(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 105493044 B
(45)授权公告日 2019.10.11

(21)申请号 201480047844.X
(22)申请日 2014.07.01
(65)同一申请的已公布的文献号
申请公布号 CN 105493044 A
(43)申请公布日 2016.04.13
(30)优先权数据
14/025,556 2013.09.12 US
(85)PCT国际申请进入国家阶段日
2016.02.29
(86)PCT国际申请的申请数据
PCT/US2014/045017 2014.07.01
(87)PCT国际申请的公布数据
WO2015/038219 EN 2015.03.19
(73)专利权人 波音公司
地址 美国伊利诺斯州
(72)发明人 A·J·斯特恩 J·哈利
(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 吕俊刚
(51)Int.Cl.
G06F 9/455(2006.01)
(56)对比文件
CN 101960464 A,2011.01.26,
CN 101122937 A,2008.02.13,
US 2006230439 A1,2006.10.12,
US 2006230439 A1,2006.10.12,
JP 2009169841 A,2009.07.30,
审查员 杨黎鹏

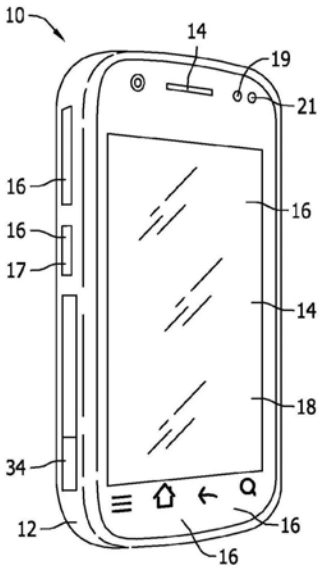
权利要求书2页 说明书14页 附图9页

(54)发明名称

移动通信装置及其操作方法

(57)摘要

移动通信装置及其操作方法。提供了一种移动通信装置。所述移动通信装置包括:第一可信平台模块、第二可信平台模块、处理器以及存储介质。所述存储介质包括这样的指令,这些指令致使所述处理器建立针对第一角色的信任根和针对第二角色的信任根,其中,所述第一角色包括第一操作系统和第一可信执行环境,而所述第二角色包括第二操作系统和第二可信执行环境。所述指令还致使所述处理器在所述第一可信平台模块中存储限定针对所述第一角色的信任根的测量,在所述第二可信平台模块中存储限定针对所述第二角色的信任根的测量,以及利用针对所述第一角色的信任根和针对所述第二角色的信任根,来加载所述第一角色和所述第二角色。



CN 105493044 B

1.一种移动通信装置,该移动通信装置包括:

第一可信平台模块(60);

第二可信平台模块(62);

处理器(24);以及

存储介质(22),该存储介质(22)包括这样的指令,这些指令致使所述处理器(24)进行如下操作:

建立针对第一角色(110)的第一信任根,所述第一角色(110)包括第一操作系统(112)和第一可信执行环境(114);

建立针对第二角色(120)的第二信任根,所述第二角色(120)包括第二操作系统(122)和第二可信执行环境(124),其中,所述第一信任根与所述第二信任根分离;

在所述第一可信平台模块(60)中存储限定针对所述第一角色(110)的所述第一信任根的测量;

在所述第二可信平台模块(62)中存储限定针对所述第二角色(120)的所述第二信任根的测量;

利用针对所述第一角色的所述第一信任根和针对所述第二角色的所述第二信任根,来加载所述第一角色(110)和所述第二角色(120);以及

在所述第一可信执行环境(114)与所述第二可信执行环境(124)之间建立互信,使得所述第一角色(110)与所述第二角色(120)通信联接。

2.根据权利要求1所述的移动通信装置,所述移动通信装置还包括:高安全防护,当所述第一角色(110)与所述第二角色通信联接时,该高安全防护易于限制在所述第一角色(110)与所述第二角色(120)之间的数据传递。

3.根据权利要求1所述的移动通信装置,其中,所述存储介质(22)还包括这样的指令,这些指令致使所述处理器(24)在已经加载所述第一角色和所述第二角色之后,将所述第一可信平台模块(60)的控制传递至所述第一角色(110),而将所述第二可信平台模块(62)的控制传递至所述第二角色(120)。

4.根据权利要求3所述的移动通信装置,其中,所述第一可信执行环境(114)独占地接入第一可信平台模块(60),而所述第二可信执行环境(124)独占地接入第二可信平台模块(62)。

5.根据权利要求1所述的移动通信装置,其中,所述存储介质(22)还包括这样的指令,这些指令致使所述处理器(24)在加载期间针对关联的用于所述第一角色的所述第一信任根和关联的用于所述第二角色(120)的所述第二信任根,来验证所述第一操作系统(112)的映像和所述第二操作系统(122)的映像。

6.根据权利要求1所述的移动通信装置,其中,所述存储介质(22)还包括这样的指令,这些指令致使所述处理器(24)在彼此隔离的情况下执行所述第一角色(110)和所述第二角色(120)。

7.一种操作移动通信装置(10)的方法,该方法包括以下步骤:

建立针对第一角色(110)的第一信任根,所述第一角色(110)包括第一操作系统(112)和第一可信执行环境(114);

建立针对第二角色(120)的第二信任根,所述第二角色(120)包括第二操作系统(122)

和第二可信执行环境(124),其中,所述第一信任根与所述第二信任根分离;

在第一可信平台模块(60)中存储限定针对所述第一角色(110)的所述第一信任根的测量;

在第二可信平台模块(62)中存储限定针对所述第二角色(120)的所述第二信任根的测量;

利用针对所述第一角色的所述第一信任根和针对所述第二角色的所述第二信任根,来加载所述第一角色(110)和所述第二角色(120);以及

在所述第一可信执行环境(114)与所述第二可信执行环境(124)之间建立互信,使得所述第一角色(110)与所述第二角色(120)通信联接。

8.根据权利要求7所述的方法,其中,加载所述第一角色(110)和所述第二角色(120)的步骤包括以下步骤:利用通过装置制造方信任根签名的引导加载器(144)来加载基础操作系统。

9.根据权利要求7所述的方法,其中,建立针对所述第一角色(110)的所述第一信任根和针对所述第二角色(120)的所述第二信任根的步骤包括以下步骤:在加载期间,针对用于所述第一角色(110)的所述第一信任根和用于所述第二角色(120)的所述第二信任根,验证所述第一操作系统(112)的映像和所述第二操作系统(122)的映像。

10.根据权利要求7所述的方法,所述方法还包括以下步骤:在已经加载所述第一角色和所述第二角色之后,将所述第一可信平台模块(60)的控制传递至所述第一角色(110),而将所述第二可信平台模块(62)的控制传递至所述第二角色(120)。

11.根据权利要求7所述的方法,其中,建立针对所述第一角色的所述第一信任根和所述第二角色的所述第二信任根的步骤包括以下步骤:

测量用于建立所述第一角色(110)的所述第一信任根和所述第二角色(120)的所述第二信任根的软件组件;以及

将所述测量扩展到所述第一可信平台模块(60)和所述第二可信平台模块(62)中,其中,将针对第一信任锚的测量扩展到所述第一可信平台模块(60)中,而将针对第二信任锚的测量扩展到所述第二可信平台模块(62)中。

12.根据权利要求7所述的方法,所述方法还包括以下步骤:

限定针对所述第一角色(110)的安全策略和针对所述第二角色(120)的安全策略,其中,所述安全策略限定所述第一角色(110)和所述第二角色(120)怎样接入所述移动通信装置(10)上的物理装置;以及

利用安全监管程序(108)实施所述安全策略。

13.根据权利要求12所述的方法,其中,实施所述安全策略的步骤包括以下步骤中的至少一个:

针对所述第一角色(110)和所述第二角色(120)中的一个建立针对所述物理装置中的至少一个的独占接入;

在所述第一角色(110)与所述第二角色(120)之间建立针对所述物理装置中的至少一个的共享接入;以及

拒绝将所述物理装置中的至少一个接入所述第一角色(110)和所述第二角色(120)中的一个。

移动通信装置及其操作方法

技术领域

[0001] 本公开的领域总体上涉及移动通信装置，并且更具体地说，涉及这样的移动通信装置，即，该移动通信装置使能实现其上运行的一个或更多个隔离的虚拟化操作系统的可信操作。

背景技术

[0002] 诸如智能电话、蜂窝电话以及个人数字助理(PDA)这样的移动通信装置就用途和流行性而言在多种不同类型用户当中已经日益增长。至少一些已知装置包括中央处理单元(CPU)，其可以被虚拟化成在一个装置上同时执行多个操作系统(OS)。例如，已知为管理程序(hypervisor)的软件程序可以被用于通过管理在OS与被包括在计算机系统中的硬件装置之间传送的/输出(I/O)存取操作来分离不同的OS。更具体地说，该管理程序易于分离诸如CPU这样的底层硬件和关联外围设备(例如，显示装置、触摸屏，以及通信接口)与在硬件上运行的OS。

[0003] 虽然装置虚拟化可以易于分离已知计算装置上的一组软件与另一组软件，但该底层平台可能易受多种安全攻击。因此，对于计算机工业方面的那些来说，已经变得日益重要的是，增加已知计算装置的安全性。同样地，可以希望的是，将增强安全并入到装置虚拟化架构中。

发明内容

[0004] 在一个方面，提供了一种移动通信装置。所述移动通信装置包括：第一可信平台模块、第二可信平台模块、处理器，以及存储介质。所述存储介质包括这样的指令，这些指令致使所述处理器进行如下操作：建立针对第一角色和第二角色的信任根，其中，所述第一角色包括第一操作系统和第一可信执行环境，而所述第二角色包括第二操作系统和第二可信执行环境。所述指令还致使所述处理器在所述第一可信平台模块中存储限定针对所述第一角色的所述信任根的测量，在所述第二可信平台模块中存储限定针对所述第二角色的所述信任根的测量，以及利用针对所述第一角色的所述信任根和针对所述第二角色的所述信任根，来加载所述第一角色和所述第二角色。

[0005] 在另一方面，提供了一种操作移动通信装置的方法。该方法包括以下步骤：建立针对第一角色的信任根和针对第二角色的信任根，其中，所述第一角色包括第一操作系统和第一可信执行环境，而所述第二角色包括第二操作系统和第二可信执行环境。在该方法还包括以下步骤：在所述第一可信平台模块中存储限定针对所述第一角色的所述信任根的测量，在所述第二可信平台模块中存储限定针对所述第二角色的所述信任根的测量，以及利用针对所述第一角色的所述信任根和针对所述第二角色的所述信任根，来加载所述第一角色和所述第二角色。

[0006] 在又一方面，提供了一种存储用于操作移动通信装置的计算机可执行指令的非暂时计算机可读介质。所述移动通信装置包括：处理器、第一可信平台模块、以及第二可信平

台模块。该计算机可执行指令，致使所述处理器建立针对第一角色的信任根和针对第二角色的信任根，其中，所述第一角色包括第一操作系统和第一可信执行环境，而所述第二角色包括第二操作系统和第二可信执行环境。在该计算机可执行指令还致使所述处理器在所述第一可信平台模块中存储限定针对所述第一角色的所述信任根的测量，在所述第二可信平台模块中存储限定针对所述第二角色的所述信任根的测量，以及利用针对所述第一角色的所述信任根和针对所述第二角色的所述信任根，来加载所述第一角色和所述第二角色。

