RSA、3DES等。用户可以利用这些接口函数开发各种应用的算法。

3. ROCKEY SMART 的快速数据交互和高速数据处理

为了更好的用户算法实现和效率，ROCKEY SMART

提供了快速数据交互和高速数据处理，千次的浮点数学运算都保持在毫秒级。

三、利用 ROCKEY SMART 拓展销售模式、丰富软件升级方案

ROCKEY SMART集成了远程升级、安全文件传输、多模块管理等多种开发接口和工具。开发商可以方便的实现产品的租赁、试用、按模块销售等多种销售模式，并进行防盗版管理。

1. 软件的试用

利用ROCKEY SMART,开发商可以构建多种不同的软件试用销售模式，并进行防盗版的管理。

1.1 限制使用次数

ROCKEY SMART内置有计数器，每使用一次加密锁，计数器就减1，当计数器减到0后，加密锁就无法再使用，如果用户还想继续使用该软件只有到开发商那里重新购买。

1.2 控制使用时间

ROCKEY SMART内置有计时器，开发商可以记录用户每次使用软件的时间，当时间超过限值时，开发商就可以让软件无法再使用，这些控制都是在加密锁内完成。彻底杜绝了被破解的可能。

1.3 功能限制

开发商可以利用提供的远程升级或远程模块管理功能，将不同的功能划分到不同的模块中，然后根据用户的要求开通相应的模块。用户只能使用开通的这些模块。这样开发商就达到了限制软件功能的目的。

2. 软件的升级和维护

ROCKEY SMART提供了灵活的软件升级方案，开发商可以根据实际情况采用相应的方案。

2.1 远程升级

在远程升级管理中，只有两个相关的概念即“远程升级标志”和“远程升级密码”。

远程升级标志 - RemoteTag，是开发商为了标识当前软件的升级状况设定的信息，通常我们建议把您的软件版本号写在这里，这样开发商就能够知道用户要从哪个版本向那个版本升级。

开发商提供给客户的 RemoteTag 和 RemotePass 是相关的，用户不能修改其中的任何一个，如果 RemoteTag 的最高位是 1，那么升级密码只针对特定的加密锁有效。而用户提供给开发商的信息中，

只有硬件 ID 和上一次的升级密码是必要的,上一次的 RemoteTag 是作为开发商升级参考用的信息,对下一次的升级信息没有影响,开发商在每次升级的时候都应该给出一个跟以前不同的 RemoteTag 作为升级的标志。

远程升级可以分为以下四个步骤:

1) 设置远程升级标志和密码

这一步骤是在开发商在加密锁交给最终用户前做的初始化工作,这个工作只能做 1 次,一旦远程升级标志和密码被设定,开发商也无法直接修改,必须对加密锁进行重新格式化之后才能重新设定基本远程升级密码。

2) 读出远程升级信息和加密锁的硬件 ID

当用户需要进行远程升级的时候,软件在用户端获得相关的信息(包括“用户当前标志”、“用户当前密码”和“硬件 ID”),并把这个信息通过某种方式发送到开发商那里。

3) 提升权限为超级用户,并获得当前远程升级密码的下次升级密码”。

这是开发商在获得用户发来的相关信息后,为指定用户获得下一次的升级密码。并把新的升级密码和升级标志发送给用户。

4) 验证升级的远程升级密码并检查是否远程升级密码验证通过了

当用户从开发商那里获得新的升级密码和升级标志后,就可以把新的密码和升级标志送到加密锁中进行验证。验证成功后,加密锁中的远程升级标志会被置位,程序可以检查这个标志来决定相关的动作。

2.2 安全文件传输

我们的加密锁支持安全文件的传送功能。对于开发商来说,一旦把加密锁卖到用户的手中,虽然可以通过远程升级功能来保证用户身份的有效性,但无法再更新用户手中加密锁的算法了,因为用户在没有超级密码验证的情况下,是不允许写入算法程序的。安全文件传输的功能可以让开发商在不验证超级密码的情况下,更新用户加密锁内部的算法或数据文件,而这个更新过程是安全的,完全不用担心文件内容泄漏的问题。

这个操作的基本流程如下:

(1) 开发商首先用自己手上的加密锁将文件生成“密文文件”。

(2) 把这个密文文件发送给用户。

(3) 用户利用开发商提供的程序把“密文文件”送入加密锁,由加密锁在锁内还原成明文文件。

在安全上我们做出如下的保障:

(1) 密文文件和明文文件的算法是完全保密的,不对任何人公开。

(2) 密文文件和明文文件的生成过程完全在加密锁内部完成,没有任何外部工作。

(3) 加密和解密的密钥同加密锁相关,不必担心有人能制造出能够在您客户手上加密锁使用的密文文件。

(4) 密文文件的内容不可修改。

3. 远程模块管理

远程模块管理就是将外置程序按模块分成几个部分,你可以选择开通或关闭其中的一个或几个部分,只有被开通外置程序才能被用户访问,从而达到模块控制的目的。

远程模块管理包含三个部分,设置模块定义文件、生成模块授权文件和对加密锁模块信息进行批量设置。对于开发商来说,只需要两个步骤即可完成远程模块管理,首先利用模块定义功能定义一个模块定义文件,并把它发送给用户,用户根据自己所购买的模块将根据模块定义文件生成模块需求文件,开发商根据模块需求文件生成模块授权文件,并发送给用户,用户拿到模块授权文件后即可对加密锁进行升级。如果开发商清楚每个用户所需要的模块,第一步也可以由开发商自己来完成。

四、利用 ROCKEY SMART 建立软件跨平台保护方案

ROCKEY SMART 可应用于多种操作系统下,支持 win98/Me/2000/XP/2003, Linux, Mac OSX 平台。我公司提供的开发接口在各个平台上均保持一致。在源代码级提供跨平台支持。

