

抢先体验 ROCKEY4 SMART

摘要

在使用某些软件的过程中，人们常常会遇到弹出“软件试用期还剩10天”或“软件已到期，请联系开发商”之类的窗口。这类软件授权限期使用的应用模式可能大家都有一定程度的了解，如果用户想继续使用的话，就需要获取开发商的新的授权。对于开发商来说，不仅要对软件进行加密、授权，还要对已售出的产品进行跟踪，以便当用户要求时，提供新的授权。如果您是一个软件开发商是否也曾尝试过开发一个这样授权管理体系的应用模型呢？当然实现一个完善而易用的授权管理是一个比较复杂的过程，涉及到对称加密算法、数据库编程、GUI开发、时间检测及授权控制，并且开发时要详细分析授权、分发、进行新的授权等每一个步骤的软件使用状态等多个方面。如果没有一个成体系的设计方案，开发商很难做到面面兼顾，容易造成管理混乱、效率低下，甚至于无法对客户授权要求及时做出反应……

但随着 ROCKEY4 SMART 的发布这一切将都可以迎刃而解了，此产品就是一款集加密、授权、分发、管理于一体的新一代加密产品，为开发商的软件授权管理提供了一整套解决方案。

ROCKEY4 SMART 有几个显著的特点，首先，ROCKEY4 SMART 使用的是智能卡芯片，这使得此产品有了很好的对抗常应用于单片机攻击方法的先天特性，如探针式、电压式、噪声等攻击方法。在硬件级提供了对授权管理的强力支持，在硬件内部模拟了一个软件时钟用于软件使用时间的控制。它既吸取了早期时钟锁的优点，同时又不需要电池，利用内置的计时功能可以很容易实现限期功能（即软件租赁）或从试用版授权到正式版。不仅如此，锁内还内置了 RSA 引擎，基于 RSA 引擎实现升级功能可对整段的授权信息

使用 RSA 算法进行加密，并结合一次一密，升级过程更加将安全。

授权管理平台这产品的核心操作界面，用于对客户授权的管理、维护、升级和分发，另外还有一些用于授权管理的辅助工具，如外壳加密工具、批量生产工具以及客户升级工具等。外壳加密工具可以实现对软件的外壳加密，这个外壳加密不同于常见的其它外壳加密工具，它充分利用了 ROCKEY4 SMART 锁的内置功能，在加密的同时可同步记录与授权相关操作，这使得在后续使用授权管理平台软件时可以很容易地实现与外壳工具进行互动。即使用户对加密技术不是十分了解，也可以很容易地利用这个工具对软件加密，集成授权使用期限等功能。

ROCKEY4 SMART 的开发背景

在软件加密的历史进程中，软件加密的方式与软件销售的模式有密不可分的联系，当销售模式发生变化时，与之对应的一种新的加密方式就会应运而生。随着互联网的不断发展，通过互联网发售软件，先试用后付费的软件发售方式得到了越来越多的客户的认可，同时电子商务及网上支付也日渐兴起。对于一个最终用户来说几乎可以足不出户，很快就能下载到一份试用版的软件拷贝，同时通过网上支付系统用户可很快就能得到一份软件正式版的许可文件。新的销售模式固然有其吸引人之处，但是对于一些售价相对较高的软件来说，纯软方式的许可文件分发毕竟存在很大的安全隐患，一旦用于控制许可文件信息的私钥被扩散，后果不堪设想。

飞天诚信也正是基于多年在软件保护及信息安全等领域从业心得，打造了这款产品。飞天诚信公司研

究了当前人们对加密方式的理解及所提出的各种要求,并根据加密方式未来发展的方向,提出了实现授权管理的一揽子解决方案,从硬件到软件提供全方位的支持,开发商可以直接使用其提供的工具进行加密、授权、升级、分发,也可以在此基础上进行二次开发,开发出适合开发商的特定加密授权的方案。

ROCKEY4 SMART 的特点

ROCKEY4 SMART 的开发充分体现了客户的需求和软件加密的发展现状及其发展方向,不仅可以满足客户当前的需要,而且为以后预留了发展方向,可以满足客户不断变化的需要。总的来说,ROCKEY4 SMART 具有下面几个显著的特点:

1、硬件方面

ROCKEY4 SMART 采用的是带 USB 接口的智能卡芯片。对于受保护的软件,通过它,可以保护该软件不被非法复制和非授权访问和使用。它的授权方式主要分为两种:限期授权和限次授权。当使用加密锁加密保护您的软件后,启动所加密保护的程序时,此时若加密锁不在或已经不再符合预定的授权,程序就会发出错误信息,从而终止,这就达到了加密保护软件的目的。同时 ROCKEY4 SMART 加密锁也可以支持许多其它的加密保护限制。