附图说明

[0007] 图1是示例性移动通信装置的正立体图。

[0008] 图2是图1所示的移动通信装置的后立体图。

[0009] 图3是可以与图1所示的移动通信装置一起使用的示例性硬件架构的示意性例示图。

[0010] 图4是可以与图1所示的移动通信装置一起使用的示例性软件架构的示意性例示图。

[0011] 图5是可以与图1所示移动通信装置一起使用的、要求角色的所有权的示例性方法的流程图。

[0012] 图6是供在授权要在图1所示的移动通信装置上执行的操作中使用的示例性系统的示意性例示图。

[0013] 图7是可以与图1所示的移动通信装置一起使用的、更新角色软件的示例性方法的流程图。

[0014] 图8是可以与图1所示的移动通信装置一起使用的、转变角色的所有权的示例性方法的流程图。

[0015] 图9是可以与图1所示的移动通信装置一起使用的、加载新角色的示例性方法的流程图。

具体实施方式

[0016] 在此描述的系统和方法可以被用于操作移动通信装置。在该示例性实现中，移动通信装置通过使用诸如基于公钥和私钥的密码这样的密码的硬件和软件架构来管理，以易于保护在其上运行的操作系统。更具体地说，该移动通信装置支持同时在该装置上运行并且皆具有分离信任根(roots of trust)的多个虚拟化操作系统。同样地，该虚拟化操作系统针对装置上的硬件的接入通过预定安全策略来实施，以使能实现对该装置的可信操作。

[0017] 图1和2例示了示例性移动通信装置10。在该示例性实现中，移动通信装置10被设置用于支持与诸如另一移动通信装置这样的另一装置的话音通信。而且，移动通信装置10可以包括多种其它功能，包括网络接入、SMS消息、主机化一个或更多个应用、数据处理、加密、和/或其它功能。移动通信装置10可以是被配置成通过一个或更多个蜂窝网络通信的智能电话。在另选实现中，移动通信装置10可以在诸如WiFi和/或卫星网络的非蜂窝网络上独占地操作。

[0018] 如所示，移动通信装置10包括外壳12和至少部分地设置在外壳12内的多个呈现装置14。呈现装置14向用户输出信息，诸如但不限于：与移动通信装置10的操作有关的数据、

命令、请求的数据、消息、一个或更多个输入装置(如虚拟键盘)、和/或任何其它类型的数据。在几个示例中,呈现装置14例如可以包括:液晶显示装置(LCD)、发光二极管(LED)显示器、发光二极管(LED)、摄像机闪光灯、有机LED(OLED)显示器、和/或“电子墨水”显示器。在一些实现中,可以包括多个呈现装置14,以可视地和/或可听地向用户呈现数据。在该示例性实现中,呈现装置14包括供在话音通信中使用的音频输出。

[0019] 移动通信装置10还包括至少部分地设置在外壳12内的多个输入装置16。根据在此描述的方法和/或处理中的一个或更多个,每一个输入装置16可以被配置成接收选择、请求、命令、信息、数据和/或其它类型的输入。输入装置16例如可以包括:按钮、键盘、麦克风、vibe、点击装置、输入笔(stylus)、触敏板(例如,触摸板或触摸屏)、陀螺仪、加速度计、数字罗盘、位置检测器、摄像机、第二摄像机、环境光传感器和/或音频输入接口。在该示例性实现中,诸如触摸屏这样的单一组件充任呈现装置14和输入装置16两者。

[0020] 在一个实现中,移动通信装置10包括易于移动通信装置10的安全操作的安全特征。安全特征包括:诸如安全按钮17这样的输入装置16,和诸如多个LED这样的呈现装置14。更具体地说,移动通信装置10包括第一LED 19和第二LED 21。如下更详细描述的,该安全特征可以用于改变和/或验证移动通信装置10的可操作可信状态。在另选实现中,移动通信装置10可以包括使得该安全特征能够如在此所述起作用的任何类型和/或数量的呈现装置。

[0021] 移动通信装置10包括与外壳12接合的背板20。背板20限定与外壳12大致一致的截面,由此,在接合至外壳12时与外壳12形成大致整体单元。可从移动通信装置10去除背板20,以提供针对移动通信装置10的一个或更多个方面的接入。

[0022] 图3是可以与移动通信装置10(图1所示)一起使用的示例性硬件架构的示意性例示图。在该示例性实现中,移动通信装置10包括:存储器22和处理器24,处理器24联接至存储器22用于执行编程指令。处理器24可以包括一个或更多个处理单元(例如,采用多核构造)和/或包括加密加速器(未示出)。移动通信装置10可编程成,通过编程存储器22和/或处理器24来执行在此描述的一个或更多个操作。例如,可以通过将一操作编码为可执行指令并将该可执行指令设置在存储器22中来对处理器24编程。

[0023] 处理器24可以包括,但不限于:通用中央处理单元(CPU)、微控制器、精简指令集计算机(RISC)处理器、开放式媒体应用平台(OMAP)、专用集成电路(ASIC)、可编程逻辑电路(PLC),和/或能够执行在此描述的功能的任何其它电路或处理器。在此描述的方法可以被编码为可执行指令,该可执行指令在计算机可读介质中具体实施,包括而不限于,存储装置和/或其它存储器装置。这种指令在通过处理器24执行时,使该处理器24执行在此描述的功能的至少一部分。上面的示例仅仅是示例性的,并由此不是旨在以任何方式限制术语处理器的定义和/或含义。

[0024] 如在此所述,存储器22是使能存储和检索诸如可执行指令和/或其它数据这样的信息的一个或更多个装置。存储器22可以包括一个或更多个计算机可读介质,如而不限于,动态随机存取存储器(DRAM)、同步动态随机存取存储器(SDRAM)、静态随机存取存储器(SRAM)、固态磁盘和/或硬盘。存储器22可以被设置成存储,而不限于,可执行指令,操作系统、应用、资源、安装脚本和/或适于与在此描述的方法和系统一起使用的任何其它类型的数据。

[0025] 用于操作系统和应用的指令按功能形式定位在非暂时存储器22上,以便由处理器

24执行以执行一个或更多个在此描述的处理。不同实现中的这些指令可以被具体实施在不同物理或有形计算机可读介质上，如存储器22或另一存储器(如计算机可读介质26)，其可以包括而不限于：闪速驱动器和/或拇指驱动器。而且，将指令按功能形式定位非暂时计算机可读介质26上，非暂时计算机可读介质26可以包括而不限于：智能介质型(SM)存储器、紧凑闪速型(CF)存储器、安全数字型(SD)存储器、存储器棒型(MS)存储器、多媒体卡型(MMC)存储器、嵌入式多媒体(e-MMC)、以及微驱动器型存储器。计算机可读介质26可以选择性地插入移动通信装置10和/或从其去除，以准许通过处理器24存取和/或执行。在一些实现中，计算机可读介质26不可去除。

[0026] 再次参照图3，移动通信装置10可以包括GPS组件30，GPS组件30被配置成向处理器24提供位置数据。该位置数据准许处理器24确定移动通信装置10的位置，和/或提供根据移动通信装置10的位置的功能(举例来说，如导航功能)。在另选实现中，可以通过标识附近的802.11和/或蓝牙基站或装置，和/或其组合，来获取用于利用蜂窝网络的移动通信装置10的位置数据。

[0027] 在一些实现中，移动通信装置10还包括至少一个加密处理器。更具体地说，移动通信装置10包括第一可信平台模块(TPM)60和第二TPM 62。该TPM加密通过处理器24存取的至少一部分数据，以向/从移动通信装置10传送和/或存储在其中。因此，一些数据可以与移动通信装置10的其它应用和/或操作隔离，并且保持比这种应用/操作更高的安全级别。同样地，TPM 60和TPM 62例如易于使能实现可信引导、测量引导、安全引导、远程认证、以及保护密钥库。

[0028] 而且，移动通信装置包括联接至处理器24的安全部件64。更具体地说，安全部件64可以与移动通信装置10集成作为通用集成电路卡(UICC)、微型SD卡中的至少一个，和/或嵌入移动通信装置10内。安全部件64是一种防篡改、存储以及执行环境，其可以被用作密钥库装置，和/或用于运行在移动通信装置10上的平台的硬件信任锚(hardware trust anchor)。更具体地说，安全部件64存储数据加密密钥、密码以及硬件和软件配置信息。而且，安全部件64生成公钥对，并且易于限制输出关联私钥。在另选实现中，安全部件64可以利用TPM来实现。

[0029] 移动通信装置10还包括安全监管程序存储器66。安全监管程序存储器66存储篡改反应数据，其可以包括多个密钥，并且可以用于掩蔽(wrap)安全部件64和/或第一TPM 60或第二TPM62内的数据。在操作中，该篡改反应数据可以被清除，以使所掩蔽的数据在检测到篡改事件时不能被恢复。安全监管程序存储器66可以保持任何量的篡改反应数据，其使得移动通信装置10能够如在此所述起作用。

[0030] 移动通信装置10还包括联接至处理器24的蜂窝控制器31。蜂窝控制器31准许移动通信装置10与一个或更多个蜂窝网络(未示出)通信，以提供与蜂窝网络的话音和/或数据通信。在该实施例中，移动通信装置10包括联接至蜂窝控制器31的两个用户标识模块(SIM)卡插槽33A和33B。按这种方式，移动通信装置10能够接纳可通过移动通信装置10的用户选择的、与两个不同蜂窝账户相关联的两个SIM卡。例如，移动通信装置10可以接入个人蜂窝账户和商业蜂窝账户，允许用户在个人蜂窝账户和商业蜂窝账户之间选择，以分开个人用途和商业用途。应当清楚，在其它实现可以包括不同数量的SIM卡插槽。

[0031] 而且，移动通信装置10包括联接至处理器24的USB控制器35。如图3所示，USB控制

器35可通过连接器37接入。按这种方式，一个或更多个不同装置可以与移动通信装置10的通信。类似的是，移动通信装置10还包括联接至处理器24并且可通过连接器41接入的高清多媒体接口(HDMI)控制器39。在至少一个实现中，连接器37和/或41可以向移动通信装置10提供微型USB和/或微型HDMI连接。

[0032] 另外或另选的是，移动通信装置10可以包括蓝牙控制器、ZigBee控制器和/或Wi-Fi控制器中的一个或更多个，以提供一个或更多个无线通信信道。虽然GPS组件30、第一TPM 60、第二TPM 62以及蜂窝控制器31被至少部分地按硬件设置，但还应清楚，集成到移动通信装置10中的一个或更多个组件可以通过与处理器24相关联的软件和/或固件来提供。在一个实施例中，处理器24提供被配置成分析移动通信装置10的低级空气接口协议的空气接口防火墙，并且基于核准的网络标识和特征来准许或拒绝网络发送。在该实施例中，来自包含蜂窝网络标识和特征的蜂窝控制器31的空气接口协议数据被提供给处理器24，并且通过处理器24来分析，以确定移动通信装置10是否应当被准许经由通过蜂窝控制器31标识的蜂窝网络来进行网络发送。在这个实施例中，在本身利用蜂窝控制器31的标准蜂窝网络协议认证机制之后，通过使处理器24还认证蜂窝控制器31的网络连接，所提供的分析水平将网络安全添加至移动通信装置10。应注意到，移动通信装置10的其它空气接口组件(举例来说，如蓝牙控制器和/或Wi-Fi控制器)还可以通过空气接口防火墙来监测。在另选实现中，第一TPM 60和第二TPM 62可以按软件来实现。

