(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113326480 B
(45)授权公告日 2024.02.20

(21)申请号 202110609120.1
(22)申请日 2021.06.01
(65)同一申请的已公布的文献号
申请公布号 CN 113326480 A
(43)申请公布日 2021.08.31
(73)专利权人 北京联创新天科技有限公司
地址 100084 北京市海淀区信息路28号1幢10层1001-16号
(72)发明人 郝桃 覃克天 陆伟 张功贵
(74)专利代理机构 北京国科程知识产权代理事务所(普通合伙) 11862
专利代理师 曹晓斐
(51)Int.Cl.
G06F 21/10(2013.01)
G06F 21/12(2013.01)
G06F 21/60(2013.01)
(56)对比文件
CN 104700002 A,2015.06.10
CN 109392310 A,2019.02.26
CN 109639644 A,2019.04.16
CN 110162936 A,2019.08.23
CN 112632476 A,2021.04.09
US 2017346807 A1,2017.11.30
CN 112417379 A,2021.02.26
CN 101853349 A,2010.10.06
CN 102547671 A,2012.07.04
CN 106570353 A,2017.04.19
CN 112528236 A,2021.03.19
CN 112733166 A,2021.04.30
审查员 余佳佳

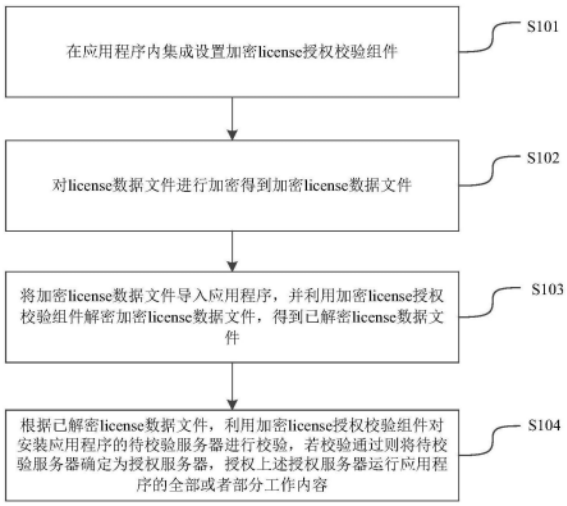
权利要求书2页 说明书8页 附图5页

(54)发明名称

一种应用程序的授权校验方法、装置、介质及设备

(57)摘要

本发明公开了一种应用程序的授权校验方法、装置、介质及设备,包括,在应用程序内集成设置加密license授权校验组件;对license数据文件进行加密得到加密license数据文件;将加密license数据文件导入应用程序,并利用加密license授权校验组件解密加密license数据文件,得到已解密license数据文件;根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验,若校验通过则将待校验服务器确定为授权服务器,授权上述授权服务器运行应用程序的全部或者部分工作内容。本发明的应用解决了现有license授权校验组件侵入性高及整合性差的问题,降低了license授权校验的成本,灵活性高,防止应用程序未授权启动,保护应用程序的知识产权。



CN 113326480 B

1.一种应用程序的授权校验方法,其特征在于,包括,

在所述应用程序内集成设置加密license授权校验组件;

对license数据文件进行加密得到加密license数据文件;

将所述加密license数据文件导入所述应用程序,并利用所述加密license授权校验组件解密所述加密license数据文件,得到已解密license数据文件;

根据所述已解密license数据文件,利用所述加密license授权校验组件对安装所述应用程序的待校验服务器进行校验,若校验通过则将所述待校验服务器确定为授权服务器,授权所述授权服务器运行所述应用程序的全部或者部分工作内容。

2.如权利要求1所述的应用程序的授权校验方法,其特征在于,所述对license数据文件进行加密得到加密license数据文件的过程包括,

利用RSA非对称加密算法的RSA私钥对所述license数据文件进行加密得到所述加密license数据文件;

所述利用所述加密license授权校验组件解密所述加密license数据文件,得到已解密license数据文件的过程包括,

利用所述RSA非对称加密算法的RSA公钥对所述加密license数据文件进行解密得到所述已解密license数据文件。

3.如权利要求1所述的应用程序的授权校验方法,其特征在于,

所述已解密license数据文件中包括所述应用程序的授权期限;

所述根据所述已解密license数据文件,利用所述加密license授权校验组件对安装所述应用程序的待校验服务器进行校验的过程包括,

利用所述加密license授权校验组件对当前时间是否超出所述授权期限进行校验。

4.如权利要求1所述的应用程序的授权校验方法,其特征在于,

所述已解密license数据文件中包括授权安装所述应用程序的服务器的授权设备信息;

所述根据所述已解密license数据文件,利用所述加密license授权校验组件对安装所述应用程序的待校验服务器进行校验的过程包括,

利用所述加密license授权校验组件获取所述待校验服务器的设备信息;

利用所述加密license授权校验组件对所述待校验服务器的所述设备信息以及所述授权设备信息进行对比校验。

5.如权利要求3所述的应用程序的授权校验方法,其特征在于,所述已解密license数据文件中还包括授权安装所述应用程序的所述服务器的授权设备信息;

所述根据所述已解密license数据文件,利用所述加密license授权校验组件对安装所述应用程序的待校验服务器进行校验的过程包括,

利用所述加密license授权校验组件对当前时间是否超出所述授权期限进行校验,若未超出,则利用所述加密license授权校验组件获取所述待校验服务器的设备信息,并且利用所述加密license授权校验组件对所述待校验服务器的所述设备信息以及所述授权设备信息进行对比校验。

6.如权利要求4或5所述的应用程序的授权校验方法,其特征在于,所述利用所述加密license授权校验组件获取所述待校验服务器的设备信息的过程包括,

所述加密license授权校验组件利用dmidecode命令组或WMIC命令组,获取所述待校验服务器的所述设备信息。

7.一种应用程序的授权校验装置,其特征在于,包括,

集成模块,用于在所述应用程序内集成设置加密license授权校验组件;

