(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104067286 B
(45)授权公告日 2017.03.29

(21)申请号 201380005350.0

(22)申请日 2013.01.10

(65)同一申请的已公布的文献号
申请公布号 CN 104067286 A

(43)申请公布日 2014.09.24

(30)优先权数据
13/350,360 2012.01.13 US

(85)PCT国际申请进入国家阶段日
2014.07.11

(86)PCT国际申请的申请数据
PCT/US2013/020913 2013.01.10

(87)PCT国际申请的公布数据
WO2013/106492 EN 2013.07.18

(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州

(72)发明人 V·伦伽纳坦 B·T·卡弗
D·B·江普 D·C·勒布朗
S·I·韦斯

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 王英

(51)Int.Cl.
*G06F 21/60*(2006.01)
*G06F 21/30*(2006.01)

(56)对比文件
CN 1729526 A,2006.02.01,
EP 1641176 A1,2006.03.29,
US 2011/0252243 A1,2011.10.13,

审查员 王春圆

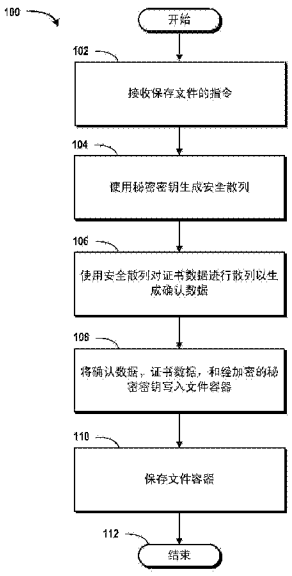
权利要求书3页 说明书8页 附图4页

(54)发明名称

# 无效托管密钥的检测

(57)摘要

使用一秘密信息(例如,秘密密钥)以及每个托管密钥专用的一公共信息(例如,证书散列或公钥)来生成安全散列,诸如基于散列的消息认证码("HMAC")。使用秘密密钥确保了托管密钥确认数据只有通过知晓秘密密钥才可生成,这阻止了攻击者生成适当的托管密钥确认数据。使用证书散列作为公共数据会将每个托管密钥确认数据绑定到特定证书,从而阻止攻击者从另一个托管密钥简单复制该确认数据。任何被发现是无效的托管密钥可从文件容器移除,并审计日志可被生成使得公司、个人、或其它实体能够知晓可能的安全性违背的企图。




CN 104067286 B

1.一种用于生成托管密钥确认数据的计算机实现的方法，所述计算机实现的方法包括执行计算机实现的操作，所述操作用于：

使用计算机，接收保存文件的指令；

使用所述计算机，使用秘密密钥生成安全散列，所述秘密密钥被用于加密所述文件；

使用所述计算机，使用所述安全散列对公钥进行散列，以生成用于托管密钥的确认数据，其中所述确认数据被生成以用作确认操作的一部分，以在对所述文件执行后面的操作期间确认所述托管密钥，所述公钥是所述托管密钥专用的一公共信息；以及

使用所述计算机，保存所述确认数据、所述公钥，和所述秘密密钥。

2.如权利要求1所述的计算机实现的方法，其特征在于，所述安全散列是基于散列的消息认证码(“HMAC”)。

3.如权利要求1所述的计算机实现的方法，其特征在于，进一步包括：

接收打开所述文件的指令；

响应于接收到打开所述文件的指令，请求用于秘密密钥的解密的用户输入；

接收用户输入；

判定所述用户输入是否有效；

响应于判定所述用户输入有效；

解密所述秘密密钥；

使用所述秘密密钥来生成进一步的安全散列；

使用所述进一步的安全散列来对所述公钥进行散列，以生成所述托管密钥的进一步的确认数据，

将所述确认数据与所述进一步的确认数据进行比较，

如果所述确认数据与所述进一步的确认数据匹配，判定所述托管密钥是有效的并打开所述文件，以及

如果所述确认数据与所述进一步的确认数据不匹配，判定所述托管密钥不是有效的并将无效的托管密钥从所述文件移除。

4.如权利要求1所述的计算机实现的方法，其特征在于，进一步包括：

生成所述托管密钥的盐值；以及

将所述盐值添加到所述安全散列。

5.如权利要求1所述的计算机实现的方法，其特征在于，保存所述确认数据、所述公钥和所述秘密密钥包括：将所述确认数据、所述公钥和所述秘密密钥保存到所述文件。

6.如权利要求1所述的计算机实现的方法，其特征在于，保存所述确认数据、所述公钥和所述秘密密钥包括：将所述确认数据、所述公钥和所述秘密密钥保存到包含所述文件的文件容器。

7.一种用于确认托管密钥的计算机实现的方法，所述计算机实现的方法包括执行计算机实现的操作，所述操作用于：

使用计算机，接收对文件执行操作的指令，所述文件具有与之相关联的托管密钥的确认数据，所述确认数据已通过使用安全散列对证书数据进行散列而生成，所述安全散列是在对所述文件执行的保存操作期间使用秘密密钥来生成的，所述证书数据是所述托管密钥专用的一公共信息；

响应于接收对所述文件执行所述操作的指令，使用所述计算机，请求对所述秘密密钥的解密的用户输入；

使用所述计算机，接收用户请求；

使用所述计算机，判定所述用户输入是否有效；

响应于判定所述用户输入有效，

使用所述计算机，解密所述秘密密钥，

使用所述计算机，使用所述秘密密钥来生成进一步的安全散列；

使用所述计算机，使用所述进一步的安全散列来对所述证书数据进行散列，以生成所述托管密钥的进一步的确认数据，

使用所述计算机，将所述确认数据与所述进一步的确认数据进行比较，

如果所述确认数据与所述进一步的确认数据匹配，使用所述计算机，判定所述托管密钥是有效的并对所述文件执行所述操作，以及

如果所述确认数据与所述进一步的确认数据不匹配，使用所述计算机，判定所述托管密钥不是有效的并移除无效的托管密钥与所述文件的关联。

8.如权利要求7所述的计算机实现的方法，其特征在于，所述安全散列和所述进一步的安全散列是基于散列的消息认证码(“HMAC”)。

9.如权利要求7所述的计算机实现的方法，其特征在于，所述操作是打开操作、重新保存操作，或后台任务。

10.如权利要求7所述的计算机实现的方法，其特征在于，还包括记录所述无效托管密钥。

11.如权利要求10所述的计算机实现的方法，其特征在于，记录所述无效托管密钥包括生成系统审计。

12.如权利要求7所述的计算机实现的方法，其特征在于，在接收对所述文件执行所述操作的指令之前，所述文件被保存为包括所述确认数据、所述托管密钥、所述证书数据，和所述秘密密钥。

