(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 110050437 B
(45)授权公告日 2020.10.23

(21)申请号 201680089029.9
(22)申请日 2016.09.06
(65)同一申请的已公布的文献号
申请公布号 CN 110050437 A
(43)申请公布日 2019.07.23
(85)PCT国际申请进入国家阶段日
2019.03.06
(86)PCT国际申请的申请数据
PCT/EP2016/070936 2016.09.06
(87)PCT国际申请的公布数据
WO2018/046073 EN 2018.03.15
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 连刚 桑泊.索维欧 邓太生 王小璞 叶宗波
(51)Int.Cl.
H04L 9/32(2006.01)
H04W 12/06(2006.01)

(56)对比文件
US 2016134621 A1,2016.05.12
US 2006085634 A1,2006.04.20
CN 101136743 A,2008.03.05
US 2003115455 A1,2003.06.19
CN 101150533 A,2008.03.26

审查员 赵勇达

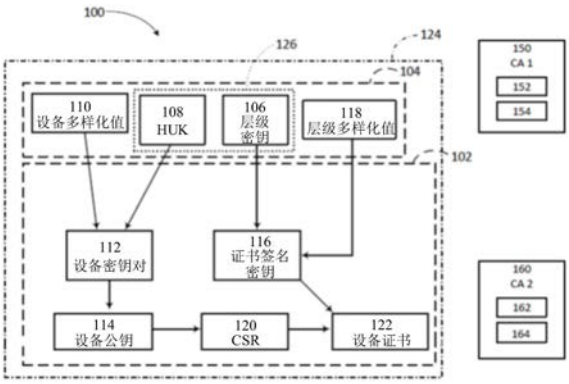
权利要求书2页 说明书13页 附图6页

(54)发明名称

分布式证书注册的装置和方法

(57)摘要

本发明提供了一种包括处理器和存储器的装置，其中，所述处理器和所述存储器用于提供安全执行环境，以及所述存储器存储硬件唯一密钥和层级密钥。所述处理器用于在所述安全执行环境中基于所述层级密钥恢复证书签名密钥，其中，所述证书签名密钥与证书颁发中心相关联。所述处理器基于所述硬件唯一密钥导出设备密钥对，其中，所述设备密钥对包括设备公钥和设备私钥；以及基于所述设备公钥和所述证书签名密钥生成设备证书。所述生成的设备证书配置为基于与所述证书颁发中心相关联的公钥进行验证。



CN 110050437 B

1.一种生成设备证书的装置(100),其特征在于,包括处理器(102)和存储器(104),其中,所述处理器(102)和所述存储器(104)用于提供安全执行环境(124),所述存储器(104)包括硬件唯一密钥(108)和层级密钥(106),所述处理器(102)用于在所述安全执行环境中:

基于所述层级密钥(106)恢复证书签名密钥(116),其中,所述证书签名密钥(116)与证书颁发中心(150)相关联;

基于所述硬件唯一密钥(108)导出设备密钥对(112),其中,所述设备密钥对(112)包括设备公钥(114)和设备私钥;以及

基于所述设备公钥(114)和所述证书签名密钥(116)生成设备证书(122),其中,所述设备证书(122)配置为基于与所述证书颁发中心(150)相关联的公钥(154)进行验证;其中,所述存储器(104)包括层级多样化值(118),以及所述处理器(102)用于基于所述层级密钥(106)和所述层级多样化值(118)恢复所述证书签名密钥(116);所述处理器还用于:更新所述层级多样化值(118);

基于所述更新后的层级多样化值和所述层级密钥(106)恢复更新后的证书签名密钥,其中,所述更新后的证书签名密钥与第二证书颁发中心(160)相关联;以及

基于所述更新后的证书签名密钥和所述设备公钥(114)生成更新后的设备证书,其中,所述更新后的设备证书配置为基于与所述第二证书颁发中心(160)相关联的公钥(164)进行验证。

2.根据权利要求1所述的装置(100),其特征在于,所述处理器(102)用于:

基于所述设备公钥(114)和所述设备私钥生成证书签名请求(120);

基于所述证书签名请求(120)和所述证书签名密钥(116)生成所述设备证书(122)。

3.根据权利要求1或2所述的装置(100),其特征在于,所述存储器(104)包括设备多样化值(110),以及所述处理器(102)用于基于所述硬件唯一密钥(108)和所述设备多样化值(110)导出所述设备密钥对(112)。

4.根据权利要求3所述的装置(100),其特征在于,所述处理器(102)用于:

更新所述设备多样化值(110);

基于所述硬件唯一密钥(108)和所述更新后的设备多样化值(110)导出更新后的设备密钥对(112),其中,所述更新后的设备密钥对(112)包括更新后的设备公钥(114)和更新后的设备私钥;以及

基于所述更新后的设备公钥(114)和所述证书签名密钥(116)生成更新后的设备证书(122)。

5.根据权利要求1或2或4所述的装置(100),其特征在于,所述证书签名密钥(116)基于白盒解密进行恢复。

6.根据权利要求1或2或4所述的装置(100),其特征在于,所述设备密钥对(112)基于白盒解密来导出。

7.根据权利要求1或2或4所述的装置(100),其特征在于,所述装置为移动电话或移动计算设备。

8.一种生成在装置的安全执行环境中执行的设备证书的方法(400),其特征在于,所述方法(400)包括:

基于层级密钥恢复(404)证书签名密钥,其中,所述证书签名密钥与证书颁发中心相关

联；

基于硬件唯一密钥导出(406)设备密钥对，其中，所述设备密钥对包括设备公钥和设备私钥；以及

基于所述设备公钥和所述证书签名密钥生成(410)设备证书，其中，所述设备证书配置为基于与所述证书颁发中心相关的公钥进行验证；其中所述装置包括处理器(102)和存储器(104)；所述存储器(104)包括层级多样化值(118)，以及所述处理器(102)用于基于所述层级密钥(106)和所述层级多样化值(118)恢复所述证书签名密钥(116)；

所述处理器还用于：

更新所述层级多样化值(118)；

基于所述更新后的层级多样化值和所述层级密钥(106)恢复更新后的证书签名密钥，其中，所述更新后的证书签名密钥与第二证书颁发中心(160)相关联；以及

基于所述更新后的证书签名密钥和所述设备公钥(114)生成更新后的设备证书，其中，所述更新后的设备证书配置为基于与所述第二证书颁发中心(160)相关联的公钥(164)进行验证。

9.根据权利要求8所述的方法(400)，其特征在于，所述证书签名密钥基于所述层级密钥和层级多样化值进行恢复(404)。

10.根据权利要求8或9所述的方法(400)，其特征在于，所述设备密钥对基于所述硬件唯一密钥和设备多样化值来导出(406)。

11.根据权利要求8或9所述的方法(400)，其特征在于，包括：

基于所述设备公钥和所述设备私钥生成(408)证书签名请求；以及

基于所述证书签名请求和所述证书签名密钥生成(410)所述设备证书。

12.一种在包括存储器的装置中使用的处理器(102)，其特征在于，所述处理器(102)和所述存储器(104)用于提供安全执行环境(124)，所述存储器(104)包括硬件唯一密钥(108)和层级密钥(106)，以及所述处理器(102)用于在所述安全执行环境中：

基于所述层级密钥(106)恢复证书签名密钥(116)，其中，所述证书签名密钥(116)与证书颁发中心(150)相关联；

基于所述硬件唯一密钥(108)导出设备密钥对(112)，其中，所述设备密钥对(112)包括设备公钥(114)和设备私钥；

基于所述设备公钥(114)和所述证书签名密钥(116)生成设备证书(122)，其中，所述设备证书(122)配置为基于与所述证书颁发中心(150)相关联的公钥(154)进行验证；其中，所述存储器(104)包括层级多样化值(118)，以及所述处理器(102)用于基于所述层级密钥(106)和所述层级多样化值(118)恢复所述证书签名密钥(116)；

所述处理器还用于：

更新所述层级多样化值(118)；

基于所述更新后的层级多样化值和所述层级密钥(106)恢复更新后的证书签名密钥，其中，所述更新后的证书签名密钥与第二证书颁发中心(160)相关联；以及

基于所述更新后的证书签名密钥和所述设备公钥(114)生成更新后的设备证书，其中，所述更新后的设备证书配置为基于与所述第二证书颁发中心(160)相关联的公钥(164)进行验证。

