(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114651251 A
(43)申请公布日 2022.06.21

(21)申请号 201980102377.9
(22)申请日 2019.11.22
(85)PCT国际申请进入国家阶段日
2022.05.20
(86)PCT国际申请的申请数据
PCT/US2019/062756 2019.11.22
(87)PCT国际申请的公布数据
WO2021/101560 EN 2021.05.27
(71)申请人 惠普发展公司,有限责任合伙企业
地址 美国德克萨斯州
(72)发明人 A·J·鲍德温 S·里斯
J·格里芬 D·埃拉姆
(74)专利代理机构 中国专利代理(香港)有限公司 72001
专利代理师 李雪娜 吕传奇
(51)Int.Cl.
G06F 21/31(2006.01)
G06F 21/62(2006.01)
H04L 9/30(2006.01)

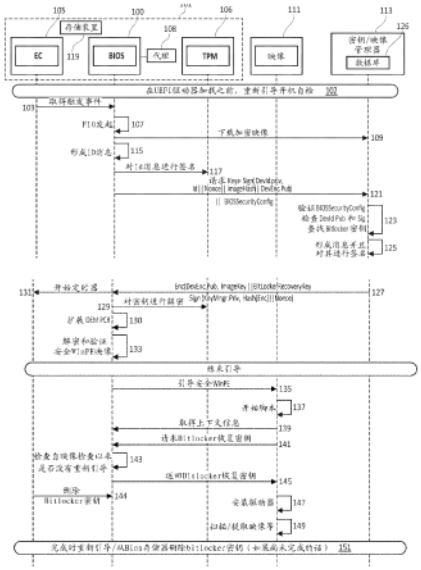
权利要求书2页 说明书7页 附图3页

(54)发明名称

恢复密钥

(57)摘要

在一些示例中,一种用于访问设备的加密系统的密码恢复密钥的方法包括:将在密钥管理系统处接收的设备身份映射到存储在密钥管理系统中的恢复密钥;指定恢复密钥链接到的至少一个设备相关操作;为设备生成经加密的消息,该经加密的消息包括恢复密钥;以及将经加密的消息和经签名的消息传输到设备。



CN 114651251 A

1.一种用于访问设备的加密系统的密码恢复密钥的方法,所述方法包括:

将在密钥管理系统处接收的设备身份映射到存储在密钥管理系统中的恢复密钥;

指定恢复密钥链接到的至少一个设备相关操作;

为设备生成经加密的消息,所述经加密的消息包括恢复密钥;以及

将经加密的消息和经签名的消息传输到设备。

2.如权利要求1中要求保护的方法,其中所述恢复密钥被链接以使得受信无盘操作系统映像能够访问设备的逻辑卷。

3.如权利要求1中要求保护的方法,其中所述经签名的消息包括经加密的消息的散列和从设备接收的随机数。

4. 如权利要求1中要求保护的方法,进一步包括:

在密钥管理系统处接收包括数据映像的散列的请求;以及

验证数据映像的散列;以及

在验证的基础上,提供经加密的消息。

5.如权利要求4中要求保护的方法,其中使用映像密钥对数据映像进行加密,所述方法进一步包括为设备提供映像密钥作为经加密的消息的一部分,由此使得设备能够对数据映像进行解密。

6. 如权利要求1中要求保护的方法,进一步包括:

接收上下文信息;以及

在上下文信息的基础上生成用于经由数据映像执行的脚本。

7.如权利要求1中要求保护的方法,进一步包括:

提供对数据映像的直接访问。

8.如权利要求1中要求保护的方法,进一步包括:

提供对令牌的访问以使能对数据映像的访问。

9.如权利要求2中要求保护的方法,进一步包括:

提供与恢复密钥相关联的至少一个硬件策略,指定在受信无盘操作系统映像的引导之前要禁用的至少一个设备硬件组件。

10.如权利要求9中要求保护的方法,进一步包括:基于硬件策略,指令设备硬件组件禁用所述至少一个设备硬件组件。

11.一种设备,包括:

设备硬件组件,用于请求存储在密钥管理系统中的恢复密钥;

受信平台模块组件,用于解密在设备处以加密形式接收的恢复密钥,所述恢复密钥链接到至少一个设备相关操作;以及

存储位置,包括使用恢复密钥可访问的经加密的部分。

12.如权利要求11中要求保护的设备,所述设备硬件组件进一步在触发事件的基础上下载数据映像。

13.如权利要求11中要求保护的设备,所述受信平台模块组件用于控制身份,所述身份用于对表示对恢复密钥的请求的消息进行签名的身份。

14.一种编码有用于访问设备的加密系统的密码恢复密钥的指令的机器可读存储介质,所述指令由装置的处理器可执行以使装置进行以下操作:

从设备接收对恢复密钥的请求,所述恢复密钥链接到至少一个设备相关操作;

将与请求相关联的设备标识符映射到设备的恢复密钥;以及

生成对请求的签名响应,所述签名响应包括恢复密钥的经加密版本。

15.如权利要求14中要求保护的机器可读存储介质,进一步编码有在受信无盘操作系统映像的引导之前禁用至少一个设备硬件组件的指令。

恢复密钥

背景技术

[0001] 诸如计算平台之类的端点设备例如可以使用各种各样不同的操作系统(OS),这些操作系统可以位于设备的本地存储装置上。这样的本地存储装置可以用在设备的主安装OS的引导(boot)周期期间提供的访问来加密。