加密模块,用于对license数据文件进行加密得到加密license数据文件;

解密模块,用于将所述加密license数据文件导入所述应用程序,并利用所述加密license授权校验组件解密所述加密license数据文件,得到已解密license数据文件;

校验授权模块,用于根据所述已解密license数据文件,利用所述加密license授权校验组件对安装所述应用程序的待校验服务器进行校验,若校验通过则将所述待校验服务器确定为授权服务器,授权所述授权服务器运行所述应用程序的全部或者部分工作内容。

8.如权利要求6所述的应用程序的授权校验装置,其特征在于,还包括,

校验授权模块包括,授权期限校验子模块以及设备信息校验子模块;

所述设备信息校验子模块包括设备信息获取单元。

9.一种计算机可读存储介质,其存储有计算机指令,其特征在于,所述计算机指令被操作以执行权利要求1~6中任一项所述的应用程序的授权校验方法。

10.一种计算机设备,其包括处理器和存储器,所述存储器存储有计算机指令,其中,所述处理器操作所述计算机指令以执行权利要求1~6任一项所述的应用程序的授权校验方法。

一种应用程序的授权校验方法、装置、介质及设备

技术领域

[0001] 本申请涉及软件开发技术领域,特别是一种应用程序的授权校验方法、装置、存储介质及设备。

背景技术

[0002] 虽然市面上已经有可用的license授权校验组件及其服务,也都能实现授权校验功能,但都需要对接各自的license接口,配置license管理服务,其侵入性较高,授权的应用程序还需要连接license服务,整合实用性也较差。并且市面上的license授权校验组件,一般都是走产品化路线,当功能上不能贴合实际情况需要时,对应产品都不会立刻做出调整、更新,所以对于license授权校验组件的灵活性、可用性没有保障。同时由于市面上的license授权校验组件,不是免费的,或者说高级功能以及高级特性不免费,使用这些组件,会产生额外成本。

发明内容

[0003] 本发明提供一种应用程序的授权校验方法、装置、介质及设备,解决了现有license授权校验组件侵入性高及整合性差的问题,降低了license授权校验的成本,灵活性高,防止应用程序未授权启动,保护应用程序的知识产权。

[0004] 为了解决上述问题,本发明采用的一个技术方案是:提供一种应用程序的授权校验方法,该方法包括:

[0005] 在应用程序内集成设置加密license授权校验组件;

[0006] 对license数据文件进行加密得到加密license数据文件;

[0007] 将加密license数据文件导入应用程序,并利用加密license授权校验组件解密加密license数据文件,得到已解密license数据文件;

[0008] 根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验,若校验通过则将待校验服务器确定为授权服务器,授权上述授权服务器运行应用程序的全部或者部分工作内容。

[0009] 本发明采用的另一个技术方案是:提供一种应用程序的授权校验装置,该装置包括:

[0010] 集成模块,用于在应用程序内集成设置加密license授权校验组件;

[0011] 加密模块,用于对license数据文件进行加密得到加密license数据文件;

[0012] 解密模块,用于将加密license数据文件导入应用程序,并利用加密license授权校验组件解密加密license数据文件,得到已解密license数据文件;

[0013] 校验授权模块,用于根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验,若校验通过则将待校验服务器确定为授权服务器,授权上述授权服务器运行应用程序的全部或者部分工作内容。

[0014] 在本申请的另一个技术方案中,提供一种计算机可读存储介质,其存储有计算机

指令,其中计算机指令被操作以执行方案中的应用程序的授权校验方法。

[0015] 在本申请的另一技术方案中,提供一种计算机设备,其包括处理器和存储器,存储器存储有计算机指令,其中,处理器操作计算机指令以执行方案中的应用程序的授权校验方法。

[0016] 本发明技术方案可以达到的有益效果是:本发明提出一种应用程序的授权校验方法、装置、存储介质及设备,解决了现有license授权校验组件侵入性高及整合性差的问题,降低了license授权校验的成本,灵活性高,防止应用程序未授权启动,保护应用程序的知识产权。

附图说明

[0017] 为了更清楚地说明本申请实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍,显而易见地,下面描述中的附图是本申请的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动性的前提下,还可以根据这些附图获得其他的附图。

[0018] 图1为本发明一种应用程序的授权校验方法一个具体实施例的示意图;

[0019] 图2为本发明一种应用程序的授权校验方法的一个具体实例的示意图;

[0020] 图3为本发明一种应用程序的授权校验方法的一个具体实例的示意图;

[0021] 图4为本发明一种应用程序的授权校验方法的一个具体实例的示意图;

[0022] 图5为本发明一种应用程序的授权校验装置另一个具体实施例的示意图;

[0023] 图6为本发明一种应用程序的授权校验装置一个具体实例的示意图。

[0024] 通过上述附图,已示出本申请明确的实施例,后文中将有更详细的描述。这些附图和文字描述并不是为了通过任何方式限制本申请构思的范围,而是通过参考特定实施例为本领域技术人员说明本申请的概念。

具体实施方式

[0025] 下面结合附图对本发明的较佳实施例进行详细阐述,以使本发明的优点和特征能更易于被本领域技术人员理解,从而对本发明的保护范围做出更为清楚明确的界定。

[0026] 需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0027] 图1所示为本发明一种应用程序的授权校验方法一个具体实施例的示意图。

[0028] 在该具体实施方式中,应用程序的授权校验方法主要包括:

[0029] 过程S101:在应用程序内集成设置加密license授权校验组件;

[0030] 过程S102:对license数据文件进行加密得到加密license数据文件;

[0031] 过程S103:将加密license数据文件导入应用程序,并利用加密license授权校验

组件解密加密license数据文件,得到已解密license数据文件;