13.如权利要求7所述的计算机实现的方法，其特征在于，在接收对所述文件执行所述操作的指令之前，所述文件被保存在文件容器中，所述文件容器包括所述确认数据、所述托管密钥、所述证书数据，和所述秘密密钥。

14.一种用于确认托管密钥的方法，包括：

接收打开文件的指令，所述文件具有与之相关联的托管密钥的确认数据，所述确认数据已通过使用基于散列的消息认证码(“HMAC”)对证书数据进行散列而生成，所述基于散列的消息认证码是对所述文件执行的保存操作期间使用秘密密钥来生成的，所述证书数据是所述托管密钥专用的一公共信息；

响应于接收到打开所述文件的指令，请求用于所述秘密密钥的解密的认证凭证；

接收认证凭证；

判定所述认证凭证是否有效；

响应于判定所述认证凭证有效，

解密所述秘密密钥；

使用所述秘密密钥生成进一步的HMAC，

使用所述HMAC来对所述证书数据进行散列，以生成所述托管密钥的进一步的确认数据，

将所述确认数据与所述进一步的确认数据进行比较，

如果所述确认数据与所述进一步的确认数据匹配，判定所述托管密钥是有效的并响应于打开所述文件的指令打开所述文件，以及

如果所述确认数据与所述进一步的确认数据不匹配，判定所述托管密钥不是有效的，并移除无效的托管密钥与所述文件的关联，并记录所述无效的托管密钥。

15.如权利要求14所述的方法，其特征在于，还包括：

在接收打开所述文件的指令之前，接收保存所述文件的指令；

使用所述秘密密钥来生成所述HMAC，所述秘密密钥被用于加密所述文件；

使用所述HMAC来对所述证书数据进行散列，以生成所述托管密钥的确认数据；以及

将所述确认数据、所述证书数据，和所述秘密密钥写入并保存到所述文件或包含所述文件的文件容器。

# 无效托管密钥的检测

[0001] 背景

[0002] 诸如文字处理应用、电子表格应用、和演示应用的文档创建应用，有时提供文档加密机制，通过该机制用户可提供用于加密文档的口令以防止对包含其中的信息的未经授权的访问。有些时候，没有暗中共享该口令的其他人可能需要包含在经加密的文档中的信息。例如，当用由公司一个雇员所创建的口令加密了一个文档而该雇员离开公司或仅仅是忘记该口令时，无人能够访问此文档，而该文档可能包含诸如人力资源或财务信息的至关重要且机密的公司信息。

[0003] 为了无需知晓口令而能够解密经加密的文档，可使用托管密钥机制。托管密钥机制是一种在受口令保护的文档中用于自动添加被称为托管密钥的基于证书的解密密钥的可配置机制。托管密钥机制允许口令保护的文档使用证书来解密而无需知晓口令，使得允许诸如上面所描述的实例中的文档恢复情形。

[0004] 经加密的文档有时使用两步系统。例如，在文档每一次被保存时，随机生成的秘密密钥被用于加密整个文档。用户提供的口令被用于导出新密钥，该新密钥用于加密该秘密密钥。经加密的秘密密钥可作为纯文本被存储在文档中。为解密该文档，密钥从用户输入的口令中导出并用于解密秘密密钥，秘密密钥然后被用于解密文档。

[0005] 托管密钥机制通过使用配置好的公钥加密秘密密钥来工作，公钥可以也可以不包含在文档的证书中。经加密的秘密密钥(即，托管密钥)，连同口令加密的秘密密钥一起，也被添加到文档。有私钥的任何人然后可解密该秘密密钥，从而解密该文档。由于秘密密钥在每次文档被保存时改变，文档中现存的任何托管密钥需要用新的秘密密钥来更新。托管密钥机制对设法获得对受保护的文档访问的攻击者而言不是没有弱点的。

[0006] 本文所做出的本公开正是关于这些和其他考虑事项而提出的。

## 发明内容

[0007] 在此描述了用于无效托管密钥(诸如由攻击者插入文件的那些无效托管密钥)的检测的概念和技术。作为示例，并为了示出使用上述托管密钥机制的潜在的弱点，考虑一个情形，其中攻击者获得对经口令保护的文件的访问，但是该攻击者没有口令且因此不能打开文件。该攻击者能改变文件容器以包括他或她自己的托管密码。由于攻击者不知道秘密密钥，新添加的恶意托管密钥是无效的。换言之，恶意托管密钥包含不同于实际中间加密密钥的密钥。当合法用户随后打开并接着重新保存该文件时，文件容器中全部的托管密钥可用新的秘密密钥来更新。作为该更新的结果，攻击者的恶意托管密钥现在有了有效的经加密的秘密密钥(即，新秘密密钥)而不是最初包含的不正确的密钥。攻击者随后能够解密并访问此文件，从而绕开了托管密钥机制。

[0008] 在此揭示的概念和技术提供了这样的机制，在文件被保存后文件中现存的托管密钥可被刷新并维护，而不允许上面的攻击情形。因为只有证书拥有者能够解密托管密钥，托管密钥不能被解密以检查有效性。在此描述的概念和技术还提供确认文件容器中的每个托管密钥而无需访问证书的私钥的机制。

[0009] 根据一个方面，使用一秘密信息(例如，秘密密钥)以及每个托管密钥专用的一公共信息(例如，证书散列或公钥)来生成安全散列，诸如基于散列的消息认证码(“HMAC”)。使用秘密密钥确保了托管密钥确认数据只有通过知晓秘密密钥才可生成，这阻止了攻击者生成适当的托管密钥确认数据。使用证书散列或公钥作为公共数据会将每个托管密钥确认数据绑定到特定证书，从而阻止攻击者从另一个托管密钥简单复制该确认数据。任何被发现是无效的托管密钥可从文件容器移除，并审计日志可被生成使得公司、个人、或其它实体能够知晓可能的安全性违背的企图。如果文档由某一版本的软件(其不知晓对更新先前合法托管密钥的需求)编辑，类似的，但不是恶意的情况可能发生。在任一情况下，可检测所提供的托管密钥是否应当被更新。

[0010] 根据另一方面，在被执行以保存文件的保存操作期间，确认数据被添加到文件容器中的每个托管密钥。接着，在被执行以打开文件的打开操作期间，确认数据被生成并与在保存操作期间被添加到每个托管密钥的确认数据进行比较。如果匹配存在，托管密钥被判定为有效。否则，托管密钥被判定为无效，且该托管密钥可从文件容器移除并可被记录。