附图说明

[0002] 从以下结合附图理解的详细描述中,某些示例的各种特征和优点将显而易见,附图仅作为示例一起图示了多个特征,并且其中:

图1是根据示例的用于访问设备的密码恢复密钥的方法的示意性表示;

图2是根据示例的用于访问设备的密码恢复密钥的方法的流程图;以及

图3是根据示例的密钥/映像管理器系统的示意性表示。

具体实施方式

[0003] 在以下描述中,出于解释的目的,阐述了某些示例的许多特定细节。说明书中对"示例"或类似语言的引用意味着结合该示例描述的特定特征、结构或特性包括在至少那一个示例中,但不一定包括在其它示例中。

[0004] 诸如以例如计算机、膝上型计算机或其它计算或智能装置形式的用户设备之类的端点设备可能能够使用各种各样不同的操作系统。一般而言,这样的操作系统被提供在所讨论的设备的本地存储位置(诸如例如硬盘或固态驱动器)上。在设备引导时,可以使用作为加密机制的一部分提供的加密密钥将本地存储装置从加密状态解锁。

[0005] 在示例中,端点设备可以使用除了安装在端点设备的本地存储位置中的OS之外的OS、或者由另一个设备来引导。例如,在远离端点设备的位置处的设备可以用于引导到端点设备,例如进入恢复状态。在另一个示例中,可以使用不以其它方式形成安装在端点设备上的OS的一部分的OS来引导端点设备。

[0006] 当端点设备从另一个OS或设备引导时,除非提供加密密钥,否则加密的驱动器保持锁定。诸如例如微软的bitlocker之类的磁盘加密机制通过使用包含OS引导的测量结果的平台配置寄存器(PCR)将磁盘加密密钥密封在受信平台模块(TPM)内来保护磁盘加密密钥。因此,当使用适当的Windows引导机制时,解密本地存储装置的(一个或多个)密钥变得可用。

[0007] 用户(端点)设备可能出于多个原因而变得不可操作或受损。例如,在设备的本地存储装置上提供的设备OS可能由于一般的文件系统或升级问题而变得被破坏,或者可能变得被恶意软件感染。例如,操作系统不断受到来自各种参与者(actor)的攻击,这些参与者希望找到让他们运行他们自己的软件或恶意软件的漏洞利用(exploit),所述软件或恶意软件诸如但不限于远程访问木马、勒索软件或加密货币矿工。还可能存在使端点设备受损、不可引导或不可使用的其它软件或硬件问题。

[0008] 在一些情况下,诸如当OS被破坏或可能受到恶意软件感染时,解密磁盘并引导到

替代的无盘引导映像以进行例如清理或恢复可能是有用的。然而，这样的映像不容易访问磁盘加密密钥(例如bitlocker密钥)。例如，在bitlocker的情况下，企业可以在具有适当访问控制的活动目录内保存设备的恢复密钥，使得用户和管理员可以访问所述密钥。对于消费者或小/中型企业等等，密钥可以以受控方式保存于在线存储系统内。然而，这些密钥恢复系统的接口通常不允许恢复无盘引导映像的简单自动化(easy automation)，因为解密密钥通常将由用户在已经键入长字符串以使能访问之后经由不同的系统来访问。

[0009] 根据示例，提供了一种用于自动化访问和/或检索设备的加密系统的(一个或多个)密码恢复密钥的方法，以使得能够通过例如无盘引导映像来访问设备的本地存储设备。也就是说，在示例中，提供了一种机制，使得受信无盘映像(诸如例如Win PE/RE映像)能够以自动化方式访问逻辑卷加密系统(例如bitlocker)的恢复密钥，由此使得受信无盘映像能够访问系统或端点设备的磁盘。一旦建立了访问，就可以在端点设备上执行脚本，诸如恢复和/或分析脚本。

[0010] 根据示例，响应于触发机制，可以使用受信无盘引导映像来引导端点设备。该触发机制可以是用户或系统发起的。例如，作为源自系统上可能存在的恶意软件的自动触发的结果(例如，作为反病毒扫描和随后对以触发形式发起响应的可能恶意软件的检测的结果)，可以使用受信映像来引导端点设备。替代地，用户可以被提示、或可以选择在引导时使用受信磁盘映像来引导。例如，这可能是响应于来自如上面所描述的先前反病毒扫描的结果，或者响应于来自第三方(诸如设备管理员或企业)的用于提示用户的指令。替代地，可以响应于外部指令，例如来自企业的指令，使用受信磁盘映像自动引导端点设备，而无需最终用户干预。在示例中，设备硬件组件(例如固件)可以用于在引导过程期间施行设备硬件初始化。设备硬件组件还可以为操作系统和程序提供运行时服务，并且通常将是设备上的预安装组件。这样的设备硬件组件可以被称为BIOS(基本输入/输出系统)，并且可以以一个或多个组件(诸如集成电路)的形式提供。本文中对BIOS的引用表示可以用于在设备引导过程期间施行设备硬件初始化的任何合适的设备硬件组件。