分布式证书注册的装置和方法

技术领域

[0001] 本发明各方面大体上涉及公钥加密体系,更具体地,涉及数字证书生成和注册。

背景技术

[0002] 数据网络需要进行安全通信使得公钥加密体系随之扩散。公钥加密体系可以用于授权设备、交换密钥,以及对通过公共网络交换的或存储在不安全数据存储器中的数据进行加密、签名和解密。公钥加密体系以非对称密码算法为基础,其中使用一个密钥加密数据,使用第二密钥解密数据。重要的是,用于加密数据的密钥不能用于解密数据。因此,通过对一个密钥进行保密而使第二密钥公开可用,具有该公钥的任何实体都可以对它们希望保密的信息进行加密,而只有有权使用相应私钥的实体才能解密该数据。

[0003] 在对敏感数据进行加密之前,重要的是确保正在使用的公钥实际上属于预期接收方而不是攻击者提供的假密钥。在现代公钥基础设施(public key infrastructure,PKI)中,通过使用数字证书来提供这种保证。数字证书是包括数字签名的数字文档,用于将公钥与相关联的实体信息进行加密绑定。由于证书是由已知的证书颁发中心(certificate authority,CA)颁发的,所以可以使用发证CA的公钥来验证数字证书中包括的签名。因此,信任CA的实体可以通过数字证书来建立信任。

[0004] 目前使用的几乎每个计算设备都需要安全通信,因此将需要具有可信设备证书来分发该计算设备的公钥。管理加密密钥以及为每个制造商的每个设备颁发证书会是一项艰巨的任务。为了便于颁发证书,使用公钥基础设施(public key infrastructure,PKI)来创建CA的分层结构,这样根CA为下级或中间CA签署证书,然后,下级或中间CA可以向终端实体或其它下级CA颁发证书。在PKI中,每个证书包括识别发证CA的信息,从而可以在验证主体证书之前验证发证CA的证书。这样,可以通过验证证书链来验证证书,直到找到可信CA或者直到进入可信根CA。这称为信任链。

[0005] 部署能够为每个制成的设备颁发证书的PKI要求在全球范围内分布有多家CA,因此会是一项非常复杂且高成本的任务。在典型的PKI中,CA仅在制造和维修设施时可用,因而每当需要新证书时,要求每个设备以实物交付到或安全连接到安全设施会使设备生命周期变复杂。因此,需要一种简单且低成本的用于颁发设备证书的构件,这些设备证书不限于制造和维修设施。

[0006] 因此,需要提供解决上文确定的问题中的至少一些问题的方法和装置。

发明内容

[0007] 本发明的目标是提供简单且低成本的为大量设备颁发设备证书的装置和方法,其中,证书创建不限于制造和维修设施。该目的由独立权利要求的主题来解决。更多有利修改可以在附属权利要求中找到。

[0008] 根据本发明第一方面,上述和更多目标和优点通过包括处理器和存储器的装置获得,其中,所述处理器和所述存储器用于提供安全执行环境,所述存储器存储硬件唯一密钥

和层级密钥。所述处理器用于在所述安全执行环境中基于所述层级密钥恢复证书签名密钥,其中,所述证书签名密钥与证书颁发中心相关联。所述处理器基于所述硬件唯一密钥导出设备密钥对,其中,所述设备密钥对包括设备公钥和设备私钥;以及基于所述设备公钥和所述证书签名密钥生成设备证书。所述生成的设备证书配置为基于与所述证书颁发中心相关联的公钥进行验证。所公开实施例的各方面提供了一种简单且低成本的颁发设备证书的构件,这些构件不限于制造和维修设施。

[0009] 根据所述第一方面,在所述装置的第一可能实施形式中,所述处理器用于基于所述设备公钥和所述设备私钥生成证书签名请求,并且基于所述证书签名请求和所述证书签名密钥生成所述设备证书。这样可以将可信CSR并入到新型证书生成和注册装置中。

[0010] 根据如上所述第一方面或根据所述第一方面的所述第一可能实施形式,在所述装置的第二可能实施形式中,所述存储器包括层级多样化值,以及所述处理器用于基于所述层级密钥和所述层级多样化值恢复所述证书签名密钥。这样有助于通过更新所述层级多样化值以及基于所述更新后的层级多样化值生成新的证书,将所述装置从与一个CA相关联的一个PKI转移至不同的CA或不同的PKI。

[0011] 根据如上所述第一方面或根据所述第一方面的所述第一或第二可能实施形式,在所述装置的第三可能实施形式中,所述存储器包括设备多样化值,以及所述处理器用于基于所述硬件唯一密钥和所述设备多样化值导出所述设备密钥对。这样会使所述设备密钥对发生改变,而且因为所述设备多样化值不是保密的,所以可以在不用将所述装置返回到制造或维修设施的情况下改变所述设备密钥对。

[0012] 根据如上所述第一方面或根据所述第三可能实施形式,在所述装置的第四可能实施形式中,所述处理器用于:更新所述设备多样化值;基于所述硬件唯一密钥和所述更新后的设备多样化值导出设备密钥对,其中,所述更新后的设备密钥对包括更新后的设备公钥和更新后的设备私钥;以及基于所述更新后的设备公钥和所述证书签名密钥生成更新后的设备证书。所述更新后的设备证书的优点是在注册在所述CA的所述PKI中的证书中公开了新的设备公钥。

[0013] 根据如上所述第一方面或根据所述第一方面的所述第二至第四可能实施形式,在所述装置的第五可能实施形式中,所述处理器用于:更新所述层级多样化值;基于所述更新后的层级多样化值和所述层级密钥恢复更新后的证书签名密钥,其中,所述更新后的证书签名密钥与第二证书颁发中心相关联;以及基于所述更新后的证书签名密钥生成更新后的设备证书,其中,所述更新后的设备证书用于基于与所述第二证书颁发中心相关联的公钥进行验证。这样可以通过更新公共值来生成在与第二CA相关联的PKI中注册的设备证书,该操作可以在不用将所述装置返回到制造或维修设施的情况下完成。

[0014] 根据如上所述第一方面或根据所述第一方面的任意前述可能实施形式,在所述装置的第六可能实施形式中,所述证书签名密钥基于白盒解密进行恢复。白盒解密的使用简化了对安全存储器的安全要求。

[0015] 根据如上所述第一方面或根据所述第一方面的任意前述可能实施形式,在所述装置的第七可能实施形式中,所述设备密钥对基于白盒解密来导出。白盒解密的使用简化了对安全存储器的安全要求。

[0016] 根据如上所述第一方面或根据所述第一方面的任意前述可能实施形式,在所述装

置的第八可能实施形式中，所述装置为移动电话或移动计算设备。由于移动设备在全球制造和部署，所述移动设备特别适合借鉴本文所公开的分布式证书注册。

[0017] 根据本发明第二方面，上述和更多目标和优点通过包括耦合到存储器和硬件安全设备的处理器的装置获得，其中，所述处理器和所述存储器用于提供安全执行环境。所述处理器用于在所述安全执行环境中从所述硬件安全设备接收证书签名密钥，其中，所述证书签名密钥与证书颁发中心相关联；所述处理器基于设备私钥导出设备密钥对，其中，所述设备密钥对包括设备公钥和所述设备私钥；所述处理器基于设备公钥和所述证书签名密钥生成设备证书，其中，所述设备证书配置为基于与证书颁发中心相关联的公钥进行验证。所述硬件安全设备的使用提供了一种保护和分发所述机密层级密钥的替代方式。

[0018] 根据所述第二方面，在所述装置的在第一可能实施形式中，所述处理器用于在所述安全执行环境中从所述硬件安全设备接收所述设备私钥。所述硬件安全设备的使用提供了一种保护和分发所述设备私钥的替代方式。

[0019] 根据本发明第三方面，上述和更多目标和优点通过包括处理器和存储器的装置获得，其中，所述处理器和所述存储器用于提供安全执行环境。所述存储器存储硬件唯一密钥和共享密钥。所述处理器用于在所述安全执行环境中基于所述硬件唯一密钥导出设备密钥对。所述设备密钥对包括设备公钥和设备私钥。所述处理器基于所述设备公钥和所述设备私钥生成证书签名请求，基于所述共享密钥导出消息认证码密钥，以及基于所述消息认证码密钥和所述证书签名请求生成消息认证码。所述处理器向证书颁发中心传输所述证书签名请求和所述消息认证码，并且从所述证书颁发中心接收设备证书。所述设备证书配置为基于与所述证书颁发中心相关联的公钥进行验证。

[0020] 根据本发明第四方面，上述和更多目标和优点通过一种生成在装置的安全执行环境中执行的设备证书的方法来获得。所述方法包括：基于层级密钥恢复证书签名密钥，其中，所述证书签名密钥与证书颁发中心相关联；以及基于硬件唯一密钥导出设备密钥对，其中，所述设备密钥对包括设备公钥和设备私钥。所述方法包括：基于所述设备公钥和所述证书签名密钥生成设备证书，其中，所述设备证书配置为基于与所述证书颁发中心相关联的公钥进行验证。所公开实施例的各方面提供了一种简单且低成本的颁发设备证书的构件，这些构件不限于制造和维修设施。