[0033] 应当清楚，其它移动通信装置实现可以包括与处理器24集成的或者在处理器24外部的更多或更少组件。

[0034] 图4是可以与移动通信装置10(图1所示)一起使用的、示例性软件架构100的示意性例示图。在该示例性实现中，软件架构100包括安装在包括处理器24和存储器22的硬件平台102上的操作系统104。硬件平台102包括上述移动通信装置10的组件。软件架构100还包括运行在操作系统104之上的诸如管理程序106的虚拟化软件层(即，类型2管理程序)，和与管理程序106通信联接的安全监管程序108。在另选实现中，管理程序106可以安装在硬件平台102上并操作(即，类型1管理程序)。管理程序106支持多个虚拟机执行空间，以使多个虚拟机可以同时实例化并执行。

[0035] 管理程序106虚拟化可以在管理程序106之上执行并运行的第一角色110和第二角色120。第一角色110包括第一角色操作系统(OS)112和第一可信执行环境(TEE)114，而第二角色120包括第二角色操作系统122和第二可信执行环境124。

[0036] 第一角色110和第二角色120皆具有限定信任锚(trust anchor)，该限定信任锚可以用于验证信任，并且授权通过每一个角色执行的动作。更具体地说，第一角色110具有第一信任锚，而第二角色120具有与第一信任锚分离的第二信任锚。如在此使用的，术语“信任锚”指限定可以用于签名(sign)角色资产的角色拥有者的一个或更多个机密加密密钥(即，加密证书)。相反的是，如在此使用的，术语“拥有者”和/或“所有权”指通过保持信任锚而具有针对角色的管理控制的个人或实体。在一些实现中，该信任锚根证书可以用于对中间证书授权签名，其对角色包的资产进行签名。

[0037] 每一个信任锚追溯根证书授权，其可以是企业或组织和/或可以针对台式计算机上的单一用户按轻量级方式来限定。同样地，第一角色110的资源可以保持与第二角色120分离，并且可以实施已经通过每一个信任锚同意并且签名的接入策略。根证书授权可以离

线存储并存储在安全位置中。而且，信任锚可以包括具有具体定义能力的多个中间证书授权。示例性能力包括，但不限于：用于定义操作系统的权利、用于定义TEE的权利、用于定义安全策略的权利、用于定义其它中间证书授权和/或用户证书的权利、备份能力、备份策略、用于更新操作系统的能力、用于更新TEE的能力、移动装置管理(MDM)功能、以及密钥输入和/或输出。

[0038] 第一角色110和第二角色120的可信软件皆在与其它默认条件下隔离的背景下运行。更具体地说，如上所述，管理程序106易于彼此分离并隔离第一TEE 114和第二TEE 124。同样地，每一个角色不会受运行在移动通信装置10上的其它操作系统所影响。而且，第一角色110和第二角色120可以被配置成建立第一TEE 114与第二TEE124之间的相互信任。建立这种相互信任使能实现形成在第一角色110与第二角色120的可信通信路径。第一TEE 114与第二TEE 124之间的通信可以仅通过第一角色110和第二角色120的安全策略中的相互同意来允许。而且，可以实现高可信防护(未示出)，以易于限制第一角色110与第二角色120之间的数据流。例如，高安全防护(high assurance guard)可以易于限制第一角色110与第二角色120之间的敏感和/或分类数据流，同时允许第一角色110与第二角色120之间的未分类数据流。

[0039] 虽然第一角色110及其部件将在下面加以更详细描述，但应当明白，同一描述可以应用至第二角色120及其部件。在该示例性实现中，第一角色OS 112是具有使能够运行完整操作系统的资源和虚拟设备驱动器的执行环境。示例性完整操作系统可以包括，但不限于：Android®开源项目(AOSP)操作系统。第一角色OS 112可以包括使得第一角色OS 112能够与第一TEE 114通信的库。而且，多个应用130可以从外部源(未示出)获取并且在第一角色OS 112之上运行。

[0040] 第一TEE 114是与第一角色OS 112分离并且以通信方式联接的轻量级执行环境。第一TEE 114是提供可以用于存储敏感数据和运行敏感应用的区域的安全环境。在另选实现中，第一TEE 114可以是具有使能运行完整操作系统和/或可以运行在分离硬件上的资源和虚拟设备驱动器的执行环境。而且，第一角色110可以包括一个以上的可信执行环境。

[0041] 第一TEE 114直接接入ISO7816用户标识模块(SIM)接口和/或TPM。更具体地说，第一TPM 60(图3所示)被指配给第一角色110，而第二TPM 62(图3所示)被指配给第二角色120。同样地，第一TPM 60可以用作针对第一角色110的拥有者的硬件信任锚，而第二TPM 62可以用作针对第二角色120的拥有者的硬件信任锚。而且，第一TEE 114直接接入第一TPM 60并且直接接入可信执行环境服务，举例来说，如认证、密钥库存取、虚拟私人网络(VPN)配置、和/或因特网话音传输协议(VoIP)软件。隔离第一TEE 114内的这种敏感数据路径并且远离第一角色OS 112易于确保移动通信装置10的可信操作，同时利用角色拥有者保持对TEE服务的控制。而且，允许第一TEE 114控制第一TPM 60易于隔离敏感信息与第一角色OS 112，使得该信息处于更安全且受保护环境中。

[0042] 而且，第一TEE 114可以使用加密服务，以使可以代表第一角色OS 112来执行加密操作，而不将其暴露至明文密钥。更具体地说，第一TEE 114可以使用第一TPM60中的加密模块，其使能实现未经证明的硬件加速加密、套件B、以及FIPS-140-2证明的加密。移动通信装置10还可以包括VPN模块和/或VoIP模块。该VPN模块使得第一角色110能够认证VPN并且利用来加密通信，而不需要认证或加密密钥可见于不可信代码。另外，该VoIP模块使得第一角

色110能够建立并认证VoIP呼叫，并且利用加密来通信，而不需要认证或加密密钥可见于不可信代码。

[0043] 第一角色OS 112和第二角色OS 122的信任根据通过平台硬件102加载的每一个角色的引导映像的完整性来限定。例如，第一TEE 114的信任根据在通过平台硬件102加载时其静态映像的完整性来限定，如下更更详细描述。更具体地说，加载到第一TEE 114中的代码在加载期间针对信任锚进行证实，并且一旦加载其，该映像就不可改变。因为该映像不可改变，所以第一TEE 114可以仅通过将新的已签名的映像加载到第一TEE 114上来改变。而且，第一角色OS 112和第二角色OS 122可以使用它们自身执行环境之外的资源，来管理它们的完整性。例如，操作系统的加载可以被加密并证实，并且该操作系统接入硬件资源，可以通过它们的控制之外的配置来限制和实施。

[0044] 软件架构100还包括加载操作系统104的主引导加载器140、加载第一角色OS112的第一次引导加载器142、以及加载第二角色OS 122的第二次引导加载器144。在该示例性实现中，移动通信装置10使用易于在引导过程期间建立平台信任的处理器。更具体地说，该处理器使能实现对引导加载器的签名验证，以易于在加载每一个操作系统期间建立信任。例如，移动通信装置10使用固定散列值和签名验证的组合，以使信任链随着其从硬件平台102扩展至第一角色110和第二角色120而保持不中断。

[0045] 在操作中，如果处理器24通过装置制造方的信任根以数字方式签名，则其加载主引导加载器140。如在此使用的，术语“装置制造方信任根”指通过装置制造方使用的一个或更多个机密加密密钥(即，密码证书)，以签名安装在移动通信装置10上的资产。该信任链连续不中断地通过管理程序106，易于建立隔离执行环境，验证移动通信装置10内的组件，和/或在可信平台模块内存储测量，供以后通过用户代码用于针对可信状态加以绑定。

[0046] 将第一TPM 60的控制传递至第一角色110，而将第二TPM 62的控制传递至第二角色120，以使TPM 60和62的测量引导方面可以被第一角色110和第二角色120使用。更具体地说，TPM 60和62通过移动通信装置10的可信引导软件而初始化，并接着在加载了角色之后，将控制传递至每一个角色，以供它们独占使用。如果角色使用针对可信引导的TPM，则硬件和/或软件变化可以导致无能力检索已经针对原始配置绑定的密钥，使得该角色在没有重新设置整个装置的情况下不能被重新引导。

[0047] 在引导过程期间，TPM测量(即，散列化)在移动通信装置10内使用的关键软件和固件组件。例如，在将针对主引导加载器140、操作系统104、管理程序106、安全监管程序108、引导加载器142、以及第一角色OS 112的测量扩展到第一TPM 60时，可以建立用于测量的信任根。该测量可以存储在位于第一TPM 60中的平台配置寄存器(PCR)中，并且可以用于在引导时间针对关联信任锚验证操作系统的映像。同样地，该系统的完整性可以在允许存取可以绑定至PCR的敏感信息之前加以验证。

[0048] 一旦在引导加载期间根据装置制造方信任而转移控制，该角色就可以负责它们自身的完整性。例如，证实安装并运行在第一角色OS 112上的应用130是第一角色OS112的责任是。同样地，对于流氓应用(未示出)危害运行在移动通信装置10上的来宾操作系统的完整性的情况来说，如果其它来宾操作系统的完整性没有与被危及的操作系统的信任关系，则该危害不影响它们的完整性。

[0049] 安全监管程序108与第一角色OS 112和第二角色OS 122通信联接。安全监管程序

108是易于存储并执行供在移动通信装置10的操作中使用的安全策略的操作系统。安全监管程序108运行在隔离环境中，并且可以使用平台资源、附加接口和/或附加能力。在一些实现中，第一角色110和第二角色120通过可信机制(即，CPU虚拟化)分离，使得角色拥有者无法配置不被该角色拥有者所拥有的角色的安全策略。例如，第一角色110的安全策略可以仅通过第一角色拥有者来配置，而第二角色120的安全策略可以仅通过第二角色拥有者来配置。更具体地说，每一个安全策略都可以用角色拥有者的私钥来签名，并且可以在安全监管程序108向关联角色应用安全策略之前，利用角色拥有者的对应公钥通过移动通信装置10来证实。针对第一角色110和第二角色120的所有权和安全策略被存储在可以通过安全监管程序108保持的配置文件中。而且，所有权和安全策略通过加密证书来验证。同样地，每一个角色拥有者可以针对其拥有的角色来限定操作系统、可信执行环境以及安全策略。