[0011] 图1是根据示例的用于访问设备的密码恢复密钥的方法的示意性表示。在图1的示例中，端点设备101的BIOS 100可以接收触发事件103。在图1的示例中，可以在BIOS 100处接收来自设备安全性控制器(EC)105的触发事件103。在示例中，作为设备的受信管理组件的角色的EC 105可以管理从设备的另一个组件接收的触发事件，以便使该触发事件在引导时可用。EC 105可以存储已经经由安全通信从运行在OS内的代理或管理代理(在OS中或经由替代通道)提供给它的触发事件。在示例中，这可以响应于例如反病毒扫描的结果。替代的触发可以是当BIOS引导时，用户可以(例如，通过按f10)进入BIOS菜单，并且请求使用替代的引导和访问加密密钥的服务。

[0012] 因此，EC 105可以存储响应于例如如上面所描述的反病毒扫描的结果、或者响应于来自诸如管理设备101的安全性策略的企业之类的第三方的用户输入或指令而发起的触发事件。在另一个示例中，在设备重新引导102时施行的检查之后，BIOS 100可以接收触发事件103。例如，在重新引导时，作为设备运行时的问题(例如，检测到恶意软件)的结果而可能已经被存储的EC 105中的任何触发事件可以在设备101引导之前被传递到BIOS 100。也就是说，触发事件103可以包括在设备重新引导时执行或起作用的指令，以便迫使该设备进入BIOS配置状态。在图1的示例中，触发事件103可以在重新引导之后、但是在任何设备驱动

器已经被加载到系统存储器中之前，由BIOS 100接收。

[0013] 在示例中，BIOS 100可以下载109映像111，诸如来自映像管理器113的受信无盘引导映像，该映像管理器113可以以存储映像的远程储存库的形式，例如，基于云的企业存储位置。

[0014] 根据示例，可以使用BIOS内的代理108来下载映像111，该代理可以将映像111下载到以ram盘形式的存储器中(或者从本地存储装置检索它)，使得它然后可以引导。一旦下载到例如设备101的本地存储装置119，就可以检查映像111以确保其被签名。例如，还可以使用被配置到BIOS 100(或EC 105)中的信息来检查映像的版本信息。在示例中，可以使用代理108来施行这样的检查。其它基于BIOS的机制可以提供类似的过程来下载和引导受信无盘映像。

[0015] 在图1的示例中，BIOS 100形成由TPM 106使用设备身份密钥(PlatKeySign.Private)签名117的消息115。消息115是用于管理系统113的消息，该消息用于请求密钥，该密钥可以用于使能设备101的正常OS引导之外的服务。如上所述，脚本可以被自动化，该脚本可以在已知且受信的映像111(其可以是windows的无盘引导版本，诸如例如Windows PE或RE)内运行，以访问加密的设备101的本地存储装置，诸如例如通过诸如Bitlocker之类的机制的方式。因此，消息115提供了对可以用于访问设备101的加密本地存储装置119的(一个或多个)恢复密钥的请求。设备身份密钥(PlatKeySign.Private)将被标识为TPM的平台层次结构内的密钥，并且TPM可以用于对此进行验证。这确保了签名密钥可以在BIOS的控制下使用，并且因此对OS具有更高的信任度。

[0016] 因此，根据示例，在重新引导之后，设备101可以检查以查看它是否有理由引导到受信无盘映像111中，例如由于用户干预(107)，或者由于触发事件103。如果存在理由，则设备101可以从已经由例如企业管理系统配置的位置113下载映像111。在示例中，映像111可以是加密的映像，并且可以被预加密以确保例如攻击者不能容易地对其进行逆向工程。

[0017] 根据示例，消息117包括映像111的散列(例如，如果在下载映像111之后而不是同时施行消息生成)、随机数(其可以使用TPM 106生成)、设备的身份PlatKeySign.Pub和PlatKeyEnc.Pub。

[0018] TPM 106用设备身份或密码密钥(PlatKeySign.Private)对消息115进行签名117。在示例中，TPM 106可以对消息115进行散列化(hash)，因为该密钥是受限签名密钥。

[0019] 经签名的消息连同BIOS状态证明消息(例如，参考图1以BIOSSecurityConfig的形式记录BIOS 100的配置的相关经签名的信息)一起被发送121到密钥管理服务113。因此，BIOS 100联系密钥管理器服务113，以便获得供受信映像111使用的Bitlocker/(一个或多个)加密恢复密钥。

[0020] 根据示例，密钥管理器服务113检查(123)消息115的签名，并且针对设备101的已知PlatKeySign.Pub(身份)进行检查(作为从例如管理和BIOS状态证明记录获得的，或者作为设备ID)。如果包括映像111的散列，则密钥管理器服务113可以检查这是否与最新(可能加密的)映像的散列相匹配。密钥管理器服务还可以检查它是否之前从该设备尚未查看过随机数，因此防止请求的重放。

[0021] 密钥管理器服务113然后可以在数据库126中查找所请求的加密密钥，以使得能够访问设备101的本地存储装置119。替代地，用户可以(例如，经由使用QR码的智能设备)登录