[0021] 根据所述第三方面，在所述方法的第一实施形式中，所述证书签名密钥基于所述层级密钥和层级多样化值进行恢复。这样有助于通过更新所述层级多样化值以及基于所述更新后的层级多样化值生成新的证书，将所述装置从与一个CA相关联的一个PKI转移至不同的CA或不同的PKI。

[0022] 根据如上所述第三方面或根据所述第三方面的所述第一实施形式，在第二可能实施形式中，所述设备密钥对基于所述硬件唯一密钥和设备多样化值来导出。这样会使所述设备密钥对发生改变，而且因为所述设备多样化值不是保密的，所以可以在不用将所述装置返回到制造或维修设施的情况下改变所述设备密钥对。

[0023] 根据如上所述第三方面或根据所述第三方面的所述第一或第二可能实施方式，在第三可能实施形式中，所述方法包括：基于所述设备公钥和所述设备私钥生成证书签名请求，以及基于所述证书签名请求和所述证书签名密钥生成所述设备证书。这样可以将可信CSR并入到新型证书生成和注册装置中。

[0024] 根据本发明第五四方面，上述和更多目标和优点通过一种生成在装置的安全执行环境中执行的设备证书的方法来获得。所述方法包括：从硬件安全设备接收证书签名密钥，其中，所述证书签名密钥与证书颁发中心相关联；以及基于硬件唯一密钥导出设备密钥对，其中，所述设备密钥对包括设备公钥和设备私钥。然后，基于所述设备公钥和所述证书签名密钥生成设备证书。所述设备证书配置为基于与所述证书颁发中心相关联的公钥进行验证。所公开实施例的各方面提供了一种简单且低成本的颁发设备证书的构件，这些构件不限于制造和维修设施，进而提供了保护硬件安全设备内的机密密钥材料的安全性。

[0025] 根据本发明第六方面，上述和更多目标和优点通过一种生成在装置的安全执行环境中执行的设备证书的方法来获得。所述方法始于：基于硬件唯一密钥导出设备密钥对，其中，所述设备密钥对包括设备公钥和设备私钥。然后，基于所述设备公钥和所述设备私钥生成证书签名请求，以及基于共享密钥导出消息认证码密钥。然后，使用所述消息认证码密钥生成与所述证书签名请求相关联的消息认证码，以及向证书颁发中心传输所述证书签名请求和所述消息认证码。从所述证书颁发中心接收设备证书，其中，所述设备证书配置为基于与所述证书颁发中心相关联的公钥进行验证。所公开实施例的各方面提供了一种简单且低成本的颁发设备证书的构件，这些构件不限于制造和维修设施。

[0026] 根据本发明第七方面，上述和更多目标和优点通过一种计算机程序来获得，所述计算机程序包括非瞬时性计算机程序指令，当所述指令由处理器执行时，所述指令使得所述处理器执行根据所述第四至第六方面中任意方面所述的方法。

[0027] 根据本发明第八方面，上述和更多目标和优点通过在包括存储器的装置中使用的处理器来获得。所述处理器和所述存储器用于提供安全执行环境，所述存储器存储硬件唯一密钥和层级密钥。所述处理器用于在所述安全执行环境中基于所述层级密钥恢复证书签名密钥，其中，所述证书签名密钥与证书颁发中心相关联。所述处理器基于所述硬件唯一密钥导出设备密钥对，其中，所述设备密钥对包括设备公钥和设备私钥。然后，所述处理器基于所述设备公钥和所述证书签名密钥生成设备证书。所述设备证书配置为基于与所述证书颁发中心相关联的公钥进行验证。所公开实施例的各方面提供了一种简单且低成本的颁发设备证书的构件，这些构件不限于制造和维修设施。

[0028] 根据本发明第九方面，上述和更多目标和优点通过在包括存储器的装置中使用的处理器来获得。所述处理器和所述存储器用于提供安全执行环境，以及所述存储器存储硬件唯一密钥。硬件安全设备耦合到所述处理器，以及所述处理器用于在所述安全执行环境中从所述硬件安全设备接收证书签名密钥，其中，所述证书签名密钥与证书颁发中心相关联。所述处理器基于所述硬件唯一密钥导出设备密钥对，其中，所述设备密钥对包括设备公钥和所述设备私钥。然后，所述处理器基于所述设备公钥和所述证书签名密钥生成设备证书，其中，所述设备证书配置为基于与所述证书颁发中心相关联的公钥进行验证。所公开实施例的各方面提供了一种简单且低成本的颁发设备证书的构件，这些构件不限于制造和维修设施。

[0029] 根据本发明第十方面，上述和更多目标和优点通过在包括存储器的装置中使用的处理器来获得。所述处理器和所述存储器用于提供安全执行环境，以及所述存储器存储硬件唯一密钥和共享密钥。所述处理器用于在所述安全执行环境中基于所述硬件唯一密钥导出设备密钥对，其中，所述设备密钥对包括设备公钥和设备私钥。然后，所述处理器基于所

述设备公钥和所述设备私钥生成证书签名请求，基于所述共享密钥导出消息认证码密钥，以及基于所述消息认证码密钥和所述证书签名请求生成消息认证码。所述处理器向证书颁发中心传输所述证书签名请求和所述消息认证码，以及从所述证书颁发中心接收设备证书，其中，所述设备证书用于基于与证书颁发中心相关联的公钥进行验证。所公开实施例的各方面提供了一种简单且低成本的颁发设备证书的构件，这些构件不限于制造和维修设施。

附图说明

[0030] 在本公开内容的以下详述部分中，将参看附图中所示的示例性实施例来更详细地解释本发明，其中：

[0031] 图1所示为根据所公开实施例各方面的示例性装置的框图，该装置用于生成自身可信设备证书；

[0032] 图2所示为根据所公开实施例各方面的用于在内部生成设备密钥对和证书签名请求的装置的示例性实施例的框图；

[0033] 图3所示为并入所公开实施例各方面的用于提供安全执行环境的示例性计算装置的框图；

[0034] 图4所示为根据一项实施例的用于生成设备证书的示例性方法的流程图；

[0035] 图5所示为根据一项实施例的用于生成设备证书的示例性方法的流程图；

[0036] 图6所示为根据一项实施例的示出用于从证书颁发中心获得设备证书的示例性方法的流程图。

具体实施方式

[0037] 图1所示为示例性装置100的框图，该装置用于生成其自己的可信设备证书122，其中，内部生成并签署的设备证书122可以基于来自相关联证书颁发中心150的公钥进行验证。所公开实施例的各方面用于提供安全执行环境(secure execution environment，SEE)124，SEE 124可以保护已存储的和/或在SEE 124内执行的数据和程序的机密性和完整性。

[0038] 参照图1，装置100包括处理器102和存储器104。根据所公开实施例的各方面，处理器102和存储器104用于提供安全执行环境124。在图1的示例中，存储器104包括硬件唯一密钥108和层级密钥106。

[0039] 处理器102用于在安全执行环境124中基于层级密钥106恢复证书签名密钥116。证书签名密钥116与证书颁发中心(certificate authority，CA)150相关联。处理器102用于基于硬件唯一密钥108导出设备密钥对112。设备密钥对112包括设备公钥114和设备私钥。处理器102还用于基于设备公钥114和证书签名密钥116生成设备证书122，其中，设备证书122配置为基于与证书颁发中心150相关联的公钥154进行验证。

[0040] 在图1的示例中，SEE 124提供了包括连接到存储器104的处理器102的计算环境。存储器104用于存储数据和程序指令，程序指令在由处理器102执行时使得处理器生成设备证书122。SEE 124可以实现为单独的硬件设备，例如安全实体(secure entity，SE)或用于根据需要提供编程、电磁和/或物理安全性的其它合适的硬件安全设备。

[0041] 适当的SEE 124的一个示例可以是安谋控股公司(ARM Holdings plc)提供的

CryptoCell™硬件技术。可选地,SEE 124可以由计算装置100中的主处理器102和存储器104的安全部分提供,计算装置100包括:移动电话或其它移动或固定计算设备,配置为包括可信执行环境(trusted execution environment,TEE)或其它适当SEE。在某些实施例中,SEE 124可以将安全文件系统并入到用户空间(FUSE™)中。在某些实施例中,将(计算机)存储器104的一部分配置为安全存储区域126是有利的,安全存储区域126用于保护存储在安全存储区域126中的密钥材料的机密性。