ROCKEY4 SMART 除了可以利用模块字进行限次授权之外,还提供了两个内置功能来对授权管理进行支持,这两个功能分别是:计时功能和 RSA 引擎。

◇ 计时功能

计时功能的实现主要是通过一个软件模拟的时钟来实现的,另外添加了一些辅助的功能。时间锁的基本原理就是,利用加密锁内部 CPU 的时钟频率,计算一个接近外部时间的近似值,当加密锁的计数器被置于倒计时状态时,时间锁便不断地更改计数器的值,并将更改后的结果存放于时间锁的永久存储区当中。这样就可以利用时间锁来实现限期(包括限

定时间、限定截止日期)功能,根据不同的需要,可以转换为限制天数,限制小时数或者限制截止日期等方式。由于加密锁是独立存在的,与系统时间没有直接联系,因此通过加密锁内部的时间锁,可以避免用户以更改系统时间来延长软件使用时间的可能,从而可以更好的加密保护软件。计时功能是实现限期授权的必要条件,它为客户授权提供了更多的选择方式。

◇ RSA 引擎

ROCKEY4 SMART 还内置了 RSA 引擎,用户可以在加密锁的内部实现 RSA 加密解密,从而为软件的加密提供了更多选择方式,另外,它也可用于对软件进行更新授权、授权分发等,开发商将用于更新授权的文件采用 RSA 加密,由于密钥保存在加密锁中,这样只能用加密锁中的 RSA 引擎才能解密,并最终更新授权。另外通过引入母锁的机制,极大地保证私钥的安全性,降低了分发过程中造成泄密的可能。

2、软件方面

ROCKEY4 SMART 的软件当然以授权管理为主,它提供了一个授权管理平台,还有一些相关的辅助工具,例如批量生产工具、外壳加密工具、客户升级工具和编辑器等。这些工具虽然很小,但对客户来说,有了它们,就可以更方便的享受授权管理带来的便利。也许这么说,你会觉得有点难以理解,当你亲身体会过以后,你就会真正领会到 ROCKEY4 SMART 这一整套解决方案的奇妙所在。下面具体来介绍一下 ROCKEY4 SMART 中的各个软件工具。

◇ 授权管理平台

既然是授权管理,自然少不了这个软件。授权管理平台是一个以简单易用为目标的授权管理平台,即使开发商以前没有相关授权管理经验,也可以达到迅速掌握和熟练使用授权管理,这大大减轻了开发商以前授权比较繁琐且不易掌握的困难,使客户授权难以维护的历史成为了过去,将授权管理变的更简单,更方便,更安全。

授权管理平台的界面如图 1 所示, 主要有五大功能: 生产管理、开发商升级管理、客户升级管理、历史升级管理以及母锁管理。

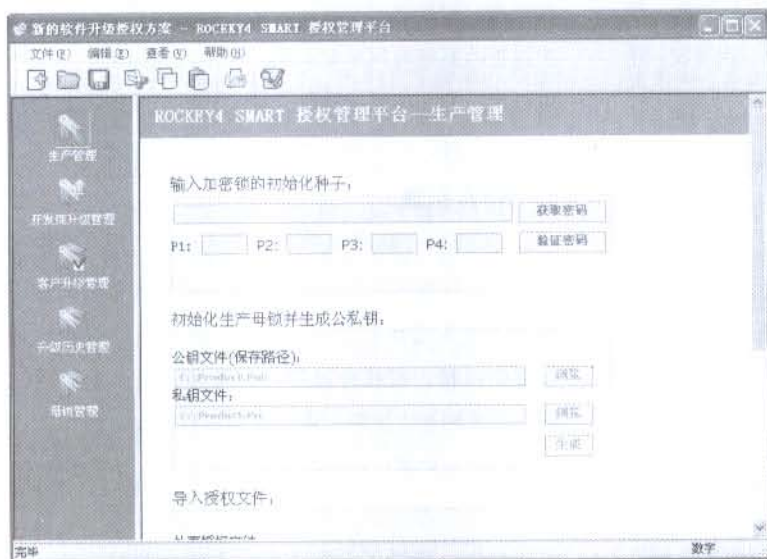


图 1 授权管理平台界面

生产管理的功能是设置锁的密码、初始化锁并生成 RSA 公私钥以及根据由外壳加密工具生成的项目文件生成授权文件等。在获取密码编辑框中输入初始化种子, 即可生成新的加密锁密码, 接下来初始化母锁, 同时生成 RSA 公私钥, 此时还可以将公私钥导出到文件中, 以防止母锁损坏或遗失而导致 RSA 公私钥遗失。RSA 公私钥在客户升级授权时使用。下面可以通过导入外壳加密工具生成的项目文件生成批量生产锁用的授权文件。