网站,并且使用例如他们的授权企业域凭证来授权恢复密钥的释放。

[0022] 密钥管理器113形成包括所请求的加密密钥的消息125并对其进行签名。在示例中,密钥管理器113使用PlatKeyEnc.Pub密钥连同与映像111相关联的任何加密密钥对该密钥进行加密(例如,在其以加密形式的情况下对其进行解密)。如果PlatKeyEnc.pub密钥是预先注册的,则可以用每个设备的PlatKeyEnc.pub密钥为每个设备的加密恢复密钥进行加密。这可以使得密钥管理器不那么可攻击。如果采用这种方法,则可以使用注册阶段,其中PubKeyEnc.Pub密钥与BIOS状态证明数据一起传递。在示例中,这可以具有用PlatKeySign签名的认证,以表明该加密密钥是具有适当限制的TPM密钥。

[0023] 在示例中,密钥管理器113对来自请求121的加密有效载荷的散列连同随机数进行签名。密钥管理器113向BIOS 100返回127加密密钥(bitlocker恢复密钥和映像加密密钥)连同经签名的结构。可以在EC 105内开始131安全定时器,以设置密钥的最大寿命。在示例中,BIOS 100可以使用通过企业管理系统113提供并存储在EC 105内的公钥来检查该经签名的结构。BIOS 100还可以检查该经签名的结构中的随机数,以确保它与它在请求121中发送的随机数相匹配。

[0024] 假设TPM密钥与BIOS一起完成,则可以通过扩展用于密封密钥的PCR、或者通过将TPM平台层次结构的授权值重置为随机值来使密钥不可用。

[0025] BIOS可以解密该映像(如果它被加密的话)并且通过以下方式验证(133)该映像:

检查其散列与从密钥管理器113返回的消息中的任何散列是否相匹配,并且使用来自BIOS状态的公钥检查(与映像一起运送的)映像的签名。

[0026] BIOS 100引导135受信无盘映像。在示例中,该受信无盘映像可以包括OS,诸如WinPE或RE。因此,当被引导时,设备101运行受信OS。

[0027] 根据示例,BIOS 100在来自映像111的请求141之后,将恢复密钥连同关于为什么受信映像正在被引导的任何上下文信息139(从受信映像)传递(145)到运行的OS。例如,这可以通过来自OS的WMI请求或者经由UEFI变量来施行。使用恢复密钥,映像111安装147设备101的存储位置119。在示例中,映像111可以执行预定义的有效载荷149,该有效载荷149可以根据上下文信息而变化。例如,作为所安装的映像111的一部分执行的受信OS可以执行在从BIOS 100接收的上下文信息的基础上所选择的脚本。在示例中,上下文信息可以包括与反病毒扫描的结果有关的信息。

[0028] 在示例中,一旦被引导,映像可能已经被配置为不允许用户活动,而代替地执行脚本。在示例中,脚本可以通过WMI调用(或UEFI变量)从BIOS拾取任何上下文信息,以确定要采取的动作。

[0029] 根据示例,脚本可以使用WMI调用(或UEFI变量)从BIOS拾取加密恢复密钥。BIOS检查(143)自安全映像引导以来是否没有发生重新引导(或者如果发生了任何重新引导,则移除密钥)。如果EC定时器(131)已经开始,则它检查密钥应该仍然是可用的,并且没有超过(pass)任何基于时间的限制。

[0030] 在示例中,可以使用加密恢复密钥安装(147)存储装置119的主加密分区。在EC定时器超时之后,然后从存储器删除(144)加密密钥,以最小化任何暴露。该脚本按照企业的设置扫描、收集数据或收集取证信息149,并且一旦完成,映像111就关闭。在重新引导时,作为重新引导过程151的一部分,可以删除加密密钥和任何其它状态。

[0031] 图2是根据示例的用于访问设备的加密系统的密码恢复密钥的方法的流程图。在框201中,BIOS 100下载映像111,并且检查该映像是否被签名,以及使用配置到BIOS中的信息检查任何版本。在示例中,这可以经由用于下载恢复代理的机制来施行。例如,如上面所描述的,恢复代理可以被下载(或本地存储)并且以ram盘的形式被放入设备101的存储器中,使得它然后可以引导。在框203中,BIOS 100联系密钥管理器服务113,并且检索(一个或多个)加密恢复密钥(例如,(一个或多个)bitlocker密钥),以供下载的安全映像111使用。

[0032] 在框205中,BIOS 100引导受信无盘映像,使得它正在运行受信OS。在框207中,BIOS 100例如通过来自OS的WMI请求或经由UEFI变量将检索到的(一个或多个)恢复密钥连同关于为什么受信映像正在被引导的任何上下文信息(从受信映像)传递到运行的OS。在框209中,安全映像安装设备101的加密驱动器。例如,存储位置119可以是设备101的加密驱动器,或者可以包括加密部分,例如,它们中的任何一个都可以存储设备101的主OS。

[0033] 在框211中,安全映像运行可以根据上下文信息而变化的预定义有效载荷。在示例中,经由安全映像执行的受信OS可以用于执行脚本,该脚本可以使用来自BIOS 100的上下文信息来确定用于扫描和/或解决可能已经是发起安全引导过程的原因的问题的方法。在框213中,安全映像关闭。