[0042] 安全存储区域126,在本文中也称为安全存储器126,可以是实体和电子安全类型的非易失性或电池备份的计算机存储器。合适的安全存储器126的示例是在某些可信执行环境中使用的一次性可编程(one-time programmable,OTP)存储器。

[0043] 计算装置100包括一种机制,在该机制中,通常由证书颁发中心150执行的颁发设备证书等操作可以委托或分发给包括适当安全SEE 124的终端用户实体。该机制基于装置100的能力来获得访问相关联CA 150所使用的证书签名密钥152的权限并来签署该装置自己的设备证书122。

[0044] 在某些实施例中,希望SEE 124,即SEE 124内运行在处理器102上的软件应用程序,用于仅为其自身签署设备证书122,并且不使用证书签名密钥116来为其它设备或为任何其它目的颁发设备证书。基于这一原因,SEE 124应该验证并入到设备证书122中的主体名称(subject name,SN)或设备标识等主体信息与装置100自己的唯一SN或设备标识或者专属于特定装置100的其它信息匹配。在SEE 124是TEE等通用计算装置的一部分的实施例中,重要的是证书签名密钥116向在丰富的执行环境或用户空间中执行的应用程序隐藏,并且受限于在SEE 124中执行的可信应用程序,而且可以在需要时仅受限于用于签署装置100自己的设备证书122。

[0045] 证书签名密钥116和设备密钥对112中的私钥部分是敏感的机密值。在某些实施例中,需要使用硬件安全设备来保护这些值。可选地,可以使用白盒密码技术。在白盒技术中,证书签名密钥116和/或设备私钥以编码形式存储,并且只有SEE 124能够解密存储的密文来恢复机密密钥材料。又或者,将在下面更详细描述如何存储层级密钥106和/或硬件唯一密钥(hardware unique key,HUK)108等隐藏的种子值,并使用专有密钥导出过程来恢复证书签名密钥116和/或设备密钥对112。

[0046] 在从机密数据导出或恢复证书签名密钥116和设备密钥对112(可选)的实施例中,当制造或配置装置100时,将机密数据安全地加载到装置100的安全存储器126中。该机密数据包括硬件唯一密钥108和层级密钥106,这两个密钥为可用于导出或恢复Rivest™、Shamir™、Adleman™(Rivest™,Shamir™,Adleman™,RSA)型加密密钥或椭圆曲线密码(elliptic curve cryptography,ECC)密钥或者其它适当的非对称或对称加密密钥等加密密钥的密钥材料。如将在下面进一步讨论的那样,将HUK 108和层级密钥106用作密钥导出过程中的密钥材料,并且它们本身就可以是完全成形的加密密钥,或者可以是可以导出适当强度的加密密钥的任何适当的密钥材料。

[0047] 如本文所使用的那样,术语制造环境和制造时间是指制造并将包括在SEE 124中运行的应用程序的机密数据加载到装置100等装置的安全环境。制造时间包括制造装置100时使用的部件或芯片组的制造时间。这些芯片组,有时称为片上系统(system on chip,SoC),通常包括适合用作安全存储器126的一次性可编程(one-time programmable,OTP)存

储器。如本文所使用的那样，配置是将机密数据和应用程序加载到SEE 126中的过程，并且可以在制造中或之后完成。然而，如本文所使用的那样，在制造和配置之间不作区分，并且这两个术语在本文中可互换使用，以指代能够将数据和程序代码安全地加载到SEE 124中的时间或环境。

[0048] 处理器102用于基于HUK 108和设备多样化值110(可选)导出设备密钥对112。设备多样化值110是用于增加HUK 108密钥材料多样性的密码盐并且是一个公共值，该公共值可以根据需要在装置100的生命周期中更新，使得装置100根据需要在装置100的整个生命周期中生成新的设备密钥对112和新的设备证书122。例如，当装置100的所有权或安全角色改变时，可能需要改变设备密钥对112。设备多样化值110可以是一个公共值，使得改变设备密钥对112而不用将设备返回到安全设施或不用建立与安全设施的安全通信。

[0049] 从设备密钥对112中提取设备公钥114以用作装置100的设备公钥114。该公钥114根据需要与主体信息、安全策略和安全角色等其它信息一起并入到证书签名请求(certificate signing request,CSR)120中。CSR 120应该包括唯一标识装置100的信息，例如可以包括在配置期间分配给设备的唯一设备标识的主体名称。然后，处理器102可以在需要防止装置100为其它可能的恶意设备颁发证书的实施例中验证CSR属于主题设备。

[0050] CSR 120可以是任何合适类型的CSR 120，例如使用设备密钥对112中的私钥来签名的公钥密码系统标准10号(PKCS#10)型CSR。可选地，由于CSR 120绝不会脱离SEE 124，因此某些实施例可以跳过对CSR 120的签名。CSR 120包括待并入到设备证书122中的数据，并且可以以任何合适的格式来配置，并且不需要遵循任何业界标准或进行加密签名。

[0051] 在传统密码体制中，向可信CA 150提供CSR 120来获得在PKI中注册的设备证书。然而，建立与CA的安全通信链路并获得设备证书122会明显使设备证书122的创建和配置变得复杂，时间延长。为了避免发生与使用单独的CA 150为每个装置100颁发设备证书122的传统过程相关联的问题，所公开实施例可以有利地用于将设备证书122的生成委托或分发给每个终端用户节点，使装置100能够颁发其自己的设备证书122。通过配置装置100来完成证书生成的委托，从而基于层级密钥106和层级多样化值118(可选)来恢复证书签名密钥116，其中，证书签名密钥116与CA 150用来颁发设备证书的证书签名密钥152相同。

[0052] 在某些实施例中，需要在整类或整组设备中使用相同的层级密钥106和/或相同的层级多样化值118，从而使得具有相同层级密钥106和层级多样化值118的所有装置100能够注册在同一个PKI中。例如，由特定手机公司出售的所有手机都可以具有相同的层级密钥106和层级多样化值118。可选地，某个地理位置或其它合适的组中的所有装置100都可以配置有相同的层级密钥106和层级多样化值118。

[0053] 一旦恢复证书签名密钥116并验证CSR 120，就使用恢复后的证书签名密钥116来生成并签署并入CSR 120中的公钥114和其它信息的设备证书122。由于证书签名密钥116与相关联CA 150使用的证书签名密钥152相同，所以CA 150可以在设备证书122中指示为证书颁发中心。因此，设备证书122自动注册在CA 150的PKI中，并且可以被能够建立与CA 150的信任关系的任何实体所信任。

[0054] 在SEE 124中生成可信设备证书122使得装置100在PKI中注册而无需建立与CA的安全通信且无需将设备返回给安全设施或无需创建与CA 150的安全连接。如上所述的分发CA能力使得装置100等设备颁发它们自己的设备证书122，从而明显降低了创建和注册设备

证书的成本和复杂度。

[0055] 验证CSR 120、恢复证书签名密钥116以及颁发设备证书122的所有操作都应该在单个安全服务内自动完成，以保证攻击者无法窃听证书签名密钥116或颁发非有意设备证书122。在某些实施例中，需要注意确保证书签名密钥116绝对不会存储在装置100中并且在使用之后被立即丢弃。将用于恢复证书签名密钥116的功能或过程限制在用于生成设备证书122并确保设备证书122绝不会分发在任何地方的可信应用中，也可能是一种很好的安全实践。

[0056] SEE 124用于使用密钥导出函数(key derivation function，KDF)从密钥材料和盐中导出非对称密钥对。HUK 108提供密钥材料，设备多样化值110提供用于导出设备密钥对112的盐，而层级密钥106提供密钥材料，层级多样化值118提供用于恢复证书签名密钥116的盐。可以通过先使用散列消息认证码(hashed message authentication code，HMAC)算法与256位安全散列算法(256bit secure hash algorithm，SHA-256)等散列算法一起从盐和密钥材料中获得密钥值(通常表示为r)，从而从密钥材料和盐值中导出非对称ECC型密钥。然后，将密钥值r转换为ECC整数证书私钥。可以通过将整数私钥乘以G来获得相关联的公钥，其中G是所选椭圆曲线的基点。可选地，可以使用任何适当的KDF，例如传统公钥密码系统标准(public key cryptography standard，PKCS)中定义的基于密码的密钥导出函数2(password based key derivation function number 2，PBKDS2)，来获得密钥值r。可选地，产生RSA型加密密钥的KDF可以有利地用于示例性装置100中。

[0057] 本领域技术人员将容易认识到，用于导出设备密钥对112的密钥导出过程可能与用于导出证书签名密钥116的密钥导出过程不同，并且设备密钥对112可以在不偏离所公开实施例的精神和范围的情况下基于不同于证书签名密钥的加密算法。例如，在一项实施例中，设备密钥对112可以使用ECC，而证书签名密钥可以使用RSA算法，反之亦然。