[0032] 过程S104:根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验,若校验通过则将待校验服务器确定为授权服务器,授权上述授权服务器运行应用程序的全部或者部分工作内容。

[0033] 通过本发明提供的一种应用程序的授权校验方法,解决了现有license授权校验组件侵入性高及整合性差的问题,降低了license授权校验的成本,灵活性高,防止应用程序未授权启动,保护应用程序的知识产权。

[0034] 在图1所示的具体实施方式中,本发明的应用程序的授权校验方法包括过程S101,在应用程序内集成设置加密license授权校验组件。此过程以便于降低license授权校验的成本。

[0035] 具体地,由于市面上的license授权校验组件,一般都是走产品化路线,当功能上不能贴合实际情况需要时,对应产品都不会立刻做出调整、更新,所以对于license授权校验组件的灵活性、可用性没有保障。同时由于市面上的license授权校验组件,不是免费的,或者说高级功能以及高级特性不免费,使用这些组件,会产生额外成本,因此为了保护应用程序的知识产权,保证对外授权部署应用的时效性、可控性,同时避免对外部署的应用被拷贝盗用,避免未授权的移植部署,自主开发实现与基础开发框架整合的加密license授权组件,在对外部署的应用程序内集成设置加密license授权校验组件。

[0036] 在图1所示的具体实施方式中,本发明的应用程序的授权校验方法包括过程S102,对license数据文件进行加密得到加密license数据文件。此过程以便于避免授权校验过程中的入侵,提高安全性,保护应用程序的知识产权。

[0037] 在本发明的一个具体实施例中,上述对license数据文件进行加密得到加密license数据文件的过程包括,利用RSA非对称加密算法的RSA私钥对license数据文件进行加密得到加密license数据文件。此过程以便于避免授权校验过程中的入侵,提高安全性,保护应用程序的知识产权。

[0038] 其中license数据文件中可以包括授权期限、安装应用程序的服务器的授权设备信息等,授权期限由开发应用程序的公司进行设定,安装应用程序的服务器的授权设备信息由客户提供。未来license数据文件中也可以包括安装应用程序的服务器的温度范围(前提是安装应用程序的服务器中有测温模块),可以通过温度条件对服务器进行校验,若超出温度范围,安全起见停止对服务器授权应用软件,在下一次校验时若温度在license数据文件中设置的温度范围,则对服务器授权应用软件。因此本发明中license数据文件中的内容不作限制。

[0039] 在本发明中,无论对license数据文件加密得到加密license数据文件,或者对加密license数据文件进行解密得到已解密license数据文件,其中的内容始终不变,与原始的license数据文件一致。

[0040] 其中,RSA非对称加密算法目前最有影响力的加密算法,它能够抵抗到目前为止已知的所有密码攻击,已被ISO推荐为数据加密标准。RSA非对称加密算法基于一个十分简单的数论事实:将两个大素数相乘十分容易,但想要对其乘积进行因式分解却极其困难。因此本发明利用RSA非对称加密算法的RSA私钥对license数据文件进行加密得到加密license数据文件。

[0041] 在图1所示的具体实施方式中,本发明的应用程序的授权校验方法包括过程S103,将加密license数据文件导入应用程序,并利用加密license授权校验组件解密加密license数据文件,得到已解密license数据文件。此过程对加密license数据文件进行解密,以便于进一步根据已解密license数据文件进行授权校验。

[0042] 在本发明的一个具体实施例中,上述利用加密license授权校验组件解密加密license数据文件,得到已解密license数据文件的过程包括,利用RSA非对称加密算法的RSA公钥对加密license数据文件进行解密得到已解密license数据文件。此过程对加密license数据文件进行解密,以便于进一步根据已解密license数据文件进行授权校验。

[0043] 其中,RSA非对称加密算法目前最有影响力的加密算法,它能够抵抗到目前为止已知的所有密码攻击,已被ISO推荐为数据加密标准。RSA非对称加密算法基于一个十分简单的数论事实:将两个大素数相乘十分容易,但想要对其乘积进行因式分解却极其困难。因此本发明利用RSA非对称加密算法的RSA公钥对加密license数据文件进行解密得到已解密license数据文件。

[0044] 在图1所示的具体实施方式中,本发明的应用程序的授权校验方法包括过程S104,根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验,若校验通过则将待校验服务器确定为授权服务器,授权上述授权服务器运行应用程序的全部或者部分工作内容。此过程对待校验服务器进行校验,灵活性高,防止应用程序未授权启动,以便于保护应用程序的知识产权。

[0045] 在本发明的一个具体实施例中,当已解密license数据文件中包括应用程序的授权期限时,根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验的过程包括,利用加密license授权校验组件对当前时间是否超出授权期限进行校验。此过程对授权期限进行校验,防止应用程序未授权启动,以便于保护应用程序的知识产权。

[0046] 具体地,参照图2本发明提供的一种应用程序的授权校验方法的一个具体实例的示意图,该具体实例中license数据文件中仅包括应用程序的授权期限,即已解密license数据文件中也仅包括应用程序的授权期限,上述实例中已经对license数据文件进行加密得到了加密license数据文件,实际应用中由开发软件一方的工作人员将加密license数据文件发送给客户,客户或工作人员将加密license数据文件导入应用程序的根目录中,加密license授权校验组件可以在应用程序启动或者定时校验任务开启时进行授权校验,首先加密license授权校验组件先读取应用程序中的加密license数据文件,若不包含加密license数据文件,则校验失败,程序退出,无法使用。若包含加密license数据文件,则对其进行解密得到已解密license数据文件,由于已解密license数据文件仅包括应用程序的授权期限,因此只需要对授权期限进行校验,若安装有应用程序的服务器的当前时间在授权期限内,则校验成功,对服务器授权该应用程序,若安装有应用程序的服务器的当前时间不在授权期限内,则校验失败,程序退出,无法使用。