[0050] 第一角色110和第二角色120的安全策略可以通过角色拥有者来限定，并且可以与角色代码隔离地限定、存储以及实施。该安全策略限定每一个关联角色可以怎样接入移动通信装置10上的物理装置。例如，该安全策略限制角色接入一个或更多个物理装置、限定用于角色独占接入一个或更多个物理装置的准则、和/或限定用于针对第一角色110和第二角色120的共享装置接入的准则。更具体地说，用于接入共享装置的准则可以使能够共享该装置，使得仅在用户接口的控制下的角色接入该共享装置。而且，在针对接入共享装置的一个或更多个安全策略中的指定规则可以使能够共享该装置，以使后台运行的角色仍可以接入该共享装置。同样地，根据安全策略限定的规则使得角色拥有者能够按多种配置将移动通信装置10特制成适合他们的需要。

[0051] 第一角色110的基线映像和/或文件系统可以被加密并存储在内部和/或可去除介质上。而且，第一角色10的引导卷可以被加密，以使在第一角色110可以引导并存取存储在其上的敏感数据之前，可以需要来自可信引导过程的预引导认证。更具体地说，在可信引导过程期间，可以提示用户在第一角色110被允许引导之前输入证书。该用户在输入他/她的证书之前可能想要验证移动通信装置10的状况。例如，用户可以在输入密码和/或个人标识号(PIN)之前请求验证移动通信装置10处于可信状态，以确保输入画面可靠。如上所述，移动通信装置10包括诸如安全按钮17和/或LED 19和21(图1所示)这样的安全特征。安全特征按不可存取运行在移动通信装置10上的不可信代码的硬件来隔离，以易于验证输入画面可靠。

[0052] 在操作中，当认证对话出现在触摸屏18(图1所示)时，用户可以致动安全按钮17。致动安全按钮17显示用于移动通信装置10的信任根信息，和/或显示用于请求出现认证对话的软件的信任根信息。例如，该信任根信息可以包括用于移动通信装置10和/或用于运行在移动通信装置10上的角色的信任根信息。同样地，该用户可以验证信任根信息，并且安全地输入所请求的证书。在另选实现中，可以在LED 19和21按预定配置启用时验证认证对话。

[0053] 在一个实现中，该用户可能希望改变移动通信装置的操作状况。更具体地说，用户可能希望在运行在移动通信装置10上的多个角色之间转变移动通信装置10的焦点。例如，致动安全按钮17易于转变第一角色110与第二角色120之间的焦点。而且，第一LED 19被指配给第一角色110，而第二LED 21被指配给第二角色120。当第一角色110受关注时，可以启用第一LED 19并且可以停用第二LED 21，而当第二角色120受关注时，可以启用第二LED 21并且可以停用第一LED 19。这样，第一LED 19和第二LED 21基于移动通信装置10的操作状

况向用户提供可视反馈。

[0054] TPM 60和62中的至少一个具有物理存在(physical presence)特征，其提示用户验证其相对于移动通信装置10的存在性。例如，该物理存在特征可以被实现成，验证在移动通信装置10上运行的操作未被远程执行。同样地，可以按压安全按钮17，以验证用户的物理存在性。

[0055] 图5是可以与移动通信装置10一起使用的、要求角色的所有权的示例性方法的流程图。在该示例性实现中，移动通信装置10使用加密信任根，来限定第一角色110和第二角色120的所有权。例如，第一角色110可以被配置由一个实体使用，而第二角色120可以被配置由另一实体使用。移动通信装置10的发行方(即，企业)可以向用户(例如，客户和/或雇员)发行一个或更多个移动通信装置10。在这种实现中，第一角色110可以被配置用于商业用途，而第二角色120可以被配置用于个人用途。在另选实现中，移动通信模块10可以被配置成，通过指配分离SIM、分离服务，和/或通过隔离第一角色110和第二角色120的数据、操作系统以及蜂窝通信来分离角色。

[0056] 利用加密信任根使得移动通信装置10能够验证角色配置的完整性，并且限制角色对经授权方的修改权利。例如，可以将移动通信装置10提供给具有安装在其上的至少一个默认角色(即，没有限定所有权的角色)的终端用户。该默认角色由制造方根据默认信任锚来签名，其指示该角色未修改，并且具有指配给其的默认策略。该终端用户因而可以使用该默认角色，但在没有首先通过限定信任根来取得所有权的情况下，不能定制该默认角色。

[0057] 操作员200通过在角色管理器(PM)202的工作站上创建(212)针对一角色(如第二角色120)的信任根，来要求该角色的所有权。在一些实现中，PM 202还可以使得操作员200能够编辑和/或定义针对该角色的安全策略，和/或更新该角色的映像和/或可信执行环境(如第二TEE 124)。操作员200请求设备管理器(DM)204生成(214)用于要求诸如第二角色OS 122这样的操作系统的要求票，以从默认信任锚向所创建(212)的信任根传递所有权。该传递接着被授权(216)，并且该移动通信装置10被重新引导(218)。

[0058] 在重新引导(218)期间，操作员200联接DM 204与移动通信装置10之间的通用串行总线(USB)线缆，并且移动通信装置10检测该USB连接，并且进入编程模式，以使角色操作系统不加载。操作员200接着从工作站请求(220)DM 204运行用于向新的拥有者传递该角色的软件。该请求被朝着安全监管程序206引导(222)，并且可以限定新的角色信任锚。安全监管程序206接着使用所生成(214)的要求票，以从操作员200请求(224)授权来验证其身份，并且操作员200响应于授权请求(224)来输入(226)预定设备密码。请求224还可以根据所创建(212)的信任根来签名。

[0059] 移动通信装置10接着向用户呈现来自安全监管程序206的认证请求228，以输入他们的证书，来解锁安全部件208。如果该角色被默认信任锚确认为无主，则将旧角色资产散列和签名传递(234)至DM 204。DM 204验证签名，并且利用被经授权签名相关资产的新角色签名密钥来重新签名该散列。而且，允许存取角色介质密钥的角色密钥被改变。接着将替换签名从DM 204传递(236)至移动通信装置10，并且移动通信装置10验证该签名，并将该新签名替换角色资产上的旧签名。

[0060] 接着创建(238)角色转变文件，并且针对角色的配置文件被检查有效性，以及与已经处于移动通信装置10上的其它配置文件的冲突。如果该配置文件被验证，则该过程继续

进行，而如果配置文件之间存在冲突，则软件更新停止。用户角色认证在授权以继续进行时被更新(240)，使得介质密钥可以通过新信任根来存取，并且返回(242)至DM 204。

[0061] DM 204对所更新的资产进行签名，并且返回所签名的散列。例如，被更新的资产可以具有利用重新签名的散列而更新的签名，和/或可以利用新签名来更新(246)。角色转变文件在每一次更新之后都被触发检查点(checkpointed)(244)，以使得该过程能够从中断更新起重新开始。在更新完成之后，将缓冲数据刷新(flushed)(248)至闪存器210，将该角色转变文件删除(250)，并且该移动通信装置10被重新引导(252)。

[0062] 图6是供在授权要在移动通信装置10上执行的操作中使用的示例性系统300的示意性例示图。在该示例性实现中，实体在被准许修改安装在诸如移动通信装置10这样的所针对的计算装置上的软件之前可能需要被授权。例如，一旦角色已经被加载到移动通信装置10上，装置保持者就保留用于去除和/或替换该角色的授权，但该角色拥有者具有用于修改该角色的授权。同样地，代表角色拥有者起作用的实体可能需要被授权为，具有通过角色拥有者准予其的预定许可，以修改角色。如在此使用的，术语“装置保持者”指使用默认角色来操作移动通信装置10的实体。

[0063] 诸如设备管理器(DM)302这样的管理员计算机可以生成并向用于授权的授权服务器304发送请求，以执行移动通信装置10上的操作。该请求是指定用于要在移动通信装置10上执行的操作的参数的文件。示例性参数包括，但不限于，目标化计算装置(例如，移动通信装置10)的标识、要在目标化计算装置上执行的操作、将执行该操作的时段，以及目标化计算装置的地理位置。而且，该请求根据指配给管理员的私钥、公钥对中的第一私钥来签名。在一些实现中，该请求可以经由可去除介质(未示出)发送。

[0064] 授权服务器304接收来自DM 302的请求，并且利用第一私钥、公钥对中的公钥来验证DM 302的签名。授权服务器304还确定用于要执行的操作的参数是否与针对移动通信装置10的安全策略保持一致。所授权的参数可以存储在授权数据库306中，其可通过授权服务器304来存取。如果该请求已经被授权，则授权服务器304生成授权响应。授权响应可以包括：来自DM 302的请求，和通过授权服务器304创建的授权令牌。该授权令牌可以用于向所请求的操作授权。在一些实施方式中，该授权令牌可以具有可以执行所请求的操作的预定授权时段，可以被限制成向特殊目标化计算装置准予授权，和/或可以向执行移动通信装置10上的单一或多个操作授权。仅作为一示例，该认证令牌可以包括用于执行预定目标化计算装置上的操作的授权，和/或用于执行目标化计算装置上的预定操作的授权。而且，该授权令牌可以在以下至少一种情况下生成：在接收用于执行移动通信装置10上的操作的请求之前，和响应于验证用于执行移动通信装置10上的操作的请求。接着，该授权响应可以根据与授权服务器计算机相关联的私钥、公钥对中的第二私钥来签名，并且发送给管理员计算机。在另选实现中，该授权响应可以由认证操作员来签名。例如，该请求可以排队并且通过认证操作员签名、准予或拒绝。在一些实现中，该授权响应以经由可去除介质(未示出)来发送。

[0065] DM 302接收授权响应，并且确定该授权令牌是否向所请求的操作授权。例如，DM 302可以利用第二私钥、公钥对中的公钥来验证授权响应，其中，该授权响应利用第二私钥、公钥对中的私钥签名。如果该请求已经经授权，则DM 302向移动通信装置10发送授权响应文件，以请求执行操作。发送授权响应可以包括利用第一私钥、公钥对中的私钥来签名授权

响应。移动通信装置10接收授权响应，并且利用与管理员计算机相关联的第一私钥、公钥对中的公钥来验证签名，并且确定在该授权响应中指定的参数是否与用于移动通信装置10的安全策略一致。如果该签名被验证并且该参数一致，则移动通信装置10允许所请求的操作继续进行。接着，可以在移动通信装置10上执行特许操作。在另选实现中，该授权响应可以包括针对授权信任根的证书链。而且，在另选实现中，授权令牌可以经由sneaker-net生成并发送。

[0066] 图7是可以与移动通信装置10一起使用的、更新角色软件的示例性方法的流程图。在该示例性实现中，操作400可以通过将USB线缆从设备管理器(DM)工作站402联接至移动通信装置10来更新现有角色OS(如第二角色120)。设备管理软件运行，并且操作员400引导移动通信装置10重新引导(410)。在重新引导(410)期间，移动通信装置10检测USB连接，并且进入编程模式，使得角色操作系统不加载。操作员400接着引导DM软件412，以请求(414)针对移动通信装置10上的角色OS的更新。DM工作站402联系授权服务器以获取授权令牌。该授权令牌可以被高速缓冲和/或从离线源加载。安全监管程序404接着可以授权(416)该请求(414)，并且角色更新(418)可以继续进行。在一些实现中，如果不存在有效的授权令牌，则DM软件将警告操作员400，并且拒绝执行更新过程。