[0011] 应当理解，上述主题可被实现为计算机控制的装置、计算机进程、计算系统或诸如计算机可读存储介质等制品。通过阅读下面的详细描述并审阅相关联的附图，这些及各种其他特征将变得显而易见。

[0012] 提供本发明内容是为了以简化的形式介绍将在以下具体实施方式中进一步描述的选择的概念。本发明内容并不旨在标识所要求保护的主题的关键特征或必要特征，也不旨在将本概述用来限制所要求保护的主题的范围。此外，所要求保护的主题不限于解决在本公开的任一部分中所提及的任何或所有缺点的实现。

## 附图说明

[0013] 图1是根据说明性实施例示出用于向文档添加一个或多个托管密钥的确认数据的方法的各方面的流程图。

[0014] 图2A和2B是根据说明性实施例示出用于确认一个或多个托管密钥的方法的各方面的流程图。

[0015] 图3是示出能够实现本文中所呈现的实施例的各方面的计算系统的说明性计算机硬件和软件体系结构的计算机体系结构图。

[0016] 详细描述

[0017] 以下详细描述涉及用于无效托管密钥的检测的概念和技术。作为在此描述的概念和技术的一个方面，使用一秘密信息(例如，秘密密钥)和每个托管密钥专用的一公共信息(例如，证书散列)来生成诸如HMAC的安全散列。该秘密密钥可以被存储在由中间密钥保护的加密信息中，仅仅为被授权解密该文档的人所知晓。使用秘密密钥确保了托管密钥确认数据只有通过知晓秘密密钥才可生成，这阻止了攻击者生成适当的托管密钥确认数据。使用证书散列或公钥作为公共数据会将每个托管密钥确认数据绑定到特定证书，从而阻止攻击者从另一个托管密钥简单复制该确认数据。任何被发现是无效的托管密钥可从文件容器移除，并审计日志可被生成使得公司、个人、或其它实体能够知晓可能的安全性违背的企图。

[0018] 尽管在结合计算机系统上的操作系统和应用程序的执行而执行的程序模块的一

般上下文中提出了本文描述的主题，但是本领域技术人员将认识到，其他实现可以结合其他类型的程序模块来执行。一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、组件、数据结构和其他类型的结构。此外，本领域技术人员将明白，可以利用其他计算机系统配置来实施本文描述的主题，这些计算机系统配置包括手持式设备、多处理器系统、基于微处理器的或可编程消费电子产品、小型计算机、大型计算机等等。

[0019] 在以下详细描述中，参考了构成详细描述的一部分并作为说明示出了各具体实施方式或示例的附图。现在参考附图(遍布若干附图中相同的标号表示相同的元素)，将提出用于无效托管密钥的检测的计算系统、计算机可读存储介质和计算机实现的方法的各方面。

[0020] 现在转到图1，将详细描述用于向一个或多个托管密钥的文件添加确认数据的方法100的各方面。应该理解，不一定按任何特定次序来呈现此处公开的方法的操作，并且构想了用替换次序来执行部分或全部操作是可能的。为了易于描述和说明，按所示次序来呈现各操作。可以添加、省略和/或同时执行操作，而不脱离所附权利要求书的范围。

[0021] 还应该理解，所示方法可以在任何时候结束并且不必完整地执行。这些方法的部分或全部操作和/或基本等效的操作可通过执行计算机存储介质上所包括的计算机可读指令来执行，如在下文中所定义的。如在说明书和权利要求书中使用的术语“计算机可读指令”及其变型，在本文是用来广泛地包括例程、应用、应用模块、程序模块、程序、组件、数据结构、算法等等。计算机可读指令可以在各种系统配置上实现，包括单处理器或多处理器系统、小型计算机、大型计算机、个人计算机、手持式计算设备、基于处理器的可编程消费电子产品、其组合等等。

[0022] 因此，应该理解，此处所述的逻辑操作被实现为(1)一系列计算机实现的动作或运行于计算系统上的程序模块，和/或(2)计算系统内的互连的机器逻辑电路或电路模块。该实现是取决于计算系统的性能及其他要求的选择问题。因此，此处描述的逻辑操作被不同地称为状态、操作、结构设备、动作或模块。这些操作、结构设备、动作和模块可以用软件、固件、专用数字逻辑及其任何组合来实现。

[0023] 该方法100被描述为在被执行来保存文件的保存操作期间执行。本文以下描述的各方面不必对某应用、应用类型、文件，或文件类型是特定的。在一些实施例中，应用被配置成打开第一状态的文件，接收诸如编辑或其它交互的用户输入，并保存不同于第一状态的第二状态的文件。在其它实施例中，文件被保存，但是不对文件数据作出修改。在一些是实施例中，文件随对元数据、格式参数，或文件内包含的不是文件数据的其它数据的改变而被保存。在一些实施例中，应用被配置成存储文件，但是可能也可能不具有执行除了打开和保存以外的操作的能力。例如，在一些实现中，应用可能不被配置成以任何方式编辑文件。在一些实施例中，保存操作包括复制和粘贴操作，其中第一文件被复制并粘贴从而创建并保存新文件。

[0024] 在一些实施例中，文件是文档，诸如文字处理文档、电子表格文档、演示文档、绘图文档，或协作文档。在一些实施例中，用于创建和/或查看这样的文档的应用分别是文字处理应用(诸如可以从华盛顿州雷蒙德市的微软公司获得的MICROSOFT WORD)、电子表格应用(诸如可以从华盛顿州雷蒙德市的微软公司获得的MICROSOFT EXCEL)、演示应用(诸如可以从华盛顿州雷蒙德市的微软公司获得的MICROSOFT POWERPOINT)、绘图应用(诸如可以从华

盛顿州雷蒙德市的微软公司获得的MICROSOFT VISIO)，或协作应用(诸如可以从华盛顿州雷蒙德市的微软公司获得的MICROSOFT SHAREPOINT)。在一些实施例中，应用是只读应用，配置成允许用户查看但不编辑文档。在其它实施例中，应用是读/写应用，配置成允许用户查看并编辑文档。该应用可以是本地地安装在计算机系统上的独立应用、安装在可由计算机系统远程地访问的远程系统上的远程应用，或web应用。可以构想其它文档类型和相关联的应用。

[0025] 方法100也针对包含一个或多个托管密钥的文件来描述。替换地或另外地，包含文件的文件容器可包含一个或多个托管密钥。一些托管密钥可被存储在文件容器中而其它可被存储在文件本身中。文件容器是容器或包装元文件格式，其规范描述了不同数据元素和元数据如何共存在文件中。