[0058] 在装置100的整个生命周期中，可能需要更新设备证书122和/或将装置与属于不同PKI的不同CA 160相关联。为了实现这一点，可以更新层级多样化值118，从而产生不同的证书签名密钥116。由于层级多样化值118是一个公共值，因此将该设备返回到安全设施对于更新层级多样化值118是不必要的。通过选择新的层级多样化值118，使得得到的证书签名密钥116对应于与第二CA 160相关联的证书签名密钥162，使用新证书签名密钥116签署的设备证书122与第二CA 160相关联，并且可以使用对应于第二CA 160的公钥164进行验证。类似地，可以通过更新设备多样化值110来改变设备密钥对112。

[0059] 图2示出了用于在内部生成设备密钥对114和CSR 120并从CA 150接收设备证书122的装置200的示例性实施例的框图。装置200与上面描述的装置100类似，并且包括耦合到存储器104的处理器102，其中，存储器具有安全存储器部分126，处理器102和存储器104用于提供SEE 124。相比于上面描述的在SEE 124内生成设备证书122的装置100，装置200将设备证书122的生成和签署委托给外部CA 150。

[0060] 装置200中的处理器102基于设备多样化值110和HUK 108使用合适的KDF来导出设备密钥对112。处理器102从设备密钥对112中提取公钥114，并根据需要将公钥112与主题信息和其它数据一起并入到CSR中。如上所述，CSR的格式可以是任何合适的格式，例如PKCS#10。然而，在某些实施例中，优选对CSR 120进行数字签名才能将CSR 120传输到SEE 124之外。然后，可以将签名后的CSR 120传输到任何期望的CA 150。

[0061] 当SEE 124和CA 150之间的通信信道不能获得充分保障或者当安全策略要求时，需要在将CSR 120传送到CA 150时对CSR 120进行加密保护。为此，当配置装置200时，将共享密钥202加载到安全存储器126中。共享密钥202可以是一个完全成形的加密密钥，或者可以是可以导出合适的加密密钥的任何适当的密钥材料。通过使用任何合适的KDF从共享密钥202恢复消息认证码(message authentication code，MAC)密钥204，MAC 204可以是对称密钥或秘密密钥且用于生成MAC 206，其中MAC 206与CSR 120一起发送到CA 150。CA 150能够获得访问用于生成MAC 206的同一MAC密钥204的权限，并且可以使用MAC密钥204来验证CSR 120。CA 150将CSR 120中的信息并入到设备证书122中，并使用自身的证书签名密钥152签署设备证书122。然后，可以将设备证书122发回装置200。

[0062] MAC密钥204的恢复和MAC 206的生成基于恢复后的MAC 206启用CA 150与SEE 124之间的安全信道。该安全信道确保只有特别定制的CA 150才可以提供设备证书122。为了提高安全性，CA 150的部署应尽可能靠近设施中的装置200，装置200在该设施中制造。

[0063] 图3所示为示例性计算装置300的框图，该计算装置300用于提供适合于用作上面结合图1和图2描述的SEE 124的SEE 324。计算装置300可以并入到各类移动电话、平板手机、平板电脑、膝上型电脑、机顶盒、电视机、汽车等计算装置中，并且可以有利地用于提供分布式CA功能以加强计算设备300的制造和维护。计算装置300用于提供SEE 324和丰富执行环境(rich execution environment，REE)330。

[0064] REE 330用于提供广泛的功能和特征以支持各种各样的应用并提供良好用户体验。然而，REE 330本质上没有SEE 324安全，并且无法在没有丢失加密密钥和数据的机密性或完整性的情况下安全地执行加密操作。丰富执行环境的示例是由GOOGLE TM开发的Android操作系统(operating systems，OS)和PPLE™开发的iOS等移动OS提供的那些环境。在某些实施例中，可能不需要REE(330)，并且本领域技术人员将容易认识到，在不偏离本发明的精神和范围的情况下，计算装置300可用于提供SEE 324而不是提供相关联的REE 330。

[0065] 在图3的示例中，计算装置300包括耦合到存储器312的处理器310，其中，处理器302的第一部分和存储器304的第一部分用于支持SEE 324。处理器306的第二部分和存储器308的第二部分用于支持REE 330。

[0066] 处理器310可以是单个处理设备或可包括多个处理设备，包括专用设备，例如数字信号处理(digital signal processing，DSP)设备、微处理器、专用处理设备、并行处理核或通用计算机处理器。处理器310用于从存储器312读取程序指令并且执行本文描述的方法和过程。处理器还可以包括与可以与图形处理单元(graphics processing unit，GPU)协作的CPU，该GPU包括DSP或其它专用图形处理硬件。

[0067] 处理器312可以是各种类型的易失性和非易失性计算机存储器的组合，例如，只读存储器(read only memory，ROM)、随机存取存储器(random access memory，RAM)、磁盘或光盘，或其它类型的计算机存储器。存储器304的安全部分可以包括用于保护机密数据的一次性可编程存储器。存储器312存储可由处理器310访问和执行的计算机程序指令，使得处理器执行各种期望的计算机实现过程或方法，例如分布式CA操作或本文描述的其它加密方法。

[0068] SEE 324用于确保存储在SEE存储器304内的数据和计算机程序的机密性和完整性，并且保护在处理器302的安全部分内执行的计算机程序。SEE 324可以使用可信执行环

境(trusted execution environment,TEE)等各种技术或用于在计算设备300内提供REE 330和SEE 324的其它合适技术来实现。在某些实施例中,可能需要使用单独的硬件安全设备326或SE等其它物理安全处理装置来保护敏感密钥材料或其它敏感加密数据。在某些实施例中,硬件安全设备326的使用可能需要基于由特定使用或应用强加的安全和其它要求。

[0069] 为了维持SEE 324与REE 330之间的安全边界,仅允许处理器306的REE部分访问318存储器308的REE部分。SEE 324是安全环境,还允许处理器302的SEE部分访问存储器308的REE部分并且访问314存储器304的SEE部分或安全部分。在使用HSD 326的实施例中,允许处理器302的SEE部分访问HSD 326,但是需要防止处理器306的REE部分访问HSD 326。

[0070] 参考图4,可以看到用于为计算设备生成设备证书的示例性方法400的流程图。示例性方法400可以有利地用于任何计算设备中,该计算机设备用于提供SEE,其中,SEE用于保证加载到SEE内部的数据和代码在保密性和完整性方面受到保护。例如,上面结合图3描述的计算设备300和上面结合图1描述的装置100为执行方法400提供了合适的安全环境。本文公开的装置实施例的原理和过程同样适用于图4至6中公开的以及下面描述的方法。

[0071] 方法400在其中执行的SEE或设备加载402有机密数据和其它种子数据。种子数据可以在制造或配置设备时加载402,并且应当进行保密,例如存储在安全存储器中。种子数据中包括HUK和层级密钥。HUK是专用于上面描述的HUK 108等特定设备或SEE的机密密钥材料,层级密钥是特定类或组中所有设备已知的机密密钥材料,并且可以是上面描述的层级密钥106等任何合适的层级密钥。层级密钥允许某个类中的所有设备恢复相同的证书签名密钥,其中该类可以是任何期望的设备分组,例如通过设备类型、为设备提供服务的公司、地理位置等。在某些实施例中,将设备标识加载到唯一标识方法400在其中执行的设备或SEE的SEE中是有利的。设备标识可以用于防止对未经授权的设备颁发设备证书,等等。

[0072] 证书签名密钥基于层级密钥进行恢复404。恢复后的证书签名密钥与相关联CA使用的证书签名密钥相同,并且是属于相关联CA的非对称密钥对中的私有部分。因此,使用恢复404后的证书签名密钥签署的设备证书可以被任何实体所信任,这些实体可建立与相关联CA的信任关系,并且这样签署的设备证书可以视为自动注册在相关联CA的PKI中。恢复404后的证书签名密钥可以是适合于签署设备证书的任何适当类型的非对称密钥。

[0073] 基于加载402到SEE中的HUK导出406设备密钥对。在某些实施例中,可能需要在导出404设备密钥对时添加设备标识,从而将密钥对绑定到特定的设备标识。当使用唯一的设备标识时,将设备标识绑定到特定装置或计算设备并且在颁发设备证书之前验证该设备标识通常是有益的。设备密钥对包括设备私钥和设备公钥,在许多实施例中,设备私钥保密在SEE内,而设备公钥公开在设备证书中。