[0067] DM工作站402包括可以用于解锁安全部件406的共享机密密钥。仅与经授权角色有关的存储加密密钥可以利用通过共享加密密钥提供的认证来从安全部件406检索。移动通信装置10接着证实该授权令牌，以验证操作员400具有用于执行所请求的操作的特许。通过安全部件406来认证(420)该用户，而且如果操作员400没有正确的证书，则放弃该操作。

[0068] DM软件接着从移动通信装置10请求(422)该角色的装置几何特征数据。该装置几何特征数据可以包括，但不限于：角色的TEE组件和OS的尺寸。如果该角色几何特征匹配装置几何特征，则软件更新继续进行，而如果不匹配，则软件更新停止并且指示错误。在另选实现中，还可以提供角色拥有包的修订号，这样，角色拥有者可以验证该更新的兼容性。

[0069] DM软件通过向移动通信装置10发送(424)要更新的软件，而开始加载过程。在一个实现中，如果角色的配置被包括在更新中，则该软件更新通过发送(426)该配置而开始。安全监管程序404接着检查并估计该配置文件的几何特征、信任根以及签名，以确定与已经加载在移动通信装置10上的其它配置文件是否出现冲突。如果该配置文件被证实(428)和/或如果配置文件未被更新，则软件更新继续进行，而如果配置文件之间存在冲突，则软件更新停止。而且，所更新的操作系统和/或可信执行环境可以被加载(430)和(432)到移动通信装置10上。

[0070] 所发送的软件更新被存储在闪速存储器408上，并且针对信任锚进行证实。接着，创建(434)色转变文件，以指示要更新哪个软件，该软件被写入到闪存408上，并且在每一次更新之后，在该转变文件中创建检查点。例如，将新的配置文件写入(436)到闪存408上，并且该转变文件被触发检查点(438)，将新的角色OS文件系统写入(440)到闪存408上，并且转变文件被触发检查点(442)，以及将新的角色TEE文件系统写入(444)到闪存408上，并且转变文件被触发检查点(446)。在该示例性实现中，目标闪存文件系统根据更早存储的存储器内容来编程，并且在传递期间利用来自配置文件的存储密钥进行加密。在更新完成之后，将缓冲数据刷新(flushed)(448)至闪存器408，将该角色转变文件删除(450)，并且该移动通信装置10被重新引导(452)。

[0071] 图8是可以与移动通信装置10一起使用的、转变角色的所有权的示例性方法的流程图。在移动通信装置10上加载的角色的所有权可以被转变给新的拥有者，而不需要更角色数据。在该示例性实现中，该新拥有者在设备管理器(DM)内生成(510)传递票(transfer ticket)(New RoT)502。该传递票可以是详细说明要转变的特定装置和所希望的当前信任根的数据块。该数据块接着被发送至当前角色拥有者，并且当前角色拥有者验证当前角色拥有者DM(New RoT)502内的信息。

[0072] 接着，代表当前角色拥有者工作的操作员500获取指示操作员和当前角色拥有者是否通过DM(Old RoT)503来授权的授权令牌，以传递角色。接着，将该授权令牌附加至所传递票并签名，并将所签名传递票传递至闪存508并存储。所签名的传递票还可以连同针对安全部件506内的角色槽(persona slot)的认证密钥一起返回至预期的新角色拥有者。在这种实现中，该认证密钥可以利用附接至传递令牌的新角色拥有者的DM操作员公钥来遮蔽。代表新角色拥有者工作的操作员因而可以使用所遮蔽的传递令牌来开始传递过程。更具体地说，移动通信装置10可以验证新角色拥有者的证书并且授权传递。

[0073] 接着，操作员500将USB线缆从DM(New RoT)的工作站502联接至移动通信装置10。设备管理软件运行并且操作员500引导移动通信装置10重新引导(518)。在重新引导(518)期间，移动通信装置10检测USB连接并且进入编程模式，使得角色操作系统不加载。接着，操作员500指令DM软件将当前角色拥有者所拥有的角色转变给新的角色拥有者。该传递票包括：授权所需的信息；和操作员500的公钥基础结构(PKI)证书，其用于认证根据针对所转变的角色的前一拥有者的信任根签名的请求。

[0074] DM软件使用操作员500的机密密钥，以解蔽来自传递票的认证密钥。接着，可以将该认证密钥用于(520)请求(522)角色传递，并且认证(524)操作员，以解锁移动通信装置10上的安全部件506。在这种实现中，该认证(524)仅使能够存储与要从安全部件506检索的已授权的角色有关的加密密钥。

[0075] 该转变还包括将旧的角色资产散列传递(530)至DM 502。DM 502验证签名，并且利用被经授权签名相关资产的新角色签名密钥来重新签名该散列。而且，允许存取角色介质密钥的角色密钥被改变，并且将新的值转递至DM 502。接着将替换签名从DM 502传递(532)至移动通信装置10，并且移动通信装置10验证该签名，并将该新签名替换角色资产上的旧签名。

[0076] 接着创建(534)角色转变文件，并且针对角色的配置文件被检查有效性，以及与已经加载在移动通信装置10上的其它配置文件的冲突。如果该配置文件被验证，则该过程继续进行，而如果配置文件之间存在冲突，则软件更新停止。在授权以继续进行时用户角色认证被更新(536)，使得介质密钥可以通过新信任根来存取，并且返回(538)至DM 502。

[0077] DM 502对所更新的资产进行签名并且返回所签名的散列。例如，被更新的资产可以具有利用重新签名的散列而更新的签名，和/或可以利用新签名来更新(542)。角色转变文件在每一次更新之后都被触发检查点(checkpointed)(540)，使得该过程能够从中断更新起重新开始。在更新完成之后，将缓冲数据刷新(flushed)(544)至闪存器508，将该角色转变文件删除(546)，并且该移动通信装置10被重新引导(548)。

[0078] 在将角色所有权传递至新的角色拥有者之后，可能需要在所转变的角色与具有和前一角色拥有者的信任关系的任何角色之间建立新的信任关系。更具体地说，运行在移动

通信装置10上的其它角色的角色配置可能必须被更新，以建立与新的角色拥有者的信任关系，从而保持和前一角色拥有者相同的功能性。

[0079] 图9是可以与移动通信装置10一起使用的、加载新角色的示例性方法的流程图。在该示例性实现中，操作员600将USB线缆从设备管理器(DM)工作站602联接至移动通信装置10。设备管理软件运行，并且操作员600引导移动通信装置10重新引导(612)。在重新引导(612)期间，移动通信装置10检测USB连接并且进入编程模式，使得角色操作系统不加载。接着，提示(614)操作员600利用通过设备拥有者保持的设备密码来授权USB连接，并且输入(616)设备密码并认证(618)，以解锁安全部件606。在另选实现中，移动通信装置10可以被重新初始化，并且重置成工厂配置。

[0080] 接着，DM软件620从移动通信装置10请求角色的装置几何特征数据，并且操作员600引导DM工作站602将角色包加载(622)到特定角色槽中。该装置几何特征数据可以包括，但不限于：角色的TEE组件和OS的尺寸。如果该角色几何特征匹配装置几何特征，则软件更新继续进行，而如果不匹配，则软件更新停止，并且指示错误。在另选实现中，还可以提供角色拥有包的修订号，这样，角色拥有者可以验证该更新的兼容性。

[0081] DM软件通过发送要加载到移动通信装置10上的软件而开始加载过程。在一个实现中，通过向移动通信装置10发送(624)角色的配置文件而开始该软件加载。安全监管程序604接着检查并估计该配置文件的几何特征、信任根以及签名，以确定与已经加载在移动通信装置10上的其它配置文件是否出现冲突。如果该配置文件被证实(626)，则该软件加载继续进行，而如果配置文件之间存在冲突，则停止软件加载。在一些实现中，将新的角色OS和新的TEE加载(628和630)到移动通信装置10上。

[0082] 所发送的软件被存储在闪速存储器608上，并且被针对信任锚进行证实。接着，创建(632)并写入角色转变文件，以指示盖写(overwrite)。该盖写指示是按持久方式写入的标记(sentinel)值，使得如果更新过程被中断，则可以采取合适的恢复措施来从失败恢复。更具体地说，删除(634)针对该角色的安全部件606中的存储介质密钥，擦除(636)旧的角色配置文件，擦除(638)角色闪存文件系统，并且强行清除(640)可信平台模块(TPM)610。

[0083] 接着，可以持久方式将新的角色加载到移动通信装置10中。更具体地说，将新的配置文件写入到闪存608上，通过安全监管程序604读取(644)用户认证数据，并且认证(646)用户，以解锁安全部件606。接着，私钥、公钥对中的公共加密密钥(PEK)可以被创建(648)，并且从安全部件606输送(650)至角色拥有者。该角色拥有者利用其证书授权来对PEK进行签名，而如果该配置文件被证实(652)，则继续进行软件加载(654)。接着，将PEK返回并存储(656)在安全部件606中。

[0084] 将PEK私钥、公钥对的机密密钥存储在安全部件606内并加以保护，使得其不从安全部件606输出。这使得角色拥有者能够通过根据私钥签名的响应，来验证用于执行服务的请求来自经授权装置。该PEK可以在限定角色所有权时创建，并且例如可以用于认证软件更新、软件请求和/或软件包。在另选实现中，可以创建第二私钥、公钥对并用于加密，使得角色拥有者可以加密针对特定装置的数据，并且使得其它装置不能够解密该数据。

[0085] 接着，将新的角色OS文件系统写入(658)到闪存608上，将新角色TEE文件系统写入(660)到闪存608上，并且创建新的角色数据分区。目标闪存文件系统根据更早存储的存储器内容来编程，并且在传递期间利用来自配置文件的存储密钥进行加密。在更新完成之后，

将该角色转变文件删除(664)，并且该移动通信装置10被重新引导(666)。

[0086] 而且，本公开包括根据下列条款的实施方式：

[0087] 条款1、提供了一种存储用于操作移动通信装置的计算机可执行指令的非暂时计算机可读介质，该移动通信装置包括处理器、第一可信平台模块以及第二可信平台模块，该计算机可执行指令致使所述处理器进行如下操作：