[0047] 在本发明的一个具体实施例中,当已解密license数据文件中包括授权安装应用程序的服务器的授权设备信息时,根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验的过程包括,利用加密license授权校验组件获取待校验服务器的设备信息;利用加密license授权校验组件对待校验服务器的设

备信息以及授权设备信息进行对比校验。此过程对授权设备信息进行校验,防止应用程序未授权启动,以便于保护应用程序的知识产权。

[0048] 具体地,参照图3本发明提供的一种应用程序的授权校验方法的一个具体实例的示意图,该具体实例中license数据文件中仅包括授权安装应用程序的服务器的授权设备信息,即已解密license数据文件中也仅包括授权安装应用程序的服务器的授权设备信息,上述实例中已经对license数据文件进行加密得到了加密license数据文件,实际应用中由开发软件一方的工作人员将加密license数据文件发送给客户,客户或工作人员将加密license数据文件导入应用程序的根目录中,加密license授权校验组件可以在应用程序启动或者定时校验任务开启时进行授权校验,首先加密license授权校验组件先读取应用程序中的加密license数据文件,若不包含加密license数据文件,则校验失败,程序退出,无法使用。若包含加密license数据文件,则对其进行解密得到已解密license数据文件,由于已解密license数据文件仅包括授权安装应用程序的服务器的授权设备信息,因此只需要对授权设备信息进行校验,若待校验服务器的设备信息与授权设备信息一致,则校验成功,对服务器授权该应用程序,若待校验服务器的设备信息与授权设备信息不一致,则校验失败,程序退出,无法使用。

[0049] 在本发明的一个具体实施例中,上述利用加密license授权校验组件获取待校验服务器的设备信息的过程包括,加密license授权校验组件利用dmidecode命令组或WMIC命令组,获取待校验服务器的设备信息,此过程以便于进一步根据待校验服务器的设备信息完成校验工作。

[0050] 具体地,liunx环境下加密license授权校验组件利用dmidecode命令组获取待校验服务器的设备信息,dmidecode命令组可以在Linux系统下获取有关硬件方面的信息。其中dmidecode遵循SMBIOS/DMI标准,以一种可读的方式转储机器的DMI(Desktop Management Interface)信息,其输出的信息包括BIOS、系统、主板、处理器、内存、缓存等。Windows环境下加密license授权校验组件利用WMIC命令组获取待校验服务器的设备信息,WMIC是扩展WMI(Windows Management Instrumentation,Windows管理规范),提供了从命令行接口和批命令脚本执行系统管理的支持,为WMIC提供了一个强大的、友好的命令行接口,便于获取待校验服务器的设备信息。

[0051] 在本发明的一个具体实施例中,当已解密license数据文件中包括授权安装应用程序的服务器的授权设备信息以及应用程序的授权期限时,根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验的过程包括,利用加密license授权校验组件对当前时间是否超出授权期限进行校验,若未超出,则利用加密license授权校验组件获取待校验服务器的设备信息,并且利用加密license授权校验组件对待校验服务器的设备信息以及授权设备信息进行对比校验。此过程对授权期限以及授权设备信息进行校验,防止应用程序未授权启动,以便于保护应用程序的知识产权。

[0052] 其中,利用加密license授权校验组件获取待校验服务器的设备信息与上述实例中的步骤相同,此处不进行赘述。

[0053] 具体地,参照图4本发明提供的一种应用程序的授权校验方法的一个具体实例的示意图,该具体实例中license数据文件中包括应用程序的授权期限以及授权安装应用程序的服务器的授权设备信息,即已解密license数据文件中也包括应用程序的授权期限以

及授权安装应用程序的服务器的授权设备信息,上述实例中已经对license数据文件进行加密得到了加密license数据文件,实际应用中由开发软件一方的工作人员将加密license数据文件发送给客户,客户或工作人员将加密license数据文件导入应用程序的根目录中,加密license授权校验组件可以在应用程序启动或者定时校验任务开启时进行授权校验,首先加密license授权校验组件先读取应用程序中的加密license数据文件,若不包含加密license数据文件,则校验失败,程序退出,无法使用。若包含加密license数据文件,则对其进行解密得到已解密license数据文件。由于已解密license数据文件包括应用程序的授权期限以及授权安装应用程序的服务器的授权设备信息,加密license授权校验组件先对授权期限进行校验,若安装有应用程序的服务器的当前时间不在授权期限内,则校验失败,程序退出,无法使用,若安装有应用程序的服务器的当前时间在授权期限内,则校验成功,加密license授权校验组件继续对授权设备信息进行校验,若待校验服务器的设备信息与授权设备信息一致,则校验成功,对服务器授权该应用程序,若待校验服务器的设备信息与授权设备信息不一致,则校验失败,程序退出,无法使用。

[0054] 在本发明的过程S104中,若校验通过则将待校验服务器确定为授权服务器,授权上述授权服务器运行应用程序的全部或者部分工作内容。其中,授权服务器运行应用程序的全部或者部分工作内容表示的是应用程序在工作时可以分为多个工作模块,本发明的应用程序的授权校验方法可以授权校验单个工作模块或多个工作模块。例如本发明的应用程序包括支付管理模块、销量统计模块、物流管理模块等,但应用程序的开发方的公司仅对支付管理模块设置权限,销量统计模块以及物流管理模块等可以无限制使用,因此在进行校验时,若校验不通过,则只关闭支付管理模块的使用权,其余工作模块均可正常使用,若校验通过,则开放应用程序的所有工作模块的使用权。