[0074] 方法400基于设备密钥对和与特定设备相关的其它识别主体信息,例如设备标识,来生成408证书签名请求(certificate signing request,CSR)。当采用已签名的CSR格式(例如标准PKCS#10CSR)时,可以使用设备的私钥对CSR进行数字签名,使得验证创建CSR的设备能够获得访问非对称密钥对中的公钥和相应私钥的权限。数字签名可以使用任何期望的方法来创建,例如在公钥密码系统标准(public key cryptography standards,PKCS)中描述的方法、美国联邦信息处理标准(United States Federal Information Processing Standard,FIPS)采用的用于数字签名的数字签名算法(Digital Signature Algorithm,DSA),或用于生成适当的数字签名的任何其它期望的方法或算法。可选地,当在生成设备密

钥对的同一SEE内创建设备证书时，可能需要跳过CSR签名过程。

[0075] 然后，为主体设备生成410设备证书。设备证书，也称为数字证书，可以是传统的公钥证书，例如流行的X.509证书，也可以是适合于认证和授权使用该设备公钥的任何所需类型的公钥证书。在对设备证书进行数字签署之前，在某些实施例中，需要验证并入到设备证书中的设备ID和与SEE相关联的设备ID匹配。该验证步骤防止SEE为可能未被相关联CA授权的其它设备颁发证书。在某些实施例中，需要将设备多样化值加载402到设备中。设备多样化值可以是一个公共值，并且可以在设备生命周期中更新。设备多样化值可以用作密码盐以增加HUK密钥材料的多样性。还允许通过改变设备多样化值以及第二次执行该方法以基于更新后的设备多样化值生成设备证书来修改设备密钥对。类似地，在证书签名密钥的恢复404期间可以加载402和使用层级多样化值。通过选择层级多样化值，使得恢复404后的证书签名密钥与新的CA相关联，可以在更新层级多样化值之后通过执行方法400将设备注册在新的CA的PKI中。

[0076] 图5所示为示出根据本发明各方面的用于生成设备证书的示例性方法500的流程图。示例性方法500可以有利地用于移动电话或其它移动计算装置等任何计算设备中，该计算设备用于提供SEE，其中该SEE用于保证加载到SEE内部的数据和代码在保密性和完整性方面受到保护。例如，上面结合图3描述的计算设备300和上面结合图1描述的装置100为执行方法500提供了合适的安全环境。

[0077] 方法500在其中执行的SEE或设备加载502有机密数据和其它种子数据。种子数据可以在制造或配置设备时加载502，并且应当进行保密，例如通过存储在安全存储器中进行保密。种子数据中包括HUK，例如上面描述的HUK 108，HUK是专用于特定设备或SEE的机密密钥材料。在某些实施例中，将设备标识加载到唯一标识方法500在其中执行的设备或SEE的SEE中是有利的。设备标识可以用于防止对未经授权的设备颁发设备证书，等等。

[0078] 从耦合到SEE并用于与SEE安全通信的硬件安全设备接收504证书签名密钥。接收到的证书签名密钥与相关联CA使用的证书签名密钥相同，并且至少包括属于相关联CA的非对称密钥对中的私有部分。因此，使用接收504到的证书签名密钥签署的设备证书可以受到任何实体的信任，这些实体可以建立与相关联CA的信任关系，并且这样签署的设备证书可以视为自动注册在相关联CA的PKI中。接收504到的证书签名密钥可以是适合于签署设备证书的任何适当类型的非对称密钥。

[0079] 设备密钥对基于加载502到SEE中的HUK来导出506。在某些实施例中，可能需要在导出504设备密钥对时添加设备标识，从而将密钥对与特定设备标识进行绑定。当使用唯一的设备标识时，将设备标识绑定到特定装置或计算设备并且在颁发设备证书之前验证该设备标识通常是有益的。设备密钥对包括设备私钥和设备公钥，在许多实施例中，设备私钥保密在SEE内，而设备公钥可以公开在设备证书中。

[0080] 方法500基于设备密钥对和与特定设备相关的其它识别主体信息，例如设备标识，来生成508CSR。当采用已签名的CSR格式(例如标准PKCS#10CSR)时，可以使用设备的私钥对CSR进行数字签名，使得验证创建CSR的设备能够获得访问对应于CSR的非对称密钥对中的公钥和相应私钥的权限。如上所述，数字签名可以使用适合于生成数字签名的任何期望的方法或算法来创建。可选地，当在生成设备密钥对的同一SEE内创建设备证书时，可能需要使用未签名的CSR，从而减少CSR创建所需的时间量和处理能力。

[0081] 然后，为主体设备生成510设备证书。如上所述，设备证书可以是适合于认证和授权使用设备公钥的任何期望类型的公钥证书。在对设备证书进行数字签署之前，在某些实施例中，需要验证并入到设备证书中的设备ID和与SEE相关联的设备ID匹配。该验证步骤防止SEE为可能未被相关联CA授权的其它设备颁发证书。

[0082] 图6所示为示出根据所公开实施例的各方面的用于从CA获得设备证书的示例性方法600的流程图。示例性方法600可以有利地用于移动电话或其它移动计算装置等各种类型的计算设备中，这些计算机设备用于提供SEE，其中，SEE用于保证SEE内部加载的数据和代码在保密性和完整性方面受到保护。例如，上面结合图3描述的计算设备300和上面结合图2描述的装置200为执行方法600提供了合适的安全环境。

[0083] 方法600在其中执行的SEE或设备加载602有机密数据和其它种子数据。种子数据可以在制造或配置设备时加载602，并且应当进行保密，例如存储在安全存储器中。种子数据中包括HUK，例如上面描述的HUK 108，HUK是专用于特定设备或SEE的机密密钥材料。在某些实施例中，将设备标识加载到唯一标识方法600在其中执行的设备或SEE的SEE中。设备标识可以用于防止对未经授权的设备颁发设备证书，等等。除HUK之外，加载602到安全存储器中的种子数据包括共享秘密值，例如上面结合图2描述的共享密钥202值。

[0084] 设备密钥对基于加载602到SEE中的HUK来导出604。在某些实施例中，可能需要在导出604设备密钥对时添加设备标识，从而将密钥对与特定设备标识进行绑定。当使用唯一的设备标识时，将设备标识绑定到特定装置或计算设备并且在颁发设备证书之前验证该设备标识通常是有益的。设备密钥对包括设备私钥和设备公钥，在许多实施例中，设备私钥保密在SEE内，而设备公钥可以公开在设备证书中。

[0085] 方法600基于设备密钥对和与特定设备相关的其它识别主体信息，例如设备标识，来生成606CSR。在方法600中，优选采用已签名的CSR格式，例如标准PKCS#10CSR，其中，可以使用设备的私钥对CSR进行数字签署，从而可以验证创建CSR的设备是否能够获得访问对应于CSR的非对称密钥对中的公钥和相应私钥的权限。如上所述，数字签名可以使用适合于生成安全加密的数字签名的任何期望的方法或算法来创建。

[0086] MAC密钥基于存储在SEE内的安全存储器中的共享密钥来导出608。根据需要，MAC密钥可以是任何适当类型的对称或非对称加密密钥。在某些实施例中，由于对称密码算法所需的处理资源减少，导出608对称密钥是有利的。然后，使用MAC密钥来生成610可由CSR的接收方(例如CA或其它预期实体)使用的MAC，从而验证CSR的完整性。

[0087] 然后，将生成606的CSR与生成610的MAC一起传输612到CA。CA能够获得访问用于导出MAC密钥的同一共享密钥的权限，从而可以在生成设备证书之前验证CSR的完整性。在某些实施例中，在传输612之前对CSR和MAC进行加密是有利的。然后，CA可以对CSR和MAC进行解密，由此确保在传输612期间CSR的机密性。CA基于CSR生成设备证书并将设备证书发回发起装置。设备证书由存储设备证书以供稍后使用的SEE接收614。通过方法600，可以为方法600在其中执行的SEE提供有效的设备证书。

[0088] 因此，尽管此处已示出、描述和指出应用于本发明的示例性实施例的本发明的基本新颖特征，但是应理解，在不脱离本发明的精神和范围的情况下，本领域技术人员可以对所所说明的设备和方法的形式和细节以及其操作做出不同省略、替代和改变。进一步地，明确希望，以大体相同的方式执行大体相同的功能以实现相同结果的那件元件的所有组合均

在本发明的范围内。此外，应认识到，结合所揭示的本发明的任何形式或实施例进行展示和/或描述的结构和/或元件可作为设计选择的通用项而并入所揭示或描述或建议的任何其它形式或实施例中。因此，本发明仅受限于随附权利要求书所述的范围。