[0026] 方法100在操作102开始，其中接收到保存文件的指令。保存文件的指令可通过由配置成保存文件的应用呈现的或该应用的图形用户界面(“GUI”)或其它用户界面来接收。GUI可被表示为菜单或菜单的一部分，如图标、如功能区界面或功能区界面的部分、作为弹出GUI、它们的一些组合等等。保存文件的指令可经由接口设备(诸如键盘、键区、鼠标、游戏垫、遥控设备)，或经由任何通过一个或多个按钮、触摸屏、触摸垫、麦克风的其它接口设备，或提供用户可用来指令应用保存文件的机制的其它人机接口来接收。可构想这些接口设备中的一个或多个上专用的或编程了的物理保存按钮。

[0027] 方法100余下的操作在由操作102中所接收的保存文件的指令所触发的保存操作期间执行。从操作102，方法100前进到操作104，其中使用秘密密钥生成安全散列。在一些实施例中，秘密密钥是随机或伪随机生成的，并被用于加密文件。在一些实施例中，秘密密钥使用用户提供的口令来加密。在一些实施例中，经加密的秘密密钥以纯文本被存储在文件中。可替换地，经加密的秘密密钥可以某其它格式被存储在文件中。

[0028] 在一些实施例中，在操作104中生成的安全散列是散列消息认证码，或被称为散列消息认证校验和(“HMAC”)。在一些实施例中，HMAC是使用作为一秘密信息的秘密密钥和专用于HMAC要被生成的特定托管密钥的某公共信息(诸如证书数据或公钥)来生成的。在替换的实施例中，替代HMAC，秘密密钥的常规散列和证书数据(或公钥)被使用。尽管各实施例中利用常规散列所得的散列可能密码性较弱，然而，常规散列的使用可在特定情形中找到应用。

[0029] 如果在每个保存操作期间或为其它熵目的不被改变，在一些实施例中，正如该情况下，每个托管密钥的随机盐值被生成并被包括在散列或HMAC中。盐值随后和托管密钥数据的其余部分一起被存储在文件容器中。

[0030] 从操作104，方法100前进到操作106，其中使用操作104中生成的安全散列来对证书数据进行散列，以生成托管密钥的确认数据。可替换地，公钥可被使用来代替证书数据。方法100接着前进到操作108，其中确认数据、证书数据，和经加密的秘密密钥被写到文件的文件容器中。可替换地，该数据的全部或部分直接被写入文件中。方法100接着前进到操作110，其中文件容器被保存。方法100从操作110行进至操作112，在此处方法100结束。

[0031] 转到图2A和2B，用于确认一个或多个托管密钥的方法200的各方面将被详细描述。方法200被描述为在打开操作期间执行，所述打开操作用于打开在参考图1所示的方法100描述的保存操作执行期间被保存的文件。文本以下描述的各方面也不必对某应用、应用类

型、文件，或文件类型是特定的。在一些实施例中，应用被配置成打开文件并允许文件的编辑。在一些实施例中，应用被配置成打开文件，但是可能也可能不具有执行除了打开以外的操作的能力。例如，在一些实现中，应用可能不被配置成以任何方式编辑文件。在一些实施例中，根据方法200的用于打开文件的应用和根据上述方法100的用于保存文件的应用是同一个。在其它实施例中，这些应用不同。用于保存文件的计算机系统或设备可以是与用于打开该文件的计算机系统或设备相同或不同的。

[0032] 首先转到图2A，方法200开始并前进到操作202，其中接收到打开文件的指令。响应于打开文件的指令，请求用于秘密密钥的解密的用户输入。在一些实施例中，对用户输入的请求是呈现在提示用户提供用户输入的应用内的通知，尽管请求可以采取替换形式。在一些实施例中所请求的用户输入是认证凭证，例如但不限于，口令、通行码、个人识别号、安全问题/答案、通行短语、语音通行短语、其它安全证书，及其组合等等。在一些实施例中，所请求的用户输入包括对来自两个或多个以下类别的多因素认证凭证的请求：一个人拥有什么、一个人是什么、一个人知晓什么、一个人已经做了什么，和一个人位于什么地方。

[0033] 打开文件的指令可通过由配置成打开文件的应用呈现的或该应用的GUI或其它用户界面来接收。GUI可被表示为菜单或菜单的一部分，如图标、如功能区界面或功能区界面的部分、作为弹出GUI或弹出GUI的部分、它们的一些组合等等。可替换地，打开文件的指令可经由接口设备(诸如键盘、键区、鼠标、游戏垫、遥控设备)，或经由任何通过一个或多个按钮、触摸屏、触摸垫、麦克风的其它接口设备，或提供用户可用来指令应用打开文件的机制的其它人机接口来接收。可构想这些接口设备中的一个或多个上专用的或编程了的物理打开按钮。

[0034] 从操作202，方法200前进到操作204，其中响应于操作202中对用户输入的请求接收到用户输入。方法200接着前进到操作206，其中作出关于在操作204中接收到的用户输入是否有效的判定。该判定可基于将在操作204中接收的用户输入与所期望的用户输入(诸如所期望的口令或其它所期望的认证凭证)进行比较来作出。所期望的用户输入可被存储在应用正在其上执行的同一个计算机或设备上，或可被远程地存储在诸如配置成确认在操作204接收的用户输入的认证服务器上。

[0035] 如果在操作206，判定用户输入不有效，方法200前进到操作208，其中指示用户输入无效的消息被呈现。可替换地，指示用户输入是无效的消息不被呈现。在一些实施例中，一旦作出用户输入不是有效的判定或在其后一时间，应用关闭。在任何情况中，方法200接着前进到操作210，其中方法200结束。

[0036] 如果，在操作206，判定了用户输入是有效的，方法200前进到操作212，其中秘密密钥被解密。从操作212，方法200前进到操作214，其中使用秘密密钥生成安全散列。在一些实施例中，操作214中生成的安全散列是HMAC。在一些实施例中，HMAC是使用作为一秘密信息的秘密密钥和专用于HMAC要被生成的特定托管密钥的某公共信息(诸如证书数据或公钥)来生成的。在替换的实施例中，替代HMAC，秘密密钥的常规散列和证书数据(或公钥)被使用。尽管各实施例中利用常规散列所得的散列可能密码性较弱，然而，常规散列的使用可在特定情形中找到应用。

[0037] 从操作214，方法200前进到操作216，其中使用操作214中生成的安全散列来对证书数据进行散列，以生成托管密钥的确认数据。可替换地，公钥可被使用代替证书数据。方

法200接着前进到图2B，具体地，操作218。在操作218，操作216生成确认数据与在图1的操作110中的文件容器中保存的确认数据进行比较。从操作218，方法200前进到操作220，其中作出关于在两组确认数据之间是否存在匹配的判定。