[0034] 根据示例,由于设备101的受信状态预引导OS并且使用该状态来确保指定的(受信的)映像111被引导,该受信映像被提供有用于设备101的存储装置119的加密密钥,因此安全性得以维护。在示例中,受信无盘映像被锁定,因此当它能够访问设备的主磁盘(119)时,它运行意图的功能,并且不向用户或攻击者提供改变设备的接口。

[0035] 根据示例,通过在本地设备101上具有强身份来加固提供使能对设备101的存储位置119的访问。在示例中,这可以由TPM 106控制的并且在引导时可用的设备身份来提供。替代地,管理系统113可以(在平台层次结构内)具有基于TPM的公钥,该公钥可以被链接到TPM背书证书和/或随着时间的推移被跟踪。使用任一机制,管理系统113可以维护表示设备101的公钥,并且该公钥可以被用作管理系统的标识符。在示例中,该身份可以包括具有在TPM 106的平台层次结构内的私钥的公钥私钥对。在图1的示例中,该身份依据“PlatKey.Sign.Public”来指代。然而,这可以是与设备相关联并且在首次注册时向管理系统注册的密钥,或者它可以具有包括公钥和设备标识符并由平台供应商密钥签名的相关联的设备Id证书。

[0036] 在示例中,安全映像111的使用可以通过由企业管理系统、本地安全性代理创建的触发(107)来触发,或者经由在引导时使用功能键(例如F10或F11)的用户请求来触发。

[0037] 根据示例,设备101的密码身份可以在密钥管理服务113处注册。该身份可以与磁盘加密密钥相关联或映射到磁盘加密密钥,以便使得服务113能够将来自设备的针对磁盘加密密钥的请求与该设备的对应的磁盘加密密钥配对。在替代的示例中,设备公共加密密钥可以连同磁盘加密密钥一起存储,或者用于加密磁盘加密密钥。在POST(预引导- 102)期间,可以使相关联的私钥可用于设备,以使得其能够解密磁盘加密密钥。在另一个示例中,如果恢复密钥可以被安全地递送到BIOS,则加密的恢复密钥可以被保存在BIOS内以用于在这个阶段期间使用。

[0038] 在替代的示例中,可以首先请求加密密钥,并且可以提供访问令牌以允许访问映像。“请求加密密钥”消息仍然可以包含加密密钥和映像散列,以确保正在使用最新的映像。

访问令牌可以用于保护开放服务器上的映像。也就是说，映像111的下载在对密钥的请求之后继续进行，具有响应于该请求所提供的令牌以使得该映像能够被检索。也可能的是，如果在EC 105中存在身份密钥，则可以使用这些身份密钥来代替基于TPM的密钥。

[0039] 在示例中，硬件策略可以与加密密钥(127)一起返回，以指令BIOS 100例如锁定硬件设备(无线、蓝牙、USB、网络、键盘等等)。通过在这一级别禁用硬件，减小了安全映像的攻击面，以免攻击者试图使用它来获得例如加密密钥。

[0040] 在示例中，恢复密钥的本地TPM加密版本可以保存在设备101的BIOS或EC内，并且在POST(102)期间可访问。当引导适当的受信无盘映像时，BIOS可以对此进行解密。

[0041] 本公开中的示例可以作为方法、系统或机器可读指令——诸如软件、硬件、固件或诸如此类的任何组合——来提供。这样的机器可读指令可以被包括在其中或其上具有计算机可读程序代码的计算机可读存储介质(包括但不限于磁盘存储装置、CD-ROM、光学存储装置等)上。

[0042] 参考根据本公开的示例的方法、设备和系统的流程图和/或框图来描述本公开。尽管上面所描述的流程图示出了特定的执行次序，但是该执行次序可以与所描绘的不同。关于一个流程图描述的框可以与另一个流程图的框进行组合。在一些示例中，流程图的一些框可能不是必需的和/或可以添加附加的框。应当理解，流程图和/或框图中的每个流程和/或框、以及流程图和/或框图中的流程和/或图解的组合可以通过机器可读指令来实现。

[0043] 机器可读指令可以例如由通用计算机、专用计算机、嵌入式处理器或其它可编程数据处理设备的处理器来执行，以实现说明书和图解中描述的功能。特别地，处理器或处理装置可以执行机器可读指令。因此，装置的模块(例如，代理108)可以由执行存储在存储器中的机器可读指令的处理器、或者根据嵌入逻辑电路中的指令操作的处理器来实现。术语“处理器”要被宽泛地解释为包括CPU、处理单元、ASIC、逻辑单元或可编程门阵列等。方法和模块可以全部由单个处理器施行，或者可以在若干处理器当中划分。

[0044] 这样的机器可读指令也可以存储在计算机可读存储装置中，其可以指导计算机或其它可编程数据处理设备在特定模式下操作。

[0045] 例如，可以在编码有由处理器可执行的指令的非暂时性计算机可读存储介质上提供指令。

[0046] 图3是根据示例的密钥/映像管理器系统113(也称为管理服务)的示意性表示。系统113包括与存储器301相关联的处理器300。存储器301包括由处理器300可执行的计算机可读指令303。指令303可以包括指令，用于：将在密钥管理系统113处接收的设备(101)身份311映射到存储在密钥管理系统中(诸如例如存储在数据库126中)的恢复密钥309；为设备101生成经加密的消息(125)，该经加密的消息包括恢复密钥；以及将该经加密的消息和经签名的消息传输(127)到设备101。在示例中，处理器300可以响应于来自设备101的BIOS 100的请求121来执行指令303。