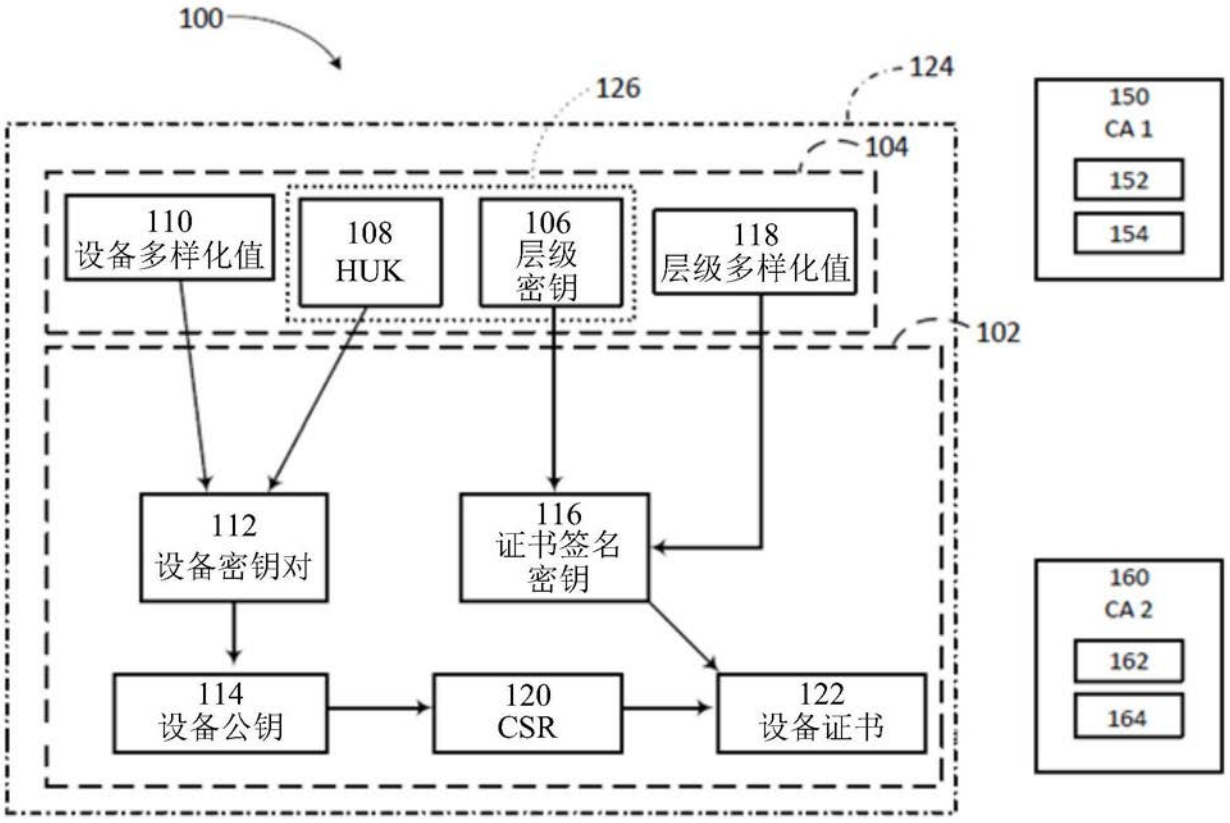

100
126
124
104
150
CA 1
152
154
110
设备多样化值
108
HUK
106
层级
密钥
118
层级多样化值
102
112
设备密钥对
116
证书签名
密钥
160
CA 2
162
164
114
设备公钥
120
CSR
122
设备证书

图1

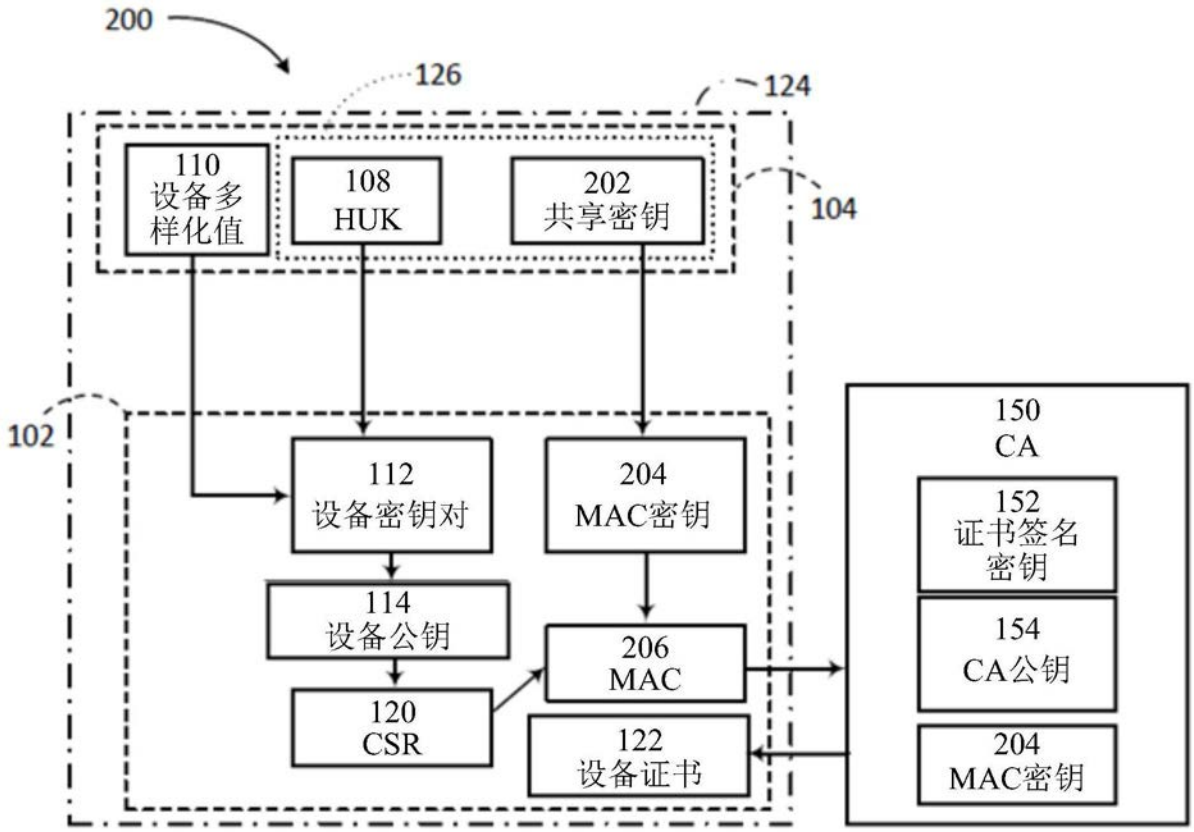

200
126
124
110
设备多
样化值
108
HUK
202
共享密钥
104
102
112
设备密钥对
204
MAC密钥
114
设备公钥
206
MAC
120
CSR
122
设备证书
150
CA
152
证书签名
密钥
154
CA公钥
204
MAC密钥