[0038] 如果，在操作220，判定在确认数据组之间不存在匹配，方法200前进到操作222，其中作出托管密钥无效的判定并且将该无效托管密钥从文件移除。方法200接着前进到操作224，其中无效托管密钥被记录。在一些实施例中，生成系统审计，使得对文件的安全性感兴趣的公司或其它实体可知晓可能的安全性违背的企图。可替换地，无效托管密钥不被记录。在任何情况中，方法200接着前进回到图2A，且具体地，操作210，其中方法200结束。

[0039] 在另一个实施例中(未示出)，在操作224，方法200前进到操作228，其中文件被打开。在这个实施例中，指示文件可能已经被篡改的警告可被呈现给用户。方法200接着可前进回到图2A，且具体地，操作210，其中方法200结束。

[0040] 如果，在操作220，判定了在确认数据组之间存在匹配，方法200前进到操作226，其中判定了托管密钥是有效的。方法200接着前进到操作228，其中文件被打开。从操作228，方法220前进回到图2A，且具体地，操作210，其中方法200结束。

[0041] 尽管托管密钥在图2中被描述为在打开操作期间确认，可以理解托管密钥可另选地在保存操作期间作为后台任务或响应于特定预定义输入来被确认。

[0042] 图3示出能够执行本文所描述的用于无效托管密钥的检测的说明性计算机体系结构300。由此，图3所示的计算机体系结构300示出服务器计算机、移动电话、PDA、智能电话、台式计算机、上网本计算机、平板计算机、和/或膝上型计算机的体系结构。计算机体系结构300可用于执行本文所呈现的软件组件的任何方面。

[0043] 图3所示的计算机体系结构300包括中央处理单元302(“CPU”)、包括随机存取存储器306(“RAM”)和只读存储器(“ROM”)308的系统存储器304、以及将存储器304耦合至CPU 302的系统总线310。基本输入/输出系统被存储在ROM 308中，该系统包含帮助诸如在启动期间计算机体系结构300中的元件之间传递信息的基本例程。计算机体系结构300还包括用于存储操作系统314、应用316和数据318的大容量存储设备312。数据318包括诸如上面所描述的托管密钥、秘密密钥、证书、安全散列、确认数据和文件数据之类的一个或多个托管密钥320、一个或多个秘密密钥322、一个或多个证书或公钥324，一个或多个安全散列326、确认数据328，和文件数据330。

[0044] CPU302被配制成执行操作系统314。操作系统314是用于控制计算机体系结构300的操作的应用程序。应用316是被配置成在操作系统314之上执行以提供本文所述的各种功能的可执行程序。例如，应用316可提供上面参考图1和2A/2B分别描述的关于确认托管密钥的保存操作和打开操作。在一些实施例中，应用316被配置成打开第一状态的文件，接收诸如编辑或其它交互的用户输入，并保存不同于第一状态的第二状态的文件。在其它实施例中，应用316被配置成保存文件，即使没有对文件数据330作出改变。在一些实施例中，文件随对元数据、格式参数，或文件内包含的不是可见数据的其它数据的改变而被保存。在一些实施例中，应用316被配置成保存文件，但是可能也可能不具有执行除了打开和保存以外的操作的能力。例如，在一些实现中，应用316可能不被配置成以任何方式编辑文件。

[0045] 在一些实施例中，应用316是文字处理应用(诸如可以从华盛顿州雷蒙德市的微软公司获得的MICROSOFT WORD)、电子表格应用(诸如可以从华盛顿州雷蒙德市的微软公司获

得的MICROSOFT EXCEL)、演示应用(诸如可以从华盛顿州雷蒙德市的微软公司获得的MICROSOFT POWERPOINT)、绘图应用(诸如可以从华盛顿州雷蒙德市的微软公司获得的MICROSOFT VISIO),或协作应用(诸如可以从华盛顿州雷蒙德市的微软公司获得的MICROSOFT SHAREPOINT)。替换地或另外地,应用316是一个或多个前述文档创建应用的基于web的版本,并且在这些实施例中,计算机体系结构300用作被配置成将应用316作为基于web的应用提供的服务器计算机的体系结构。

[0046] 大容量存储设备312通过连接至总线310的大容量存储控制器(未示出)连接至CPU 302。大容量存储设备312及其相关联的计算机可读介质为计算机体系结构300提供非易失性存储。虽然对此处包含的计算机可读介质的描述引用了诸如硬盘或CD-ROM驱动器之类的大容量存储设备,但是本领域的技术人员应该明白,计算机可读介质可以是可由计算机体系结构300访问的任何可用计算机存储介质或通信介质。

[0047] 通信介质包括诸如载波或其它传输机制等已调制数据信号中的计算机可读指令、数据结构、程序模块或其它数据,且包含任何传递介质。术语"已调制数据信号"指的是其一个或多个特征以在信号中编码信息的方式被更改或设定的信号。作为示例而非限制,通信介质包括有线介质,诸如有线网络或直接线连接,以及无线介质,诸如声学、RF、红外、和其它无线介质。上述的任意组合也应包括在计算机可读介质的范围之内。

[0048] 作为示例而非限制,计算机存储介质可包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据等信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。例如,计算机介质包括但不限于,RAM、ROM、EPROM、EEPROM、闪存或其他固态存储器技术、CD-ROM、数字多功能盘("DVD")、HD-DVD、蓝光(BLU-RAY)或其他光学存储、磁带盒、磁带、磁盘存储或其他磁性存储设备、或能用于存储所需信息且可以由计算机体系结构300访问的任何其他介质。为了声明的目的,短语计算机存储介质摂及其变型本质上不包括波、信号和/或其他瞬态和/或无形通信介质。

[0049] 根据各个实施例,计算机体系结构300可使用通过网络332到远程计算机的逻辑连接在联网环境中操作。网络332可以是互联网、因特网、内联网或外联网。可以通过一个或多个有线或无线接入网络(未示出)来提供对网络332的接入,如本领域的技术人员将理解的。

[0050] 计算机体系结构300可以通过连接至总线310的网络接口单元334来连接到网络332。应当理解,网络接口单元334还可用于连接到其他类型的网络和远程计算机系统。计算机体系结构300也可包括输入/输出控制器336,用于接收和处理来自多个其他设备,包括键盘、鼠标、电子指示笔、或其他输入设备(未在图3中示出)的输入。类似地,输入/输出控制器336可提供到显示屏、打印机、或者其他类型的输出设备(在图3中也未示出)的输出。