[0055] 图5所示本发明一种应用程序的授权校验装置一个具体实施方式的示意图。

[0056] 在图5示出的具体是实施方式中,本发明的应用程序的授权校验装置包括模块501、模块502、模块503以及模块504。

[0057] 图5示出的模块501,表示的是集成模块,用于在应用程序内集成设置加密license授权校验组件。此模块以便于降低license授权校验的成本。

[0058] 具体地,为了保护应用程序的知识产权,保证对外授权部署应用的时效性、可控性,同时避免对外部署的应用被拷贝盗用,避免未授权的移植部署,自主开发实现与基础开发框架整合的加密license授权组件,在对外部署的应用程序内集成设置加密license授权校验组件。

[0059] 图5示出的模块502,表示的是加密模块,用于对license数据文件进行加密得到加密license数据文件。此模块以便于避免授权校验过程中的入侵,提高安全性,保护应用程序的知识产权。

[0060] 在本发明的一个具体实施例中,上述加密模块的工作内容还包括,利用RSA非对称加密算法的RSA私钥对license数据文件进行加密得到加密license数据文件。此过程以便于避免授权校验过程中的入侵,提高安全性,保护应用程序的知识产权。

[0061] 图5示出的模块503,表示的是解密模块,用于将加密license数据文件导入应用程序,并利用加密license授权校验组件解密加密license数据文件,得到已解密license数据文件。此模块对加密license数据文件进行解密,以便于进一步根据已解密license数据文

件进行授权校验。

[0062] 在本发明的一个具体实施例中,上述解密模块的工作内容还包括,利用RSA非对称加密算法的RSA公钥对加密license数据文件进行解密得到已解密license数据文件。此过程对加密license数据文件进行解密,以便于进一步根据已解密license数据文件进行授权校验。

[0063] 图5示出的模块504,表示的是校验授权模块,用于根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验,若校验通过则将待校验服务器确定为授权服务器,授权上述授权服务器运行应用程序的全部或者部分工作内容。此模块对待校验服务器进行校验,灵活性高,防止应用程序未授权启动,以便于保护应用程序的知识产权。

[0064] 在本发明的一个具体实施例中,参照本发明图6提供的一种应用程序的授权校验装置一个具体实例的示意图,上述校验授权模块还包括授权期限校验子模块601,其工作内容为当已解密license数据文件中包括应用程序的授权期限时,根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验的过程包括,利用加密license授权校验组件对当前时间是否超出授权期限进行校验。此过程对授权期限进行校验,防止应用程序未授权启动,以便于保护应用程序的知识产权。

[0065] 在本发明的一个具体实施例中,参照本发明图6提供的一种应用程序的授权校验装置一个具体实例的示意图,上述校验授权模块还包括设备信息校验子模块602,其工作内容为当已解密license数据文件中包括授权安装应用程序的服务器的授权设备信息时,根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验的过程包括,利用加密license授权校验组件获取待校验服务器的设备信息;利用加密license授权校验组件对待校验服务器的设备信息以及授权设备信息进行对比校验。此过程对授权设备信息进行校验,防止应用程序未授权启动,以便于保护应用程序的知识产权。

[0066] 在本发明的一个具体实施例中,参照本发明图6提供的一种应用程序的授权校验装置一个具体实例的示意图,上述设备信息校验子模块602还包括设备信息获取单元602-1,其工作内容为加密license授权校验组件利用dmidecode命令组或WMIC命令组,获取待校验服务器的设备信息,此过程以便于进一步根据待校验服务器的设备信息完成校验工作。

[0067] 在本发明的一个具体实施例中,上述校验授权模块的工作内容还包括,当已解密license数据文件中包括授权安装应用程序的服务器的授权设备信息以及应用程序的授权期限时,根据已解密license数据文件,利用加密license授权校验组件对安装应用程序的待校验服务器进行校验的过程包括,利用加密license授权校验组件对当前时间是否超出授权期限进行校验,若未超出,则利用加密license授权校验组件获取待校验服务器的设备信息,并且利用加密license授权校验组件对待校验服务器的设备信息以及授权设备信息进行对比校验。此过程综合上述应用了上述授权期限校验子模块601、设备信息校验子模块602以及设备信息获取单元602-1,对授权期限以及授权设备信息进行校验,防止应用程序未授权启动,以便于保护应用程序的知识产权。

[0068] 通过本发明应用程序的授权校验装置的应用,解决了现有license授权校验组件侵入性高及整合性差的问题,降低了license授权校验的成本,灵活性高,防止应用程序未

授权启动,保护应用程序的知识产权。

[0069] 本发明提供的一种应用程序的授权校验装置,可用于执行上述任一实施例描述的应用程序的授权校验方法,其实现原理和技术效果类似,在此不再赘述。

[0070] 在本发明的另一个具体实施方式中,一种计算机可读存储介质,其存储有计算机指令,其特征在于,计算机指令被操作以执行任一实施例描述的应用程序的授权校验方法。其中,该存储介质可直接在硬件中、在由处理器执行的软件模块中或在两者的组合中。

[0071] 软件模块可驻留在RAM存储器、快闪存储器、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可装卸盘、CD-ROM或此项技术中已知的任何其它形式的存储介质中。示范性存储介质耦合到处理器,使得处理器可从存储介质读取信息和向存储介质写入信息。

[0072] 处理器可以是中央处理单元(英文:Central Processing Unit,简称:CPU),还可以是其他通用处理器、数字信号处理器(英文:Digital Signal Processor,简称:DSP)、专用集成电路(英文:Application Specific Integrated Circuit,简称:ASIC)、现场可编程门阵列(英文:Field Programmable Gate Array,简称:FPGA)或其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件或其任何组合等。通用处理器可以是微处理器,但在替代方案中,处理器可以是任何常规处理器、控制器、微控制器或状态机。处理器还可实施为计算装置的组合,例如DSP与微处理器的组合、多个微处理器、结合DSP核心的一个或一个以上微处理器或任何其它此类配置。在替代方案中,存储介质可与处理器成一体式。处理器和存储介质可驻留在ASIC中。ASIC可驻留在用户终端中。在替代方案中,处理器和存储介质可作为离散组件驻留在用户终端中。