[0047] 这样的机器可读指令303也可以被加载到计算机或其它可编程数据处理设备上，使得计算机或其它可编程数据处理设备施行一系列操作以产生计算机实现的处理，因此在计算机或其它可编程设备上执行的指令提供了用于实现由图1和图2中的(一个或多个)框和/或流程图中的(一个或多个)流程所指定的功能的操作。

[0048] 另外，本文中的教导可以以计算机软件产品的形式实现，该计算机软件产品存储

在存储介质中，并且包括用于使计算机设备实现本公开的示例中所述的方法的多个指令。

[0049] 虽然已经参考某些示例描述了方法、装置和相关方面，但是在不脱离本公开的情况下，可以进行各种修改、改变、省略和替换。特别地，来自一个示例的特征或框可以与另一个示例的特征/框进行组合或被另一个示例的特征/框替换。

[0050] 词语“包括”不排除权利要求中列出的元件之外的元件的存在，“一”或“一个”不排除多个，并且单个处理器或其它单元可以实现权利要求中所述的若干单元的功能。

[0051] 任何从属权利要求的特征可以与任何独立权利要求或其它从属权利要求的特征进行组合。

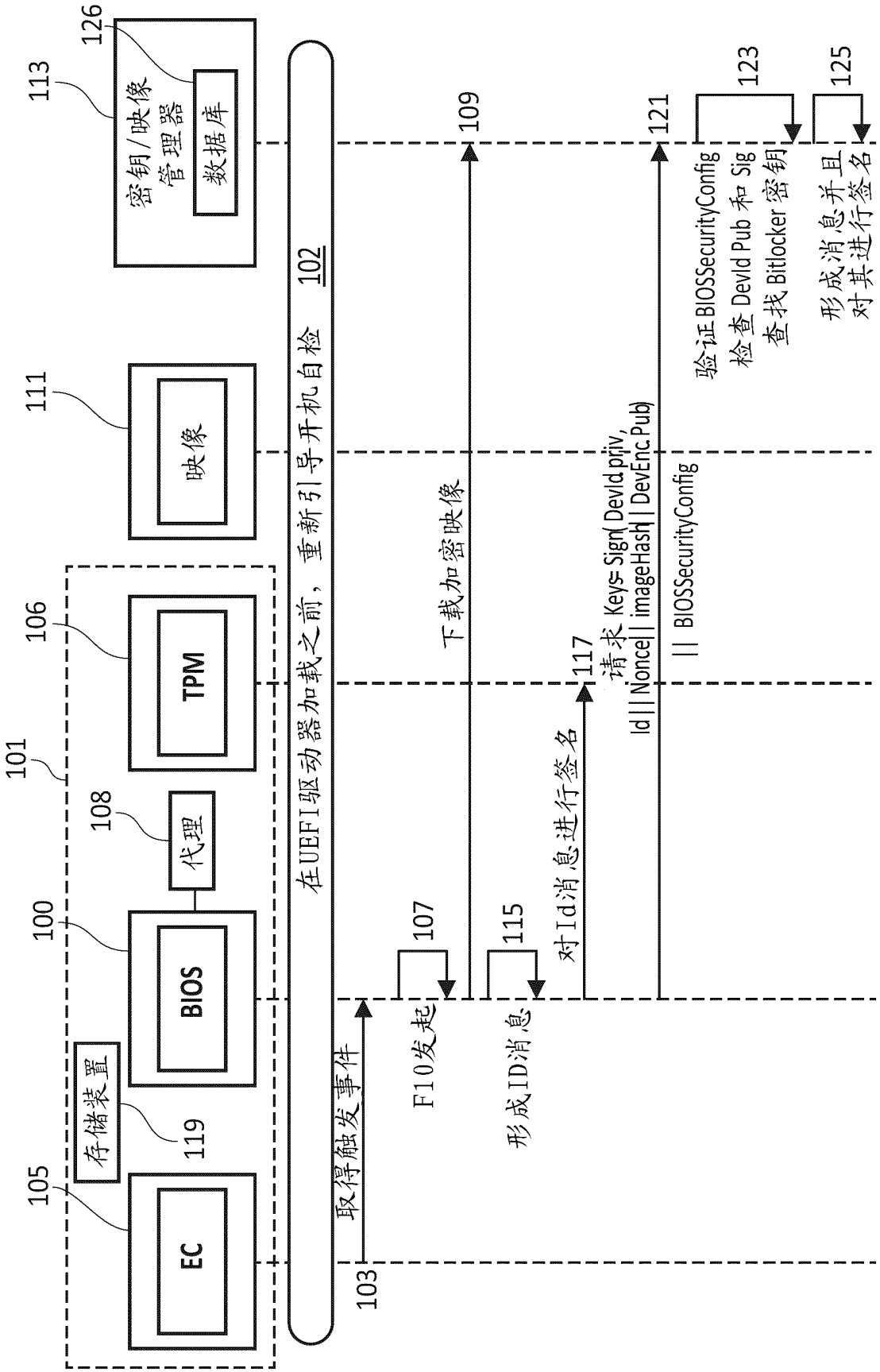

101
105
EC
存储装置
119
100
BIOS
108
代理
106
TPM
111
映像
113
126
密钥/映像管理器
数据库
102
在UEFI驱动器加载之前，重新引导开机自检
103
取得触发事件
107
F10发起
115
形成ID消息
117
对Id消息进行签名
109
下载加密映像
121
请求 Keys= Sign(DevId priv, Id||Nonce||imageHash||DevEnc Pub)
|| BIOSSecurityConfig
123
验证BIOSSecurityConfig
检查 DevId Pub 和 Sig
查找 Bitlocker 密钥
125
形成消息并且
对其进行签名