[0051] 应当理解,本文所描述的软件组件在被加载到CPU 302中并被执行时可以将CPU 302和总体计算机体系结构300从通用计算系统变换成为方便本文所提出的功能而定制的专用计算系统。CPU 302可以用任意数量的晶体管或其他分立的电路元件(它们可以分别地或共同地呈现任意数量的状态)构建。更具体地,CPU 302可以响应于包含在本文所公开的软件模块中的可执行指令来作为有限状态机进行操作。这些计算机可执行指令可以通过指定CPU 302如何在各状态之间转换来变换CPU 302,由此变换了构成CPU 302的晶体管或其它分立硬件元件。

[0052] 对本文所提出的软件模块的编码也可变换本文所提出的计算机可读介质的物理

结构。在本说明书的不同实现中，物理结构的具体转换可取决于各种因素。这样的因素的示例可以包括，但不仅限于：用于实现计算机可读介质的技术、计算机可读介质被表征为主存储器还是辅存储器等等。例如，如果计算机可读介质被实现为基于半导体的存储器，则本文所公开的软件可以通过变换半导体存储器的物理状态而在计算机可读介质上编码。例如，软件可以变换构成半导体存储器的晶体管、电容器或其它分立电路元件的状态。软件还可变换这些组件的物理状态以在其上存储数据。

[0053] 作为另一示例，本文所公开的计算机可读介质可以使用磁或光技术来实现。在这些实现中，本文所提出的软件可以在磁或光介质中编码了软件时变换所述磁或光介质的物理状态。这些转换可包括更改给定磁性介质内的特定位置的磁性特征。这些变换还可以包括改变给定光学介质内的特定位置的物理特征或特性，以改变这些位置的光学特性。在没有偏离本说明书的范围和精神的情况下，物理介质的其他转换也是可以的，前面提供的示例只是为了便于此讨论。

[0054] 鉴于以上内容，应当理解，在计算机体系结构300中发生许多类型的物理变换以便存储并执行本文所提出的软件组件。还应当理解，计算机体系结构300可包括其它类型的计算设备，包括手持式计算机、嵌入式计算机系统、个人数字助理、以及本领域技术人员已知的其它类型的计算设备。还可构想计算机体系结构300可以不包括图3所示的全部组件、可包括在图3中未明确地示出的其他组件、或者可利用完全不同于图3所示的体系结构。

[0055] 基于上述内容，应当理解，本文已经公开了用于无效第三方密钥的检测的技术。虽然用计算机结构特征、方法和变换动作、特定计算机器、以及计算机可读介质专用的语言描述了本文中所描述的主题，但是应当理解，所附权利要求书中所定义的本发明不必限于本文中所描述的具体特征、动作、或介质。相反，这些具体特征、动作以及介质是作为实现权利要求的示例形式而公开的。

[0056] 以上所述的主题仅作为说明提供，并且不应被解释为限制。可对本文中所描述的主题作出各种修改和改变，而不必遵循示出和描述的示例实施例和应用且不背离所附权利要求书中所阐述的本发明的真正精神和范围。

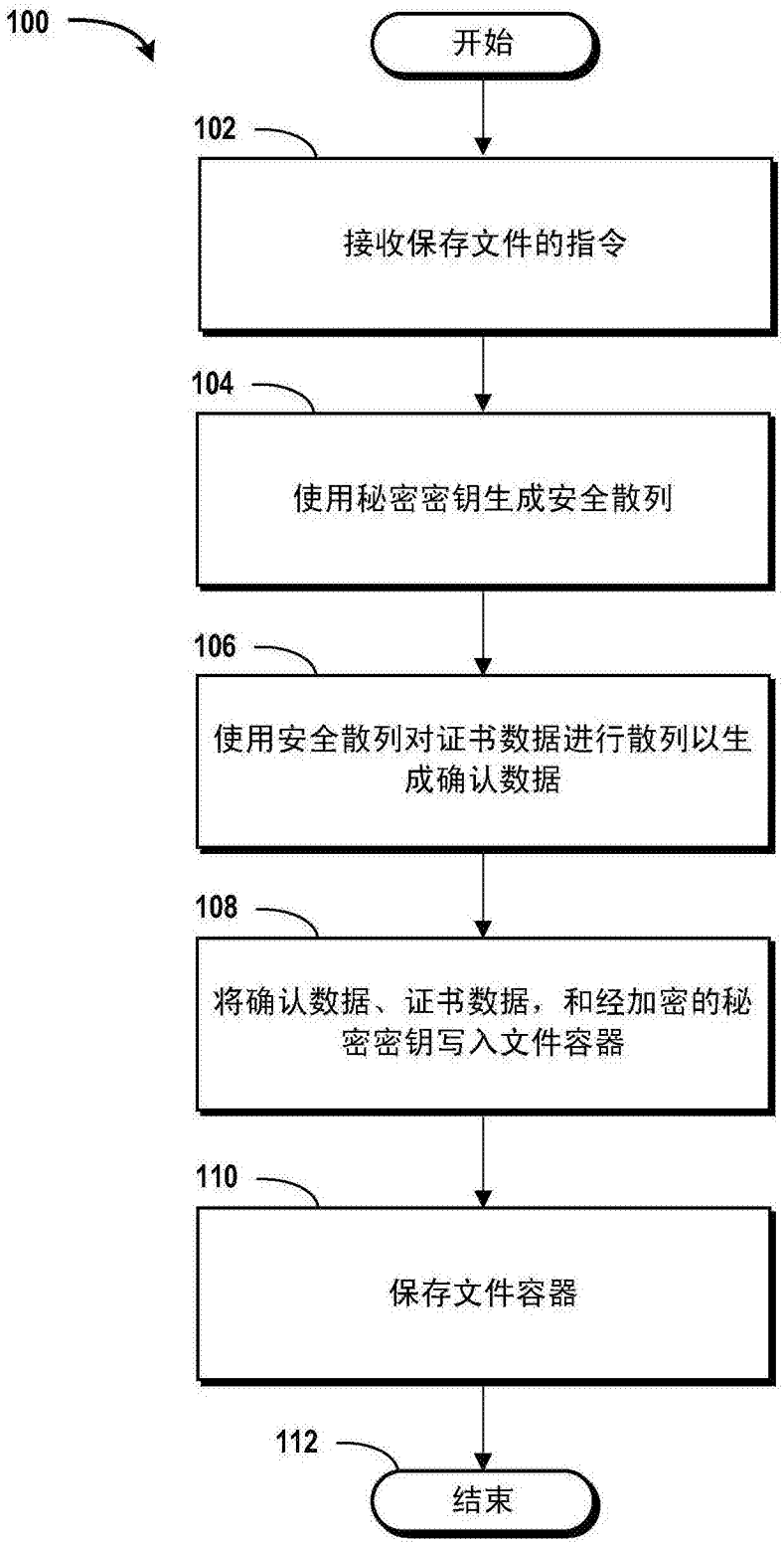

100
开始
102
接收保存文件的指令
104
使用秘密密钥生成安全散列
106
使用安全散列对证书数据进行散列以生成确认数据
108
将确认数据、证书数据，和经加密的秘密密钥写入文件容器
110
保存文件容器
112
结束