图2

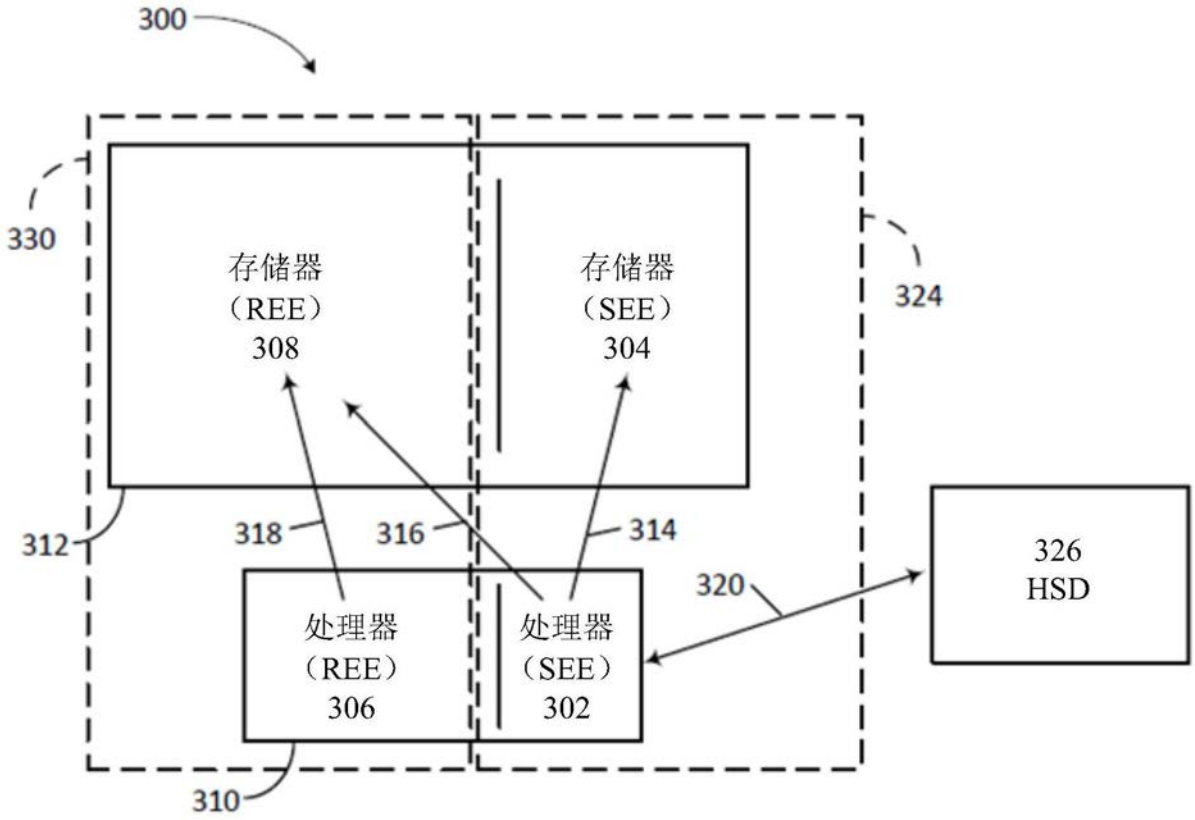

300
330
存储器
（REE）
308
存储器
（SEE）
304
324
312
318
316
314
320
326
HSD
处理器
（REE）
306
处理器
（SEE）
302
310

图3

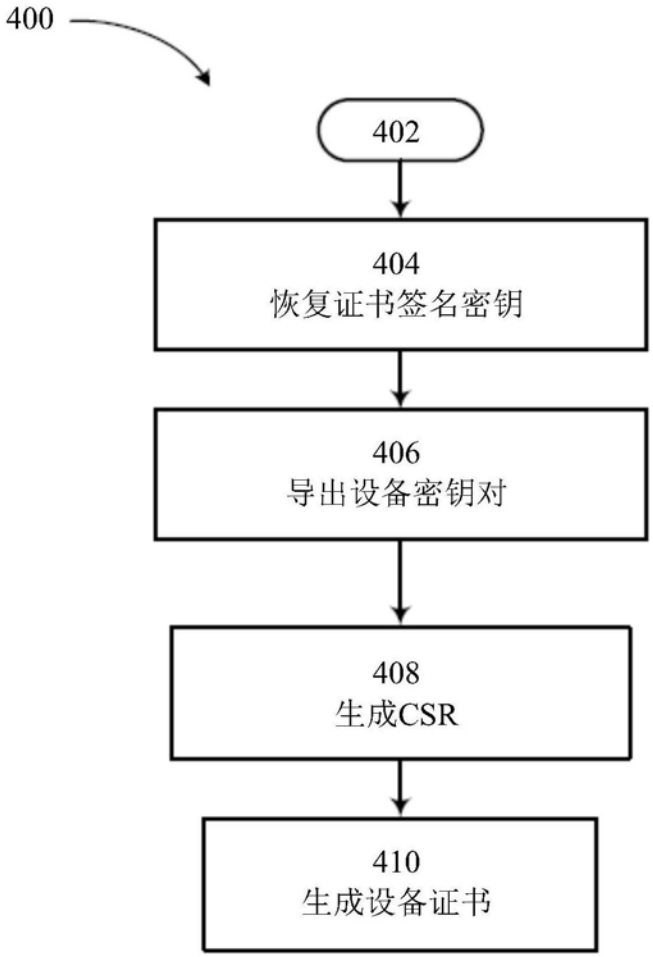


图4

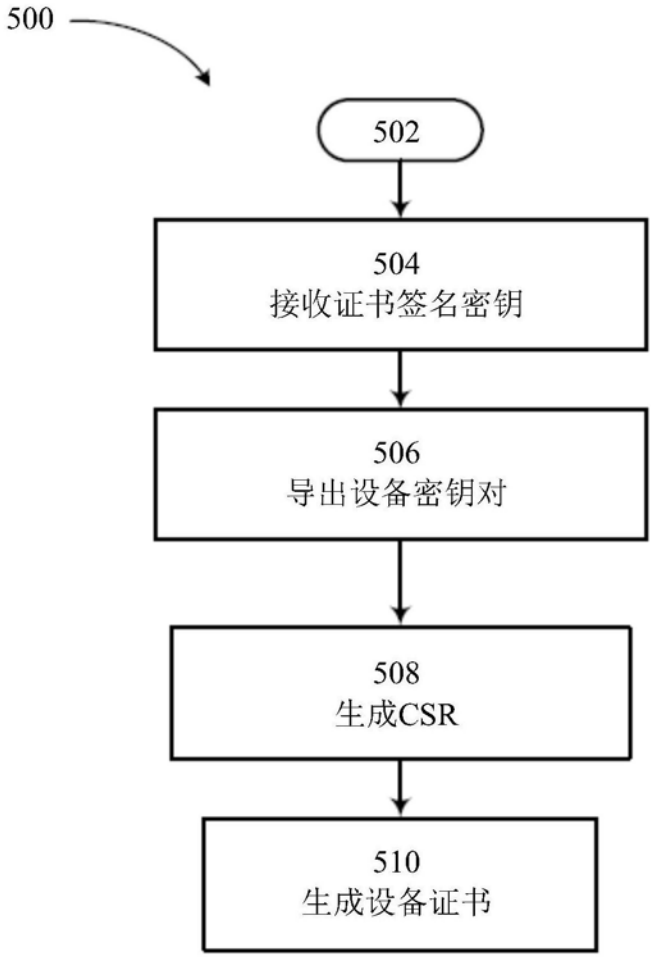


图5

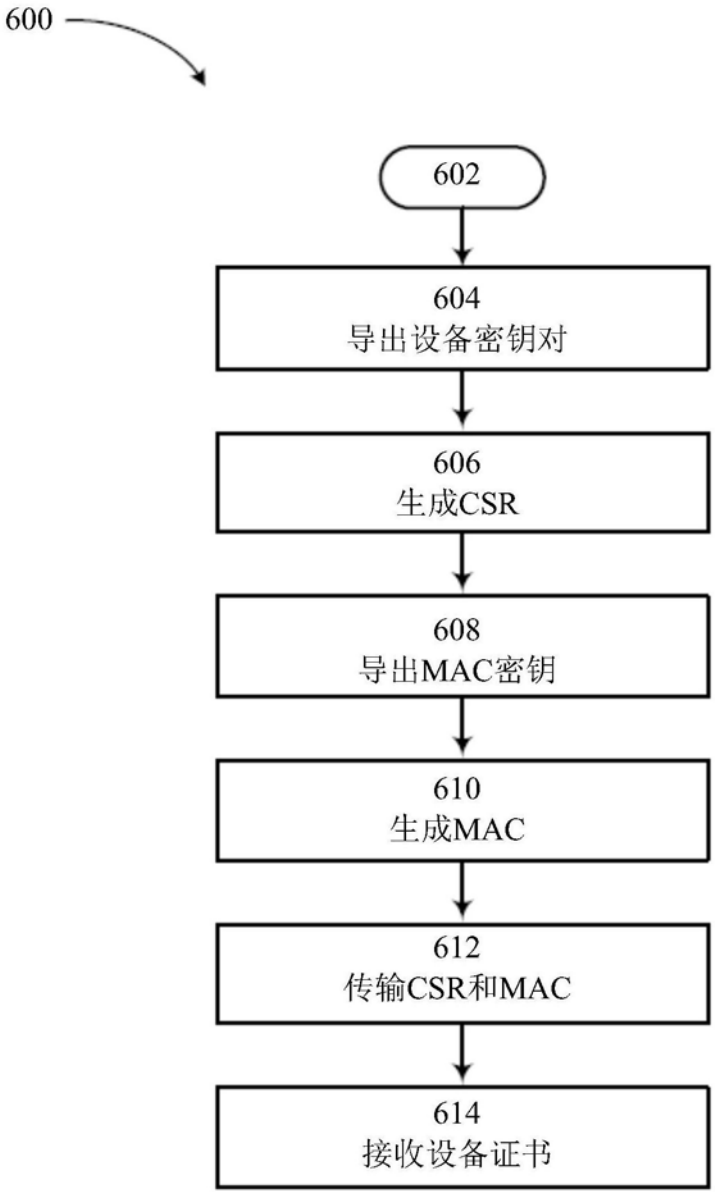

600
602
604
导出设备密钥对
606
生成CSR
608
导出MAC密钥
610
生成MAC
612
传输CSR和MAC
614
接收设备证书

图6