开发商升级管理用于开发商编辑授权, 并最终生成授权文件, 此授权文件是用于开发商批量生产加密锁的授权文件。编辑窗口简单明了, 开发商只需选择授权方式, 并设定相应参数, 即可生成相应批量生产锁用的授权文件。

客户升级管理用于对具体客户所作的授权管理, 可以导入历史授权文件, 并在此基础上编辑授权, 形成新的授权文件, 最后将此授权文件分发给客户, 由客户利用客户升级工具对自己的锁进行升

级, 更新授权。需要指出的是, 此授权文件采用 RSA 加密, 只能被保存有相应公私钥的加密锁所解密, 这也正是基于硬件的授权管理体系的优越性所在。

客户升级管理窗口与开发商升级管理窗口比较相似, 所不同的是为了限制升级文件的使用, 开发商可以在此窗口设定升级授权文件的使用限制, 例如: 只能由指定用户使用(由用户 ID 决定)、只能由指定加密锁使用(由硬件 ID 决定)、只能在指定日期前使用、只能在指定模块字相符的情况下才能使用等。另外需要注意的是, 客户升级授权文件只能使用一次。

历史升级管理中可以查看所有客户的升级授权信息记录, 以便根据

这些记录进行升级或更新授权, 它提供了多种查询方式, 以便满足各种查询需求。

母锁管理主要用来重新生成一把母锁, 防止母锁丢失或者被损坏而无法进行生产、升级等操作。

◇ 外壳加密工具

软件保护的好坏并不仅仅依赖加密锁本身, 其中很大程度取决于开发者如何使用加密锁, 即使有优秀的加密锁产品, 但是开发者不能把它的功能完全发挥出来也跟最差的加密锁没有区别。ROCKKEY4 SMART 加密锁提供了两种方式的加密手段, 第一种是外壳加密, 另外一种 API 调用加密。

对于那些对加密技术不是十分了解并且对加密要求不高的开发商, 可以采用外壳加密工具来加密自己的软件。在 ROCKKEY4 SMART 中提供了一个由飞天诚信公司自己研发的外壳加密工具, 这种外壳加密工具结合 ROCKKEY4 SMART 加密锁所提供的计时、RSA 等内置功能, 可以对 PE 格式的文件进行加密、授权, 同时产生的项目文件还可导入到授权管理平台中。

为了使用软件更加简单好用, 外壳加密工具提供

了两种操作方式：向导模式和简单模式。对于初次使用的用户可以使用向导模式，用户根据向导提供的提示一步步进行，即可完成加密授权工作。对于已经熟练掌握使用方法的用户，可使用简单模式，这样更加快捷，简单模式的界面如图2所示。用户选择所要加密的文件，然后在高级设置中选择要授权的方式以及相关的授权参数等，点击执行即可完成加密授权工作。

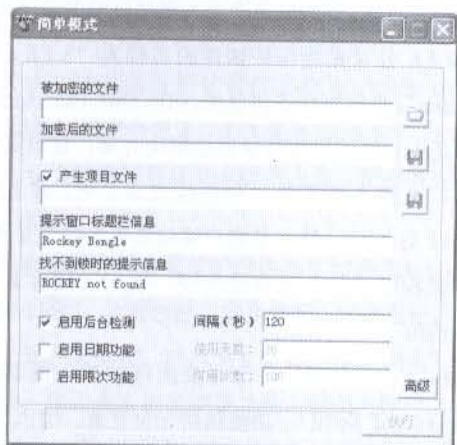


图2 简单模式

这里所介绍的只是 ROCKEY4 SMART 的冰山一角，如果想对 ROCKEY4 SMART 有更详细的了解，请参考开发包中的用户手册。

展望 ROCKEY4 SMART 的未来

作为一家有着十多年从事加密行业经验的飞天诚信公司力推的授权管理产品，它代表着当今加密锁行业发展的最新动向。随着加密技术的不断发展，人们对加密产品的要求和期望也与日俱增，把握信息时代的脉搏，引领加密技术的潮流，一直是飞天诚信公司孜孜不倦的努力方向。ROCKEY4 SMART 不仅将授权管理完美的嵌入到加密的各个环节之中，而且在此基础上开发了一个集成度很高的授权管理平台，本着急客户之所急，想客户之所想的信念，强化加密的效果，减轻客户的负担，相信 ROCKEY4 SMART 的推出会引领一个新的加密锁时代的到来。