[0073] 在本发明的一个具体实施方式中,一种计算机设备,其包括处理器和存储器,存储器存储有计算机指令,其中:处理器操作计算机指令以执行任一实施例描述的应用程序的授权校验方法。

[0074] 在本申请所提供的实施方式中,应该理解到,所揭露的系统和方法,可以通过其它的方式实现。例如,以上所描述的系统实施例仅仅是示意性的,例如,单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0075] 作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0076] 以上仅为本申请的实施例,并非因此限制本申请的专利范围,凡是利用本申请说明书及附图内容所作的等效结构变换,或直接或间接运用在其他相关的技术领域,均同理包括在本申请的专利保护范围内。

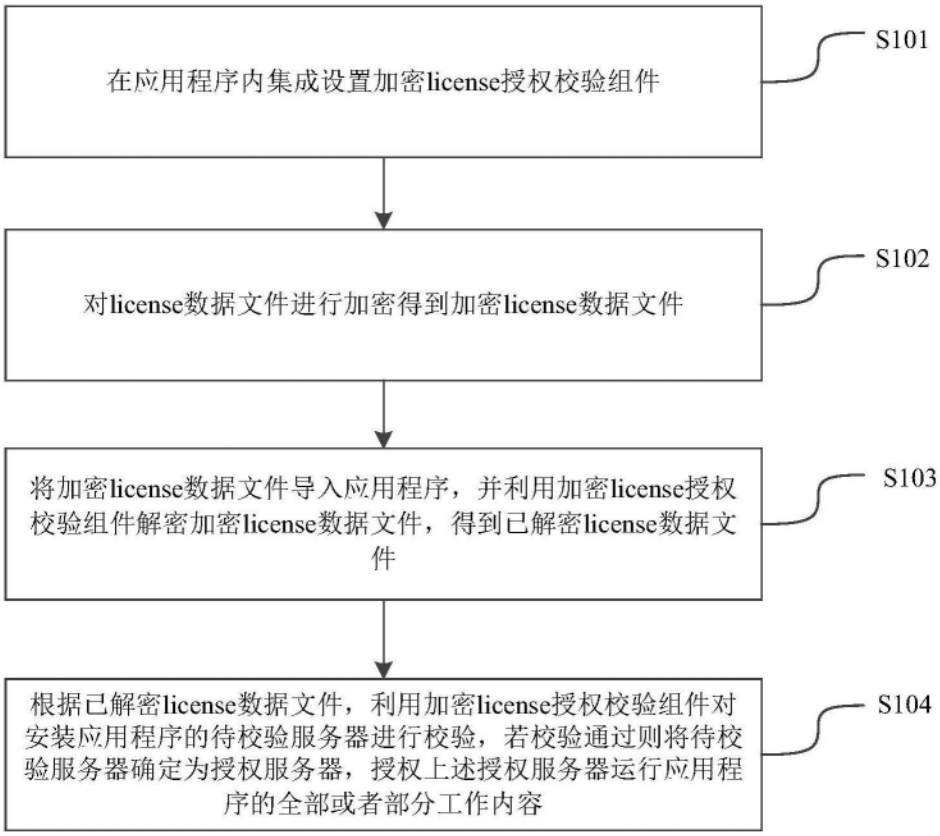

在应用程序内集成设置加密license授权校验组件
S101
对license数据文件进行加密得到加密license数据文件
S102
将加密license数据文件导入应用程序，并利用加密license授权校验组件解密加密license数据文件，得到已解密license数据文件
S103
根据已解密license数据文件，利用加密license授权校验组件对安装应用程序的待校验服务器进行校验，若校验通过则将待校验服务器确定为授权服务器，授权上述授权服务器运行应用程序的全部或者部分工作内容
S104