图 1

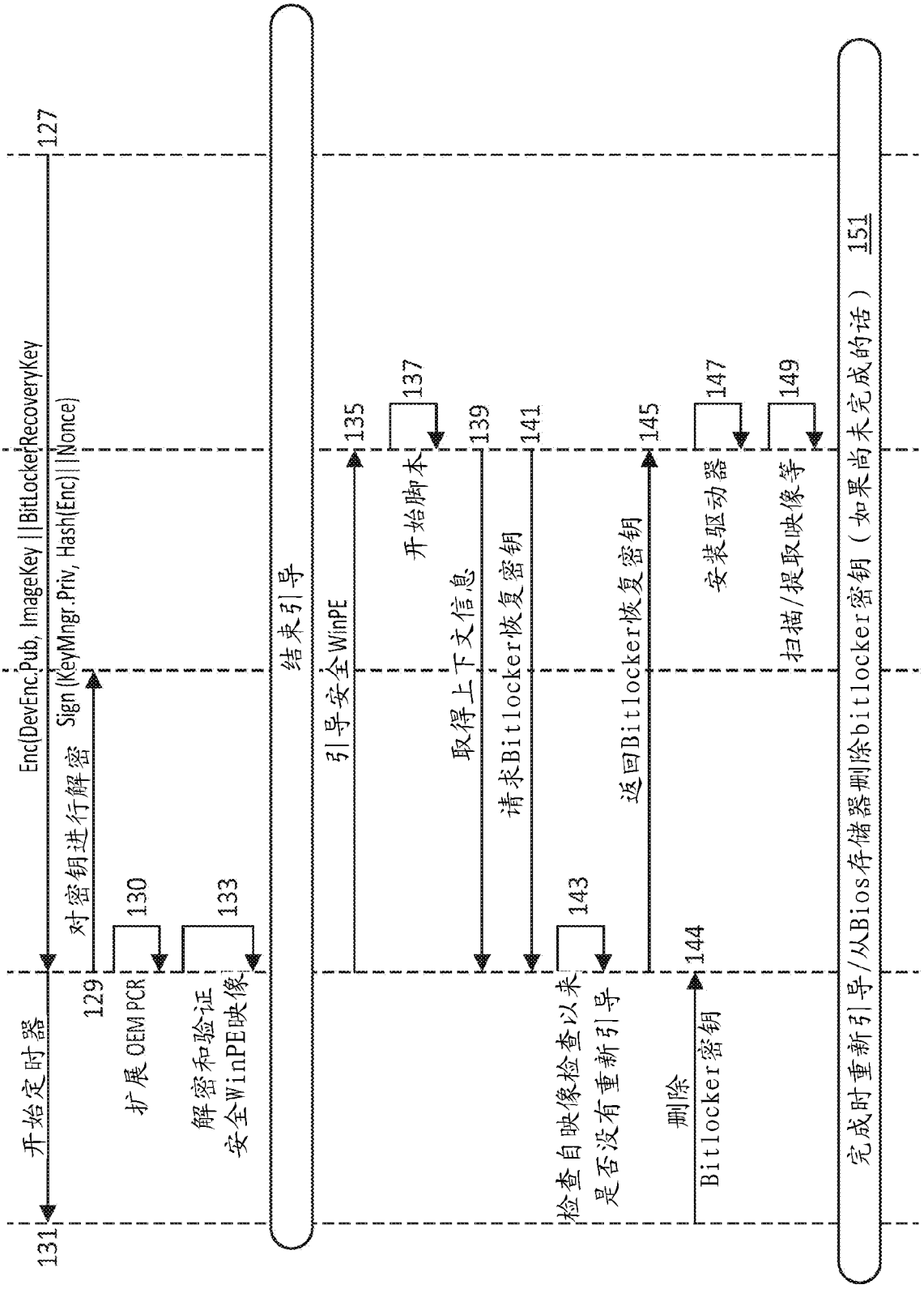

开始定时器
131
Enc(DevEnc.Pub, ImageKey ||BitLockerRecoveryKey
127
对密钥进行解密
Sign (KeyMngr.Priv, Hash(Enc)||Nonce)
129
扩展 OEM PCR
130
解密和验证
安全WinPE映像
133
结束引导
引导安全 WinPE
135
开始脚本
137
取得上下文信息
139
请求Bitlocker恢复密钥
141
检查自映像检查以来
是否没有重新引导
143
返回Bitlocker恢复密钥
145
删除
Bitlocker密钥
144
安装驱动器
147
扫描/提取映像等
149
完成时重新引导/从Bios存储器删除bitlocker密钥（如果尚未完成的话）
151