[0088] 建立针对第一角色的信任根，所述第一角色包括第一操作系统和第一可信执行环境；

[0089] 建立针对第二角色的信任根，所述第二角色包括第二操作系统和第二可信执行环境；

[0090] 在所述第一可信平台模块中存储限定针对所述第一角色的所述信任根的测量；

[0091] 在所述第二可信平台模块中存储限定针对所述第二角色的所述信任根的测量；以及

[0092] 利用针对所述第一角色的所述信任根和针对所述第二角色的所述信任根，来加载所述第一角色和所述第二角色。

[0093] 条款2、根据条款1所述的非暂时计算机可读介质，所述非暂时计算机可读介质还包括计算机可执行指令，该计算机可执行指令致使所述处理器进行如下操作：

[0094] 在所述第一可信执行环境与所述第二可信执行环境之间建立互信，使得所述第一角色与所述第二角色通信联接。

[0095] 条款3、根据条款1所述的非暂时计算机可读介质，所述非暂时计算机可读介质还包括计算机可执行指令，该计算机可执行指令致使所述处理器进行如下操作：

[0096] 利用根据装置制造方信任根签名的引导加载器来加载基础操作系统。

[0097] 条款4、根据条款1所述的非暂时计算机可读介质，所述非暂时计算机可读介质还包括计算机可执行指令，该计算机可执行指令致使所述处理器进行如下操作：

[0098] 在已经加载所述第一角色和所述第二角色之后，将所述第一可信平台模块的控制传递至所述第一角色，而将所述第二可信平台模块的控制传递至所述第二角色。

[0099] 条款5、根据条款1所述的非暂时计算机可读介质，所述非暂时计算机可读介质还包括计算机可执行指令，该计算机可执行指令致使所述处理器：

[0100] 限定针对所述第一角色的安全策略和针对所述第二角色的安全策略，其中，所述安全策略限定所述第一角色和所述第二角色怎样接入所述移动通信装置上物理装置；以及

[0101] 利用安全监管程序实施所述安全策略。

[0102] 本书面描述使用实施例来公开包括最佳模式的各个实现，并且还使得本领域任何技术人员能够具体实践各个实现，包括制造和使用任何装置或系统并且执行任何并入方法。本公开的可专利化范围通过权利要求书来限定，并且可以包括本领域技术人员想到的其它实施例。如果这种其它实施例具有不与本权利要求书的字面语言不同的结结构性部件，或者它们包括与本权利要求书的字面语言无实质差异的等同结构性部件，则该实施例处于本权利要求书的范围内。

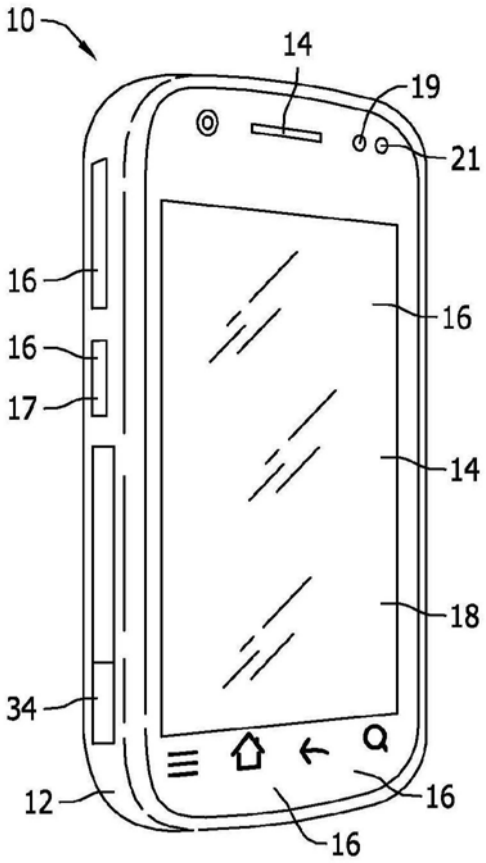


图1

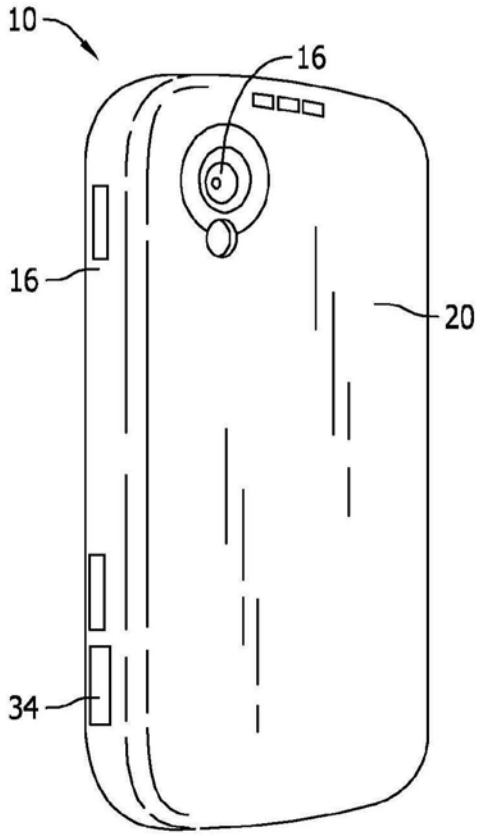


图2

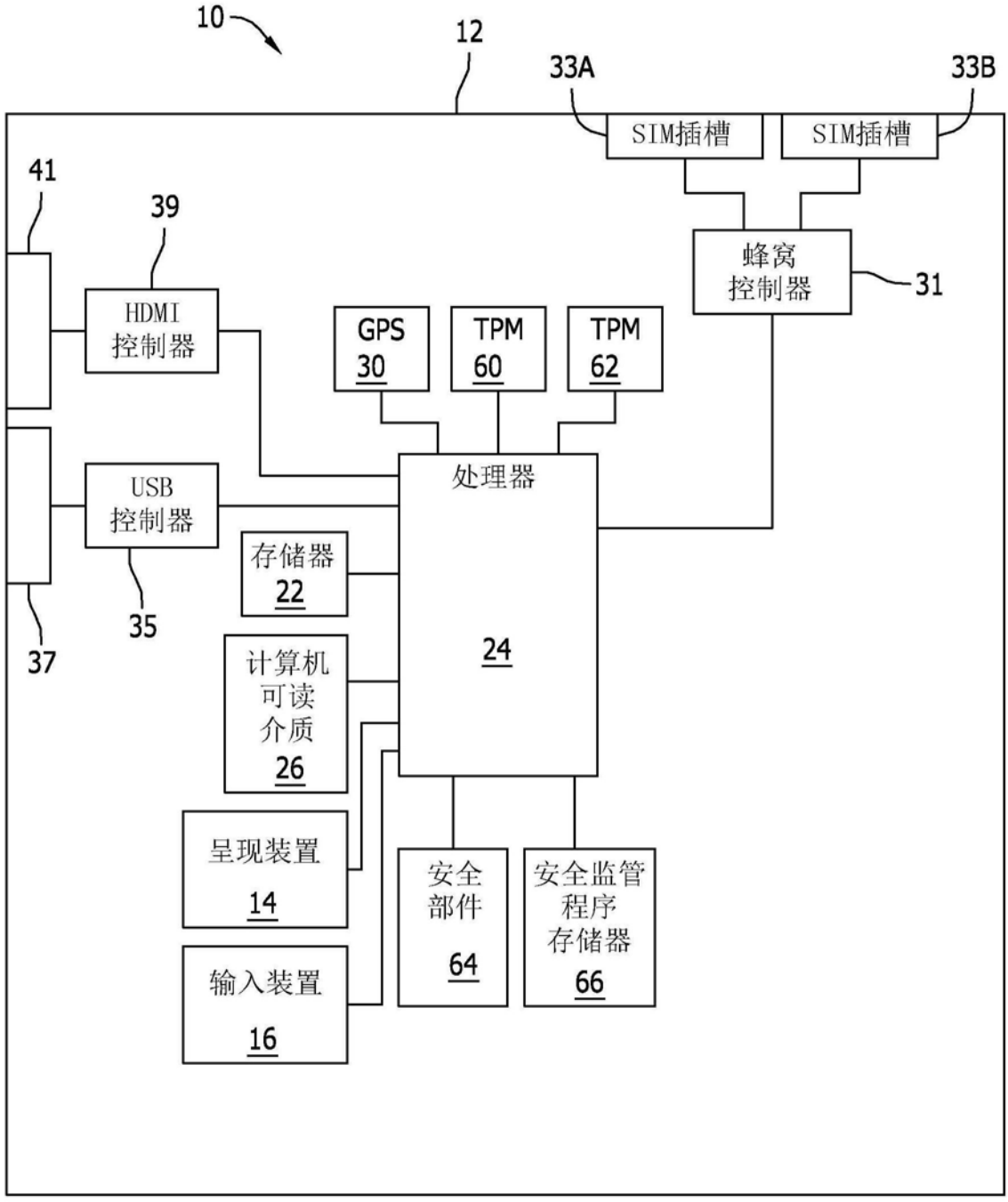

10
12
33A
33B
SIM插槽
SIM插槽
41
39
蜂窝
控制器
31
HDMI
控制器
GPS
30
TPM
60
TPM
62
处理器
USB
控制器
存储器
22
35
37
24
计算机
可读
介质
26
呈现装置
14
安全
部件
64
安全监管
程序
存储器
66
输入装置
16

图3

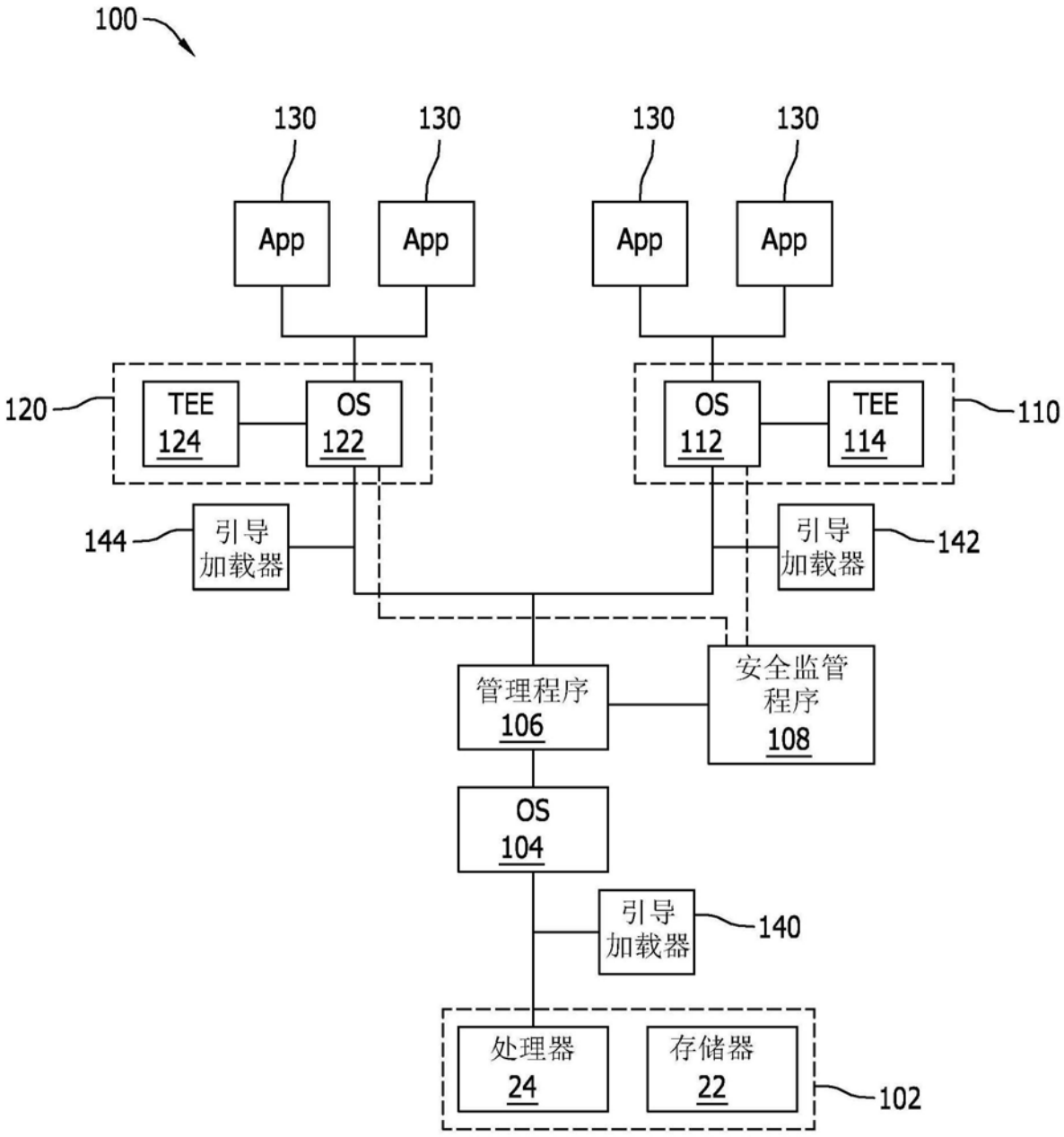

100
130
130
130
130
App
App
App
App
120
TEE
124
OS
122
OS
112
TEE
114
110
144
引导
加载器
引导
加载器
142
管理程序
106
安全监管
程序
108
OS
104
引导
加载器
140
处理器
24
存储器
22
102