图1

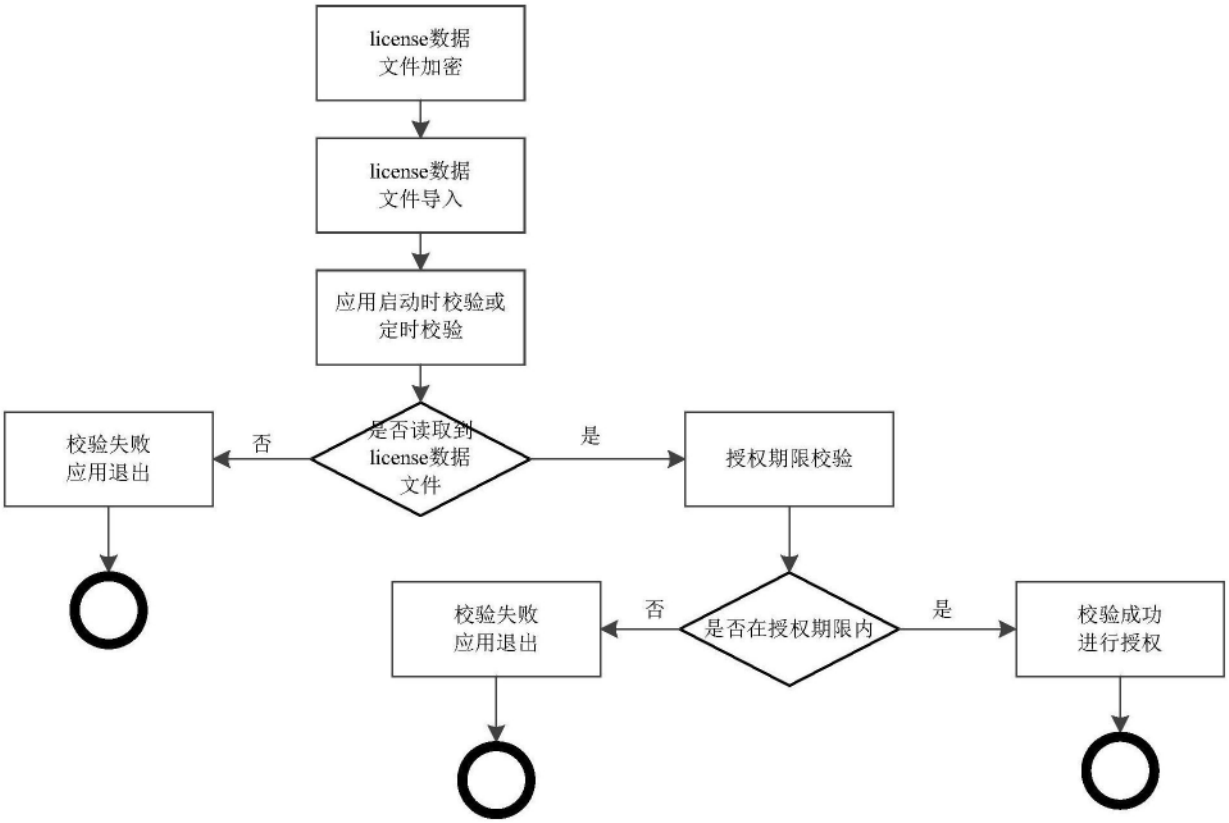

license数据
文件加密
license数据
文件导入
应用启动时校验或
定时校验
是否读取到
license数据
文件
否
校验失败
应用退出
是
授权期限校验
是否在授权期限内
否
校验失败
应用退出
是
校验成功
进行授权

图2

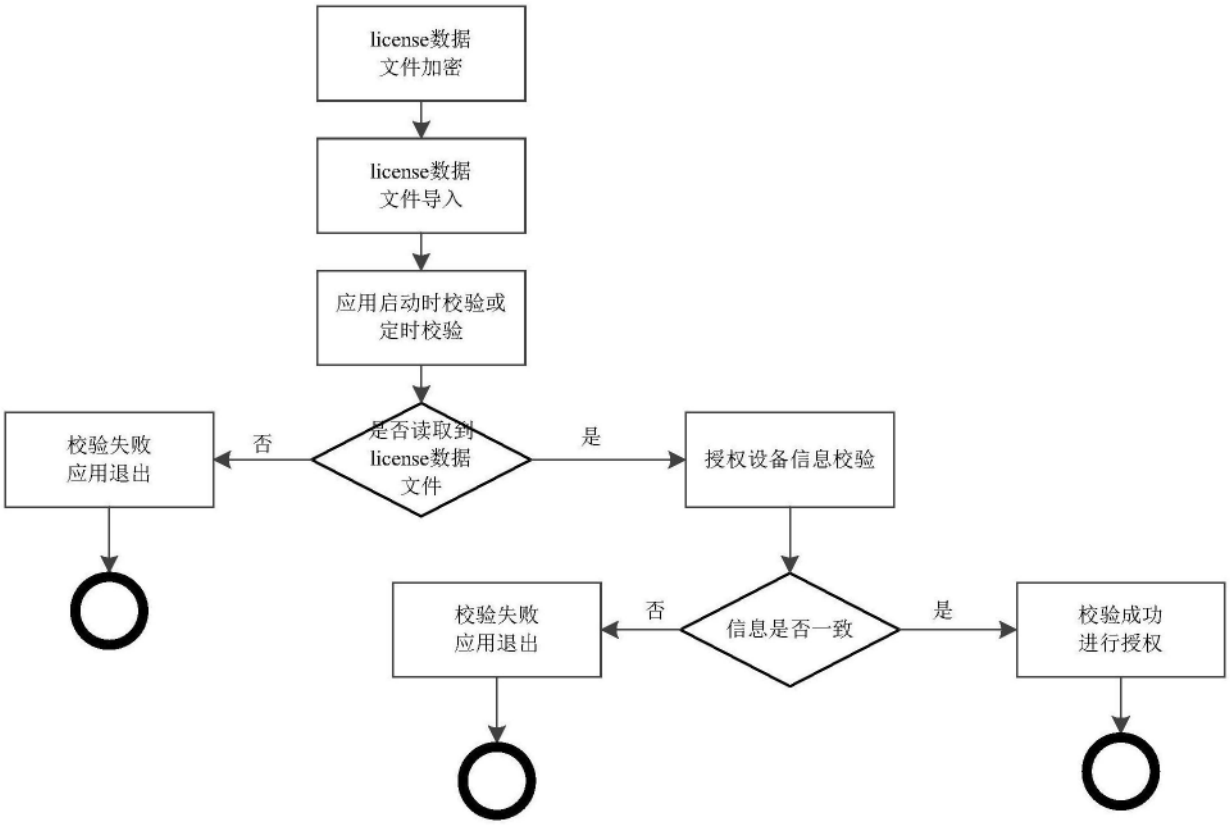

license数据
文件加密
license数据
文件导入
应用启动时校验或
定时校验
是否读取到
license数据
文件
否
校验失败
应用退出
是
授权设备信息校验
信息是否一致
否
校验失败
应用退出
是
校验成功
进行授权