图1

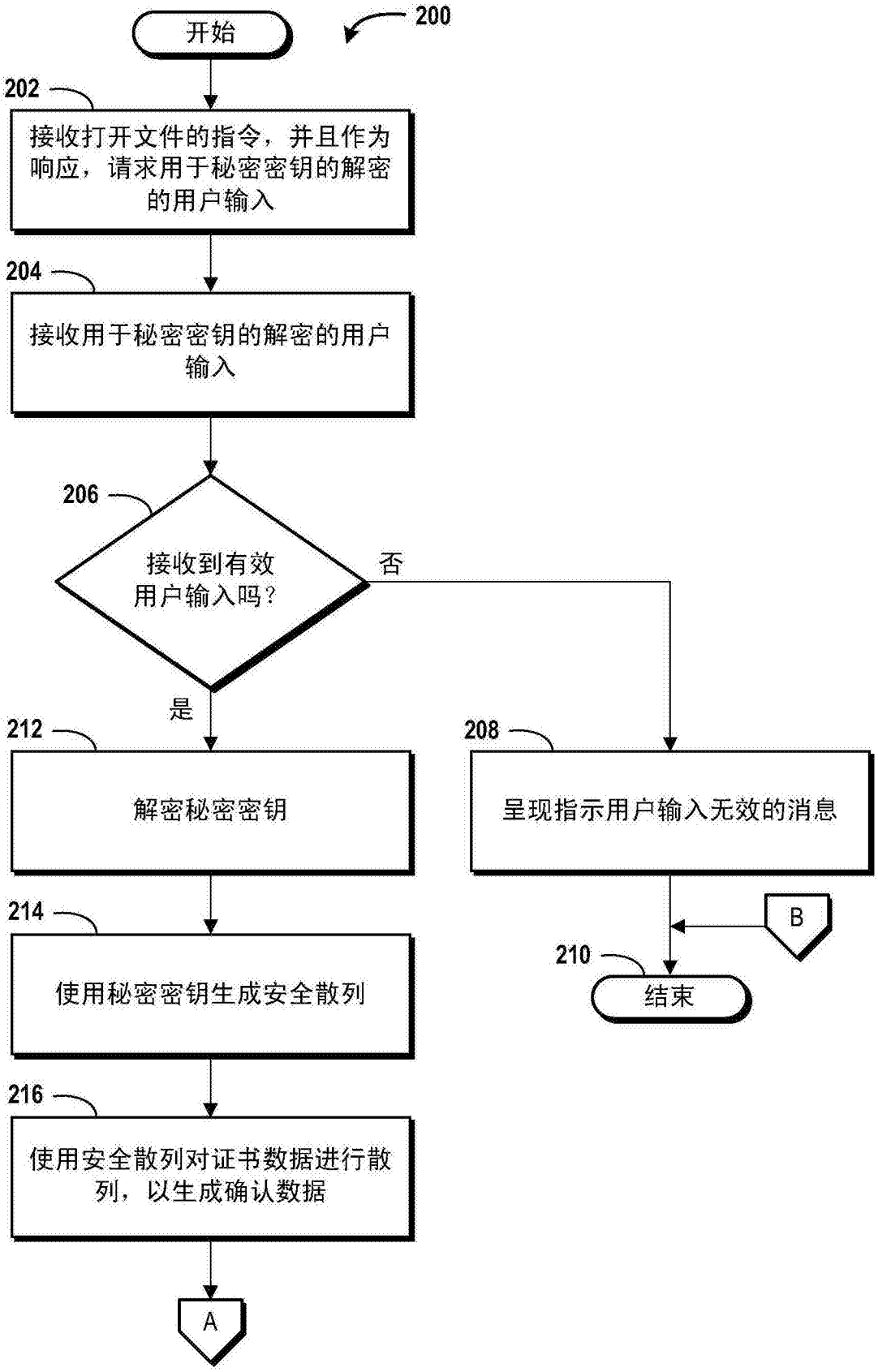

开始
200
202
接收打开文件的指令，并且作为响应，请求用于秘密密钥的解密的用户输入
204
接收用于秘密密钥的解密的用户输入
206
接收到有效用户输入吗？
否
是
212
解密秘密密钥
208
呈现指示用户输入无效的消息
B
210
结束
214
使用秘密密钥生成安全散列
216
使用安全散列对证书数据进行散列，以生成确认数据
A