图4

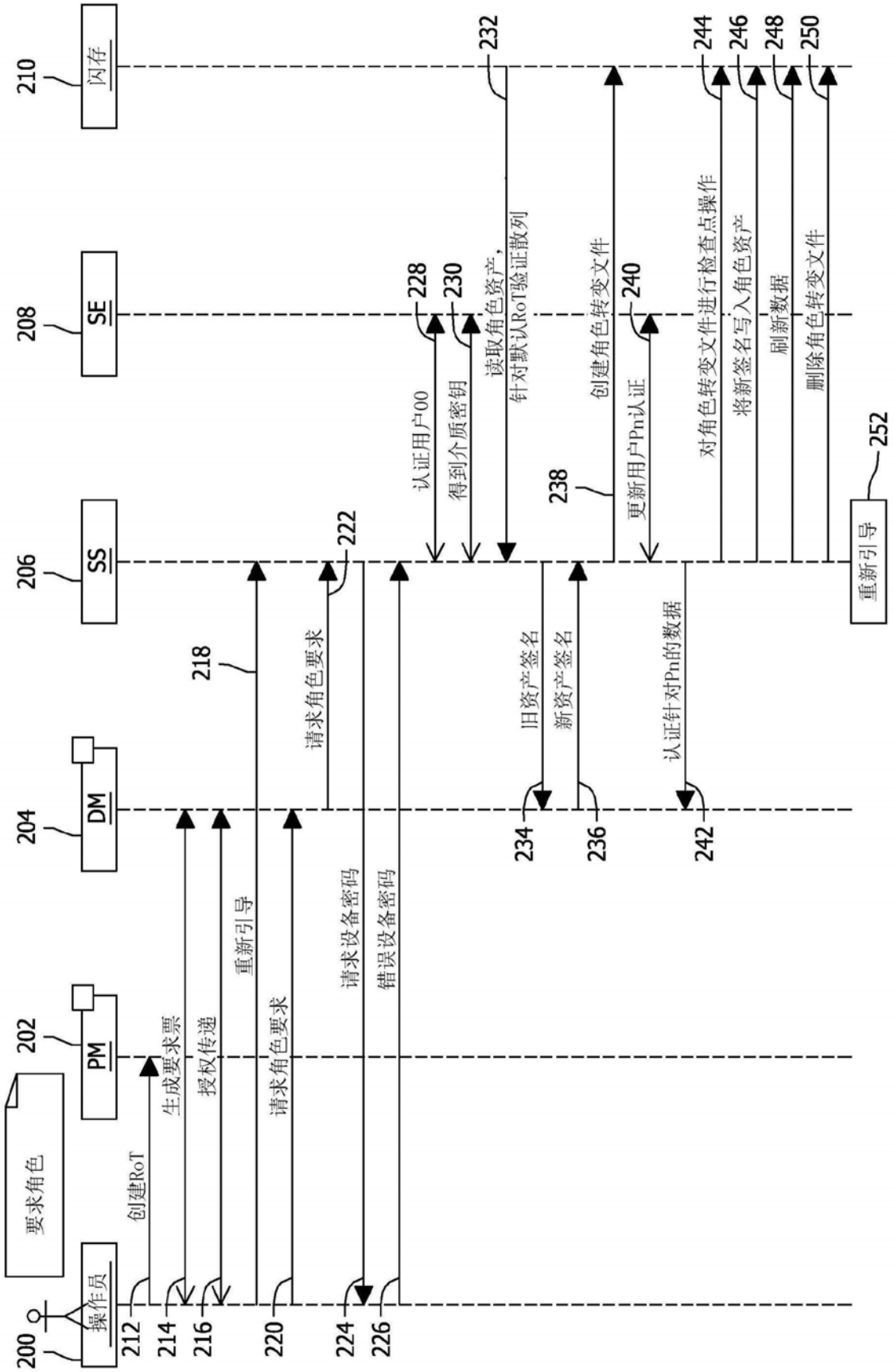

200
操作员
要求角色
202
PM
204
DM
206
SS
208
SE
210
闪存
212
创建RoT
214
生成要求票
216
授权传递
218
重新引导
220
请求角色要求
222
请求角色要求
224
请求设备密码
226
错误设备密码
228
认证用户00
230
得到介质密钥
232
读取角色资产，
针对默认RoT验证散列
234
旧资产签名
236
新资产签名
238
更新用户Pn认证
240
创建角色转变文件
242
认证针对Pn的数据
244
对角色转变文件进行检查点操作
246
将新签名写入角色资产
248
刷新数据
250
删除角色转变文件
252
重新引导