图3

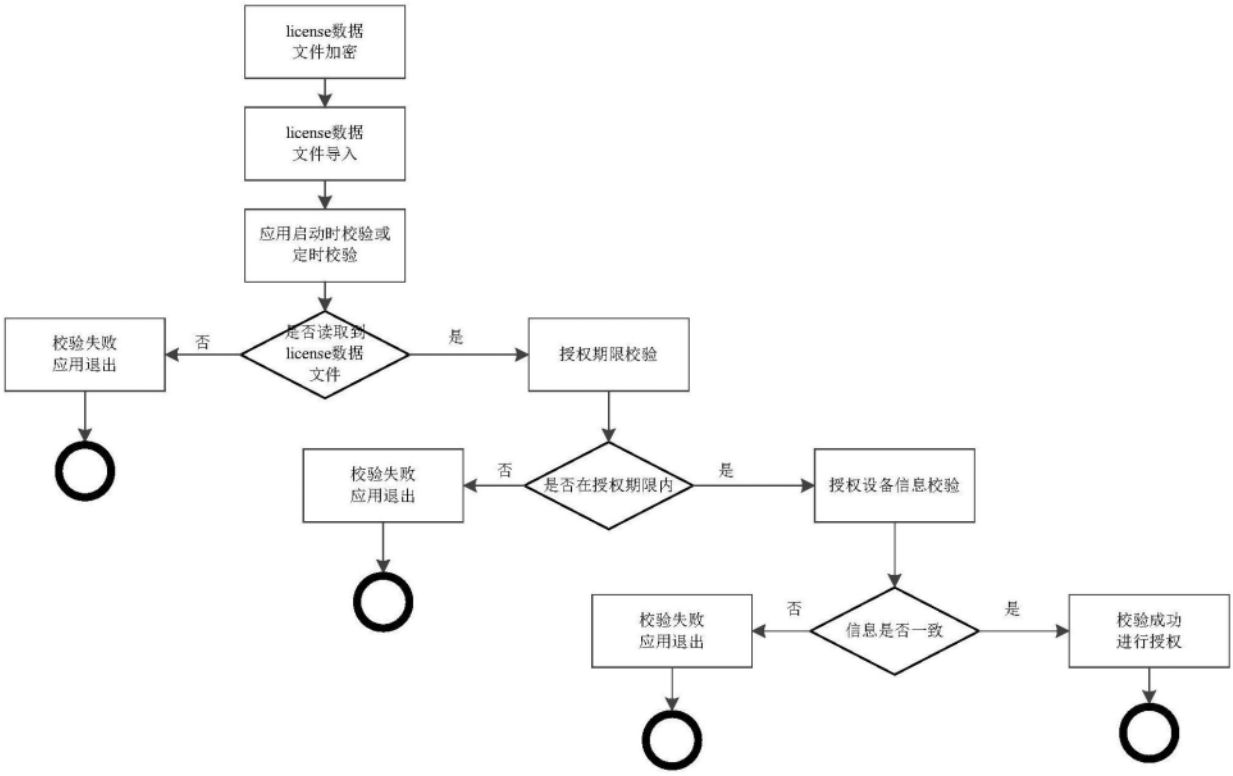

license数据
文件加密
license数据
文件导入
应用启动时校验或
定时校验
是否读取到
license数据
文件
否
校验失败
应用退出
是
授权期限校验
是否在授权期限内
否
校验失败
应用退出
是
授权设备信息校验
信息是否一致
否
校验失败
应用退出
是
校验成功
进行授权

图4

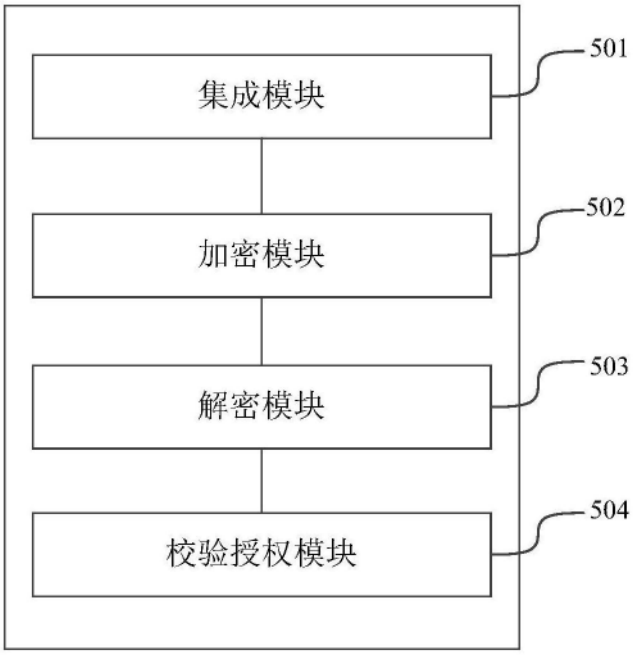

集成模块
501
加密模块
502
解密模块
503
校验授权模块
504

图5

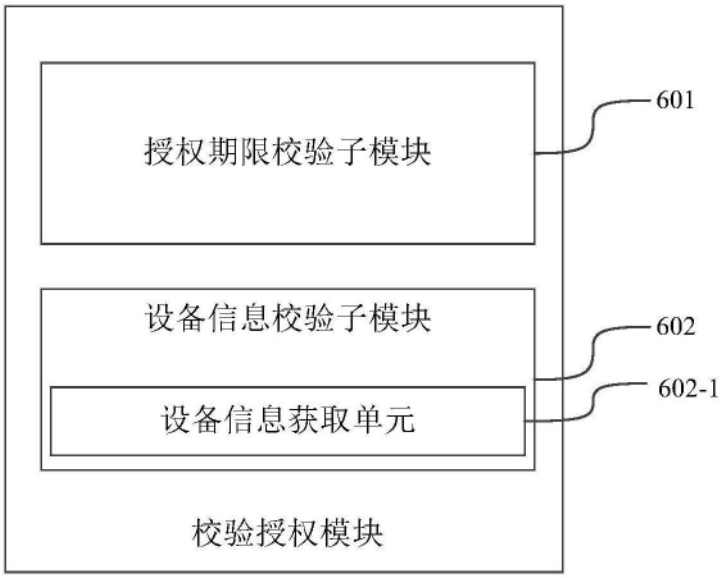


图6