图 1(续)

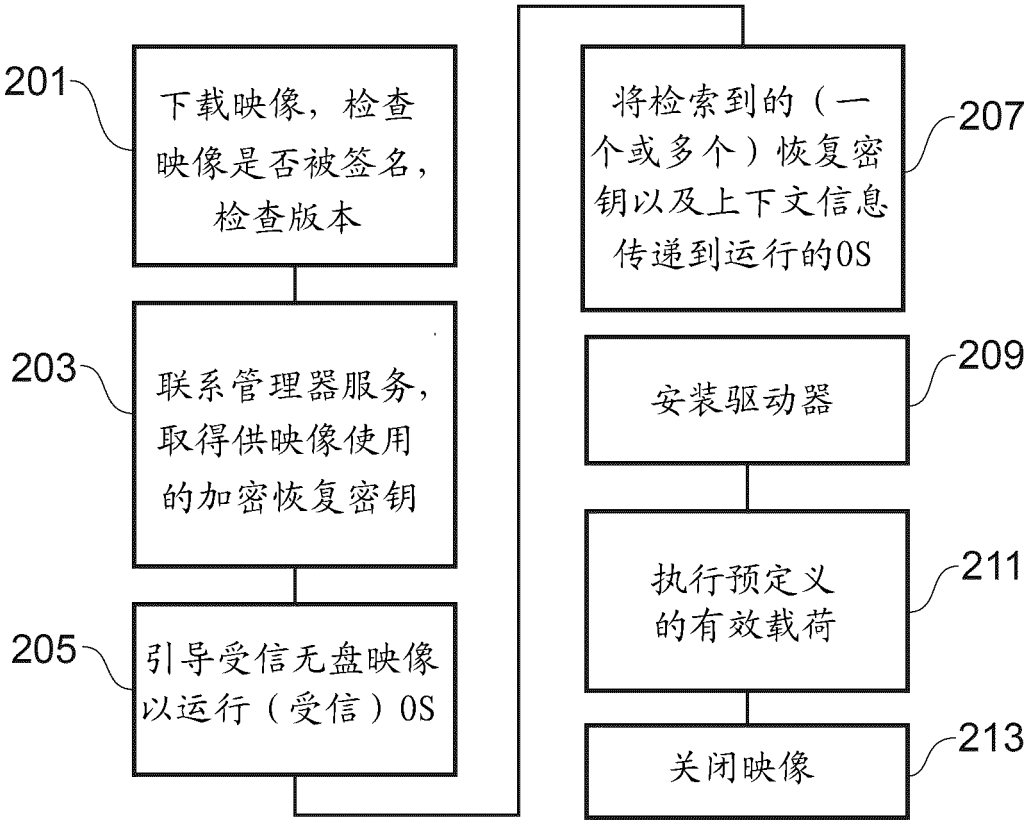

201
下载映像，检查映像是否被签名，检查版本
203
联系管理器服务，取得供映像使用的加密恢复密钥
205
引导受信无盘映像以运行（受信）OS
207
将检索到的（一个或多个）恢复密钥以及上下文信息传递到运行的OS
209
安装驱动器
211
执行预定义的有效载荷
213
关闭映像

图 2

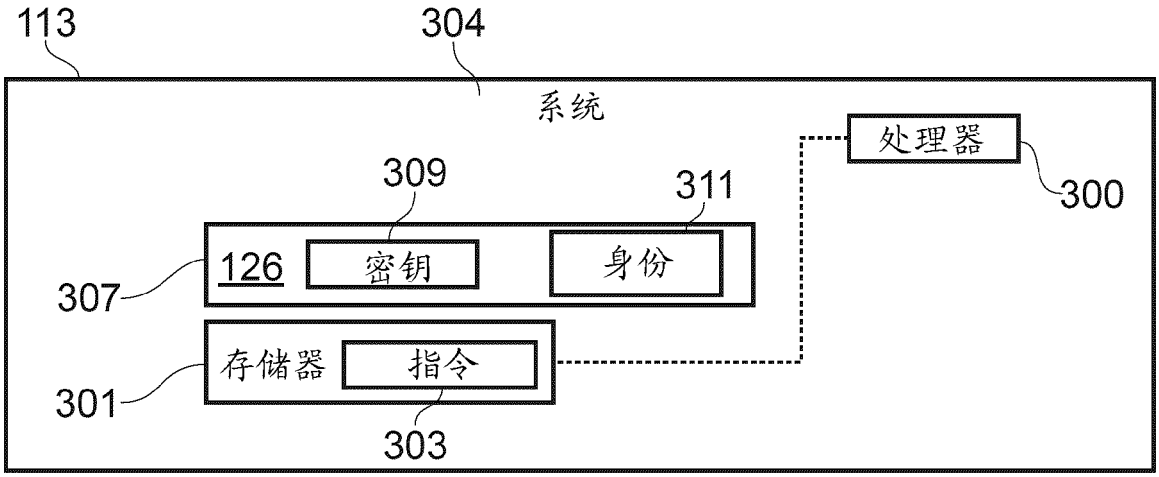

113
304
系统
处理器
300
309
311
126
密钥
身份
307
存储器
指令
301
303

图 3