图5

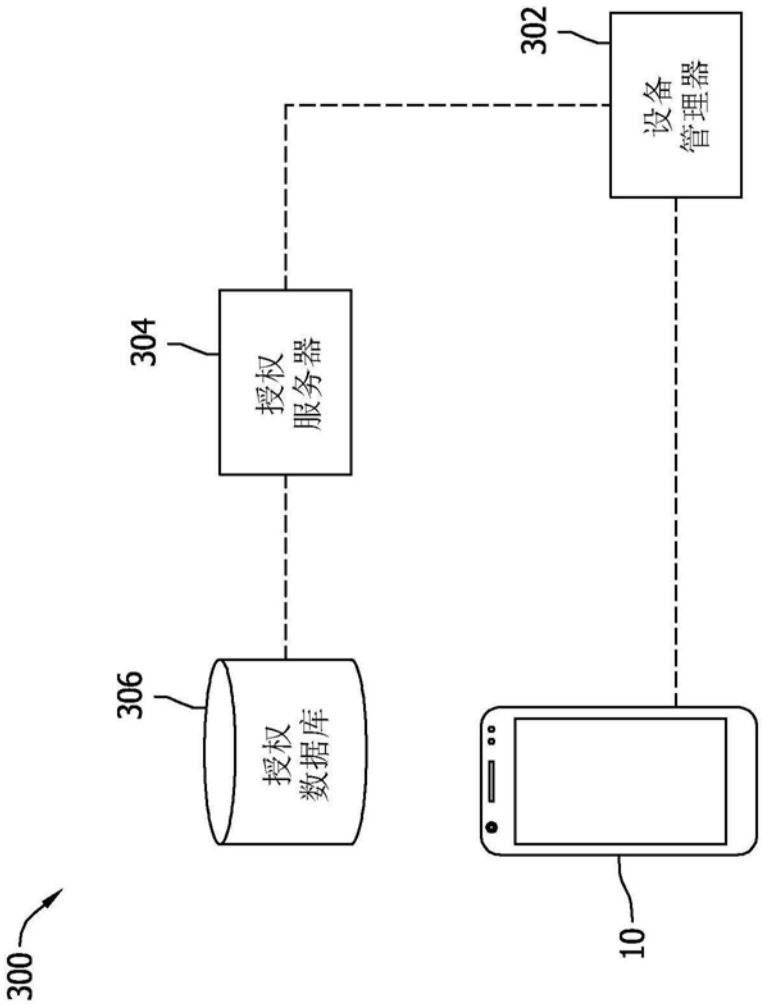


图6

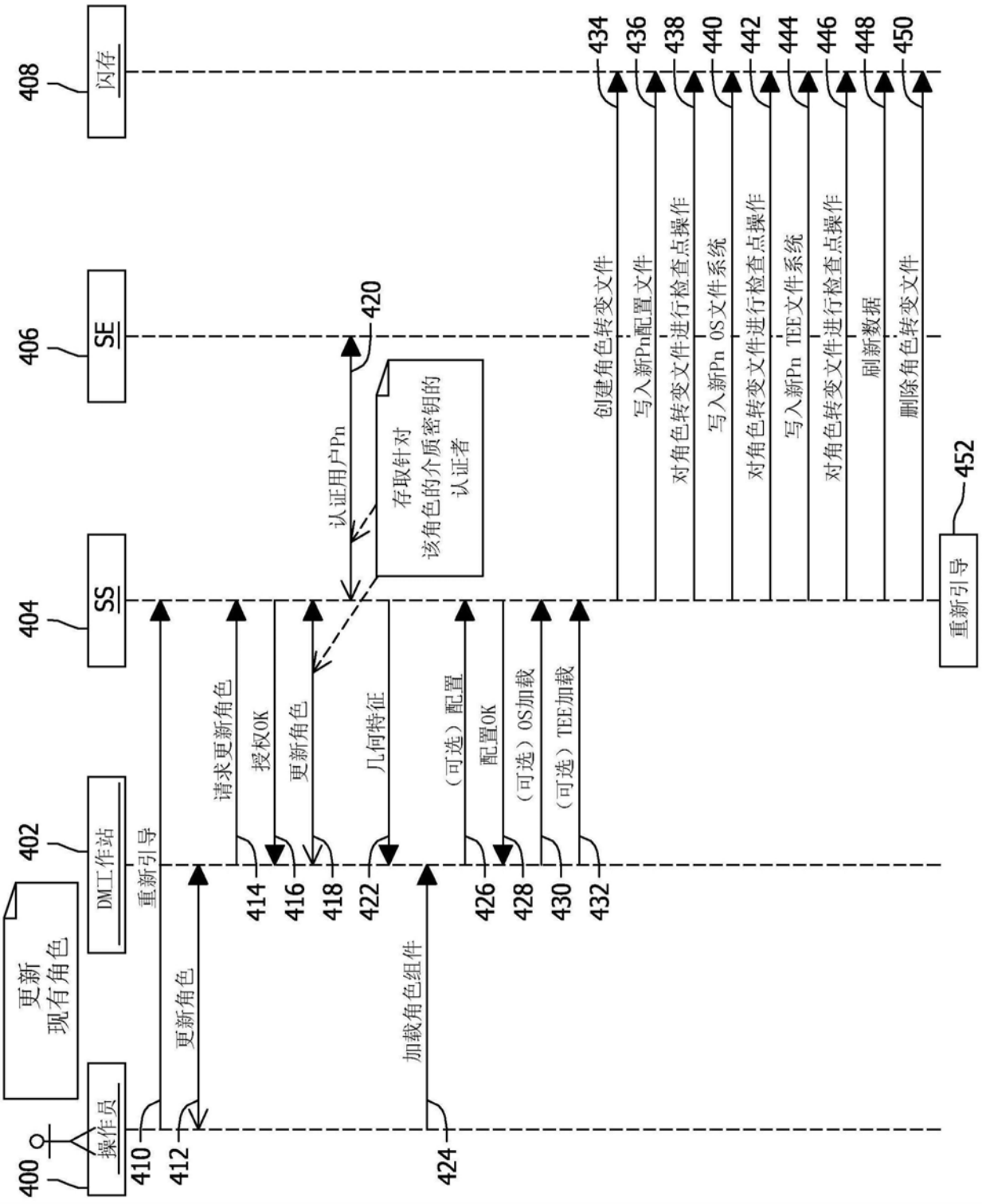

400
操作员
410
412
424
更新
现有角色
402
DM工作站
重新引导
更新角色
加载角色组件
404
SS
请求更新角色
414
授权OK
416
更新角色
418
几何特征
422
406
SE
420
认证用户Pn
存取针对
该角色的介质密钥的
认证者
（可选）配置
426
配置OK
428
（可选）OS加载
430
（可选）TEE加载
432
408
闪存
创建角色转变文件
434
写入新Pn配置文件
436
对角色转变文件进行检查点操作
438
写入新Pn OS文件系统
440
对角色转变文件进行检查点操作
442
写入新Pn TEE文件系统
444
对角色转变文件进行检查点操作
446
刷新数据
448
删除角色转变文件
450
重新引导
452

图7

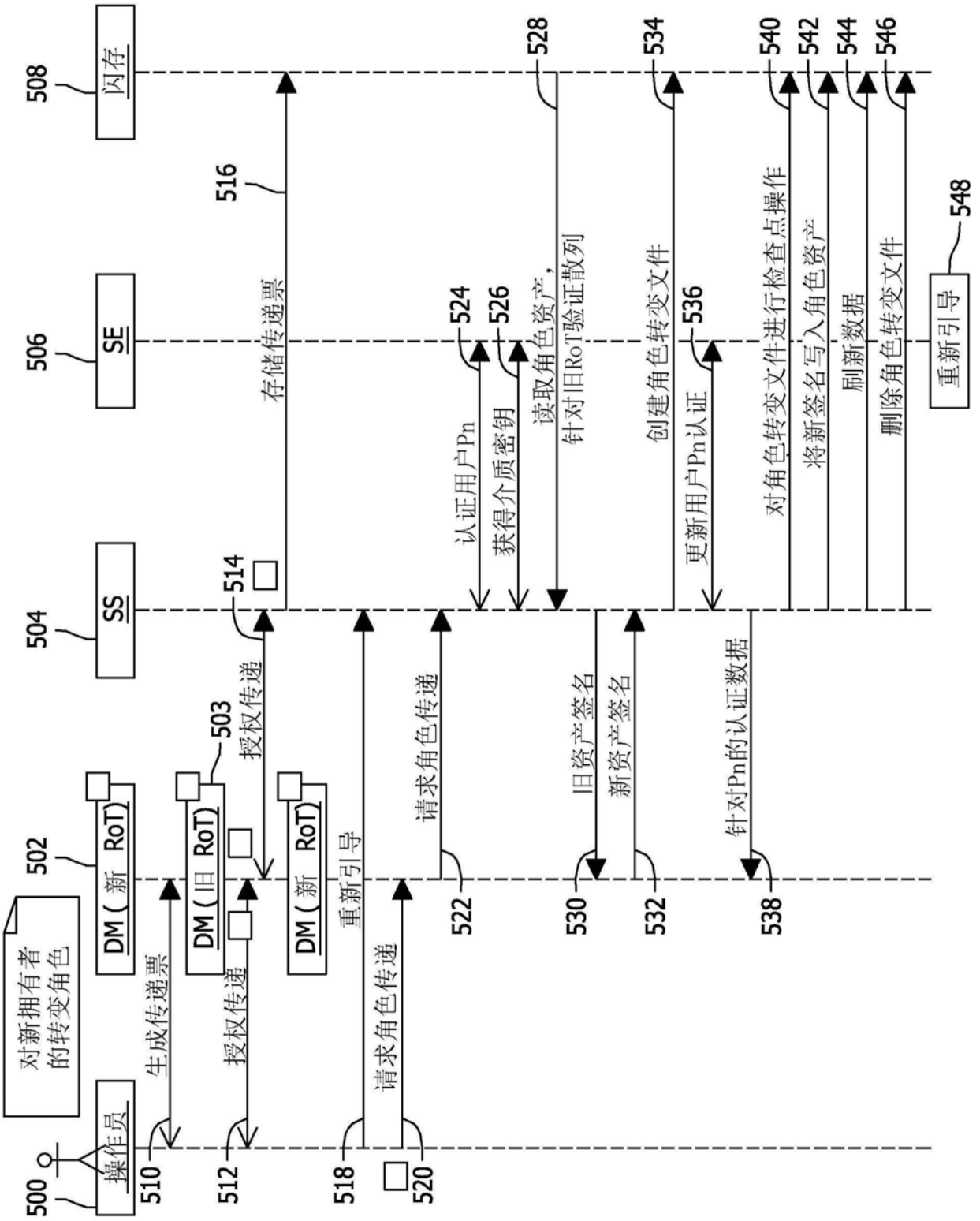

500
操作员
对新拥有者的转变角色
502
DM（新 RoT）
503
DM（旧 RoT）
DM（新 RoT）
504
SS
506
SE
508
闪存
510
生成传递票
512
授权传递
514
授权传递
516
存储传递票
518
重新引导
520
请求角色传递
522
请求角色传递
524
认证用户Pn
526
获得介质密钥
528
读取角色资产，
针对旧RoT验证散列
530
旧资产签名
532
新资产签名
534
创建角色转变文件
536
更新用户Pn认证
538
针对Pn的认证数据
540
对角色转变文件进行检查点操作
542
将新签名写入角色资产
544
刷新数据
546
删除角色转变文件
548
重新引导

图8

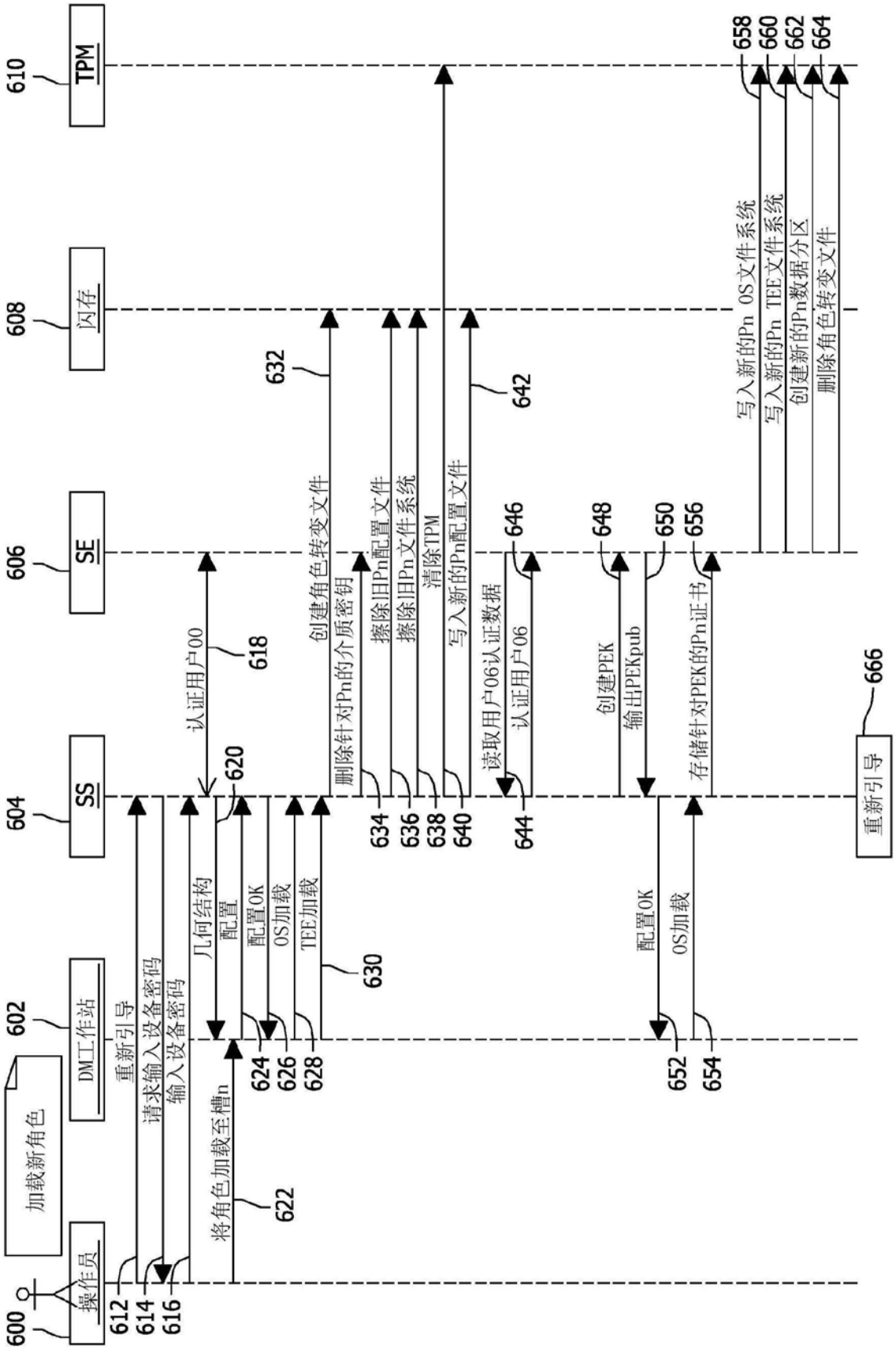

600
操作员
加载新角色
602
DM工作站
604
SS
606
SE
608
闪存
610
TPM
612 重新引导
614 请求输入设备密码
616 输入设备密码
618 认证用户00
620
622 将角色加载至槽n
624 几何结构配置
626 配置OK
628 OS加载
630 TEE加载
632 创建角色转变文件
634 删除针对Pn的介质密钥
636 擦除旧Pn配置文件
638 擦除旧Pn文件系统
640 清除TPM
642 写入新的Pn配置文件
644 读取用户06认证数据
646 认证用户06
648 创建PEK
650 输出PEKpub
652 配置OK
654 OS加载
656 存储针对PEK的Pn证书
658 写入新的Pn OS文件系统
660 写入新的Pn TEE文件系统
662 创建新的Pn数据分区
664 删除角色转变文件
666 重新引导

图9