图2A

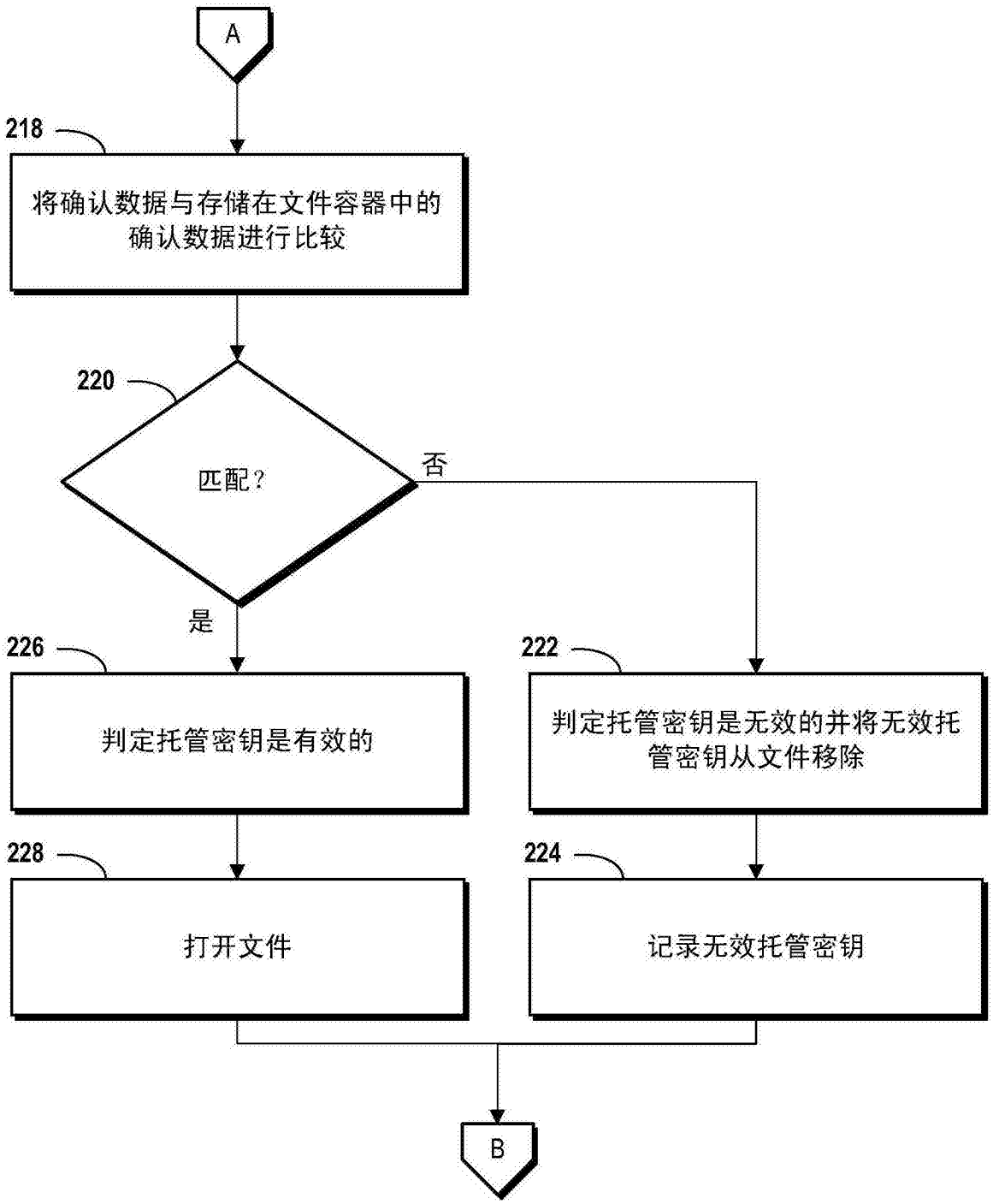

A
218
将确认数据与存储在文件容器中的确认数据进行比较
220
匹配？
否
是
226
判定托管密钥是有效的
222
判定托管密钥是无效的并将无效托管密钥从文件移除
228
打开文件
224
记录无效托管密钥
B

图2B

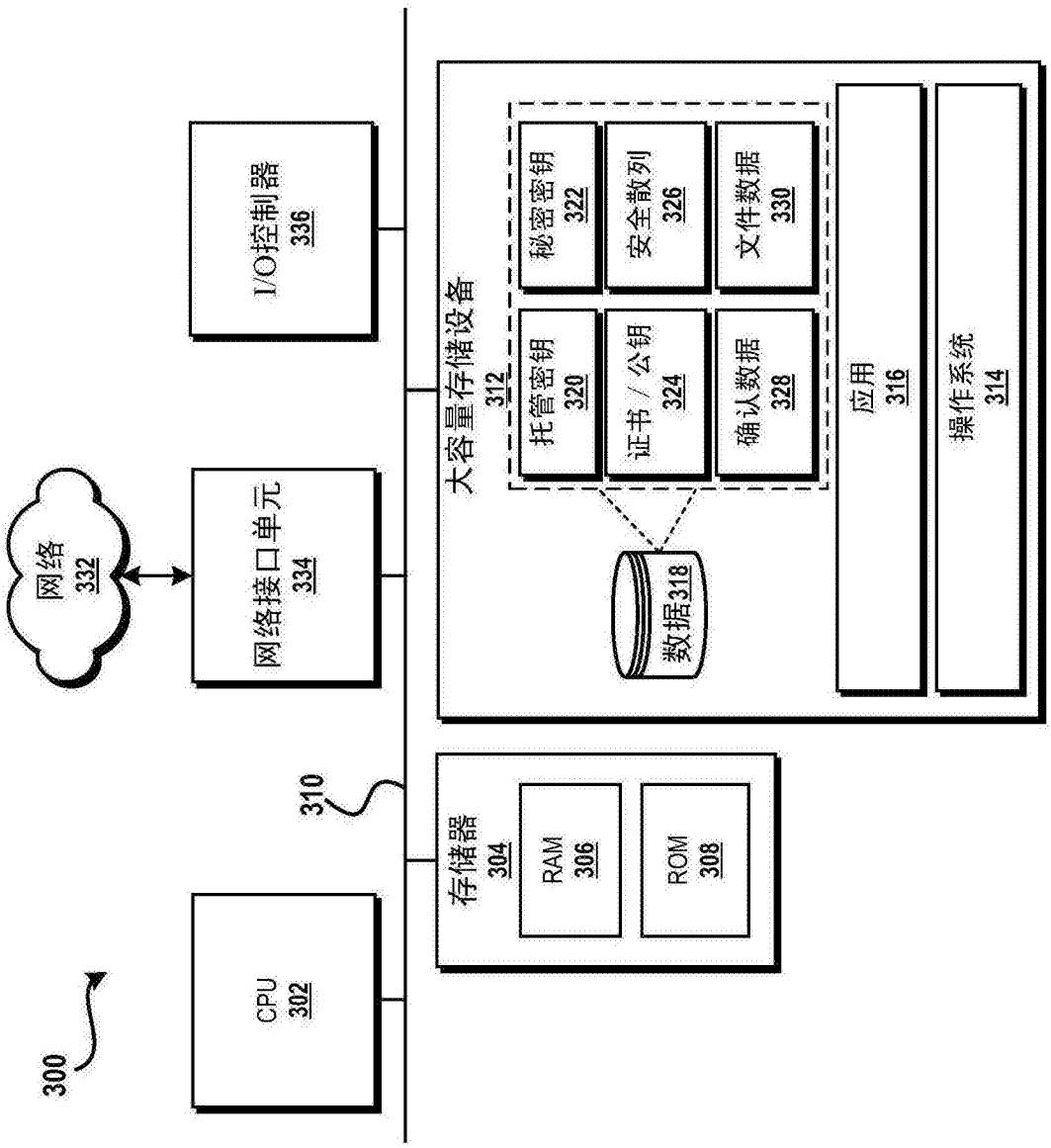

300
CPU
302
310
存储器
304
RAM
306
ROM
308
网络接口单元
334
网络
332
I/O控制器
336
大容量存储设备
312
托管密钥
320
证书 / 公钥
324
确认数据
328
秘密密钥
322
安全散列
326
文件数据
330
数据318
应用
316
操作系统
314

图3