(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103119599 A
(43)申请公布日 2013.05.22

(21)申请号 201180044823.9
(22)申请日 2011.09.12
(30)优先权数据
61/383,993 2010.09.17 US
(85)PCT申请进入国家阶段日
2013.03.18
(86)PCT申请的申请数据
PCT/CA2011/050550 2011.09.12
(87)PCT申请的公布数据
WO2012/040840 EN 2012.04.05
(71)申请人 塞尔蒂卡姆公司
地址 加拿大安大略
(72)发明人 罗伯特·约翰·兰伯特
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 苏志莲
(51)Int.Cl.
G06F 21/34(2013.01)
G06F 21/60(2013.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)

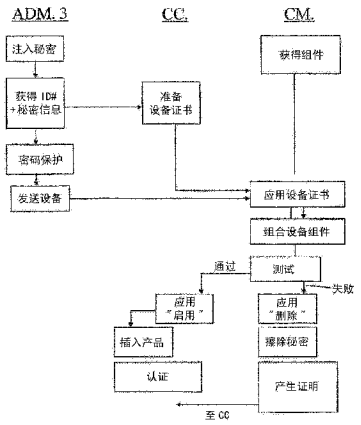
权利要求书2页 说明书5页 附图6页

(54)发明名称

用于管理认证设备生命周期的机制

(57)摘要

使用认证设备，以使用密钥来向产品认证组件。通过选择性删除密钥来控制认证设备的生命周期。认证设备在删除密钥时发送证明消息。可以使来自故障组件的认证设备或者过量供给的认证设备不可操作并被审计。



CN 103119599 A

1. 一种禁用认证设备的方法，所述认证设备具有用于向产品认证组件的密钥，所述方法包括：

发起从所述认证设备删除所述密钥，

准备指示所述密钥被删除的证明消息，

从所述认证设备删除所述密钥，以及输出所述证明消息。

2. 根据权利要求 1 所述的方法，其中，在删除所述密钥之前准备所述证明消息。

3. 根据权利要求 1 或 2 所述的方法，其中，在删除所述密钥之后输出所述证明消息。

4. 根据权利要求 1 至 3 中任一项所述的方法，其中，使用所述密钥来产生所述证明消息。

5. 根据权利要求 1 至 4 中任一项所述的方法，其中，所述密钥对指示删除所述密钥的消息起作用，以准备所述证明消息。

6. 根据权利要求 5 所述的方法，其中，所述密钥使用加密签名协议来签名所述指示删除的消息。

7. 根据权利要求 6 所述的方法，其中，所述加密签名协议是公共签名协议。

8. 根据权利要求 7 所述的方法，其中，所述证明消息包括与所述密钥相对应的公钥的证书。

9. 根据权利要求 8 所述的方法，其中，由密码的应用来发起删除所述密钥，以及指示删除的所述消息是所述密码。

10. 一种认证设备，具有实现根据权利要求 1 至 9 中任一项所述的方法的逻辑单元以及用于输出所述证明消息的通信模块。

11. 一种计算机可读介质，包括用于实现根据权利要求 1 至 9 中任一项所述的方法的计算机可执行指令。

12. 一种检验密钥的删除的方法，所述密钥用于向产品认证组件，所述方法包括：

从认证设备接收指示删除所述密钥的证明消息，以及检验所述消息。

13. 一种确定认证设备的生命周期的方法，所述认证设备具有用于向产品认证组件的密钥，所述方法包括：

在第一实体处，将所述密钥嵌入到所述认证设备中，向第二实体转发所述认证设备的标识信息和与所述密钥有关的信息，

在所述第二实体处产生设备证书，

向第三实体转发所述认证设备和所述设备证书，

所述第三实体选择性地删除所述密钥，以通过发起删除所述密钥来使所述认证设备不可操作，

所述认证设备产生证明消息，删除所述密钥，以及输出所述证明消息。

14. 根据权利要求 13 所述的方法，其中，在删除所述密钥之前准备所述证明消息。

15. 根据权利要求 13 或 14 所述的方法，其中，在删除所述密钥之后输出所述证明消息。

16. 根据权利要求 13 至 15 中任一项所述的方法，其中，使用所述密钥来产生所述证明消息。

17. 根据权利要求 13 至 16 中任一项所述的方法，其中，所述密钥对指示删除所述密钥的消息起作用，以准备所述证明消息。

18. 根据权利要求 17 所述的方法，其中，所述密钥使用加密签名协议来签名所述指示删除的消息。

19. 根据权利要求 18 所述的方法，其中，所述加密签名协议是公共签名协议。

20. 根据权利要求 19 所述的方法，其中，所述证明消息包括与所述密钥相对应的公钥的证书。

21. 根据权利要求 20 所述的方法，其中，由密码的应用来发起删除所述密钥，以及指示删除的所述消息是所述密码。

用于管理认证设备生命周期的机制

[0001] 相关申请的交叉引用

[0002] 本申请要求于 2010 年 9 月 17 日递交的美国临时申请 NO.61/383,993 的优先权，其全部内容通过引用并入本文。

技术领域

[0003] 以下涉及管理认证设备的生命周期的方法和装置。

背景技术

[0004] 很多产品并入了从各种源头获得的组件。这些组件必须具有所要求的质量和功能，并因此必须保证这些源头。在组件是整个产品的不可分割的一部分并且可影响到产品的性能和最终用户的安全的情况下，这是特别关键的。这种关键性的示例包括计算和电信设备中使用的电池、航空和运输应用中使用的机械组件、以及与医疗成像装置一起使用的医疗工具等。对伪造组件的使用可影响到性能并导致产品间接损伤的其他应用包括打印机色带盒、存储卡和摄像镜头。

附图说明

[0005] 现在将仅作为示例并参考附图来描述不同实现的实施例，其中：

[0006] 图 1 是并入具有认证设备的组件的最终用户产品的表示，

[0007] 图 2 是表示图 1 中示出的认证设备的图，

[0008] 图 3 是指示制造环境中的数据流和设备的图，

[0009] 图 4 是示出与图 3 相关联的过程的流程图，

[0010] 图 5 更详细地示出了当使用对称密钥加密协议时图 4 中示出的过程，

[0011] 图 6 是使用不对称密钥加密协议的、与图 5 相类似的流程图，以及

[0012] 图 7 是使用公钥椭圆曲线加密的、图 5 中示出的过程的特定示例。

具体实施方式

[0013] 为了确保所使用的组件来源正确，将认证设备并入到组件中。当在最终产品中使用组件时，认证设备与最终产品一起协作，以认证组件的来源。使用要求将秘密 (secret) 嵌入到认证设备中的加密协议来实现认证。

[0014] 通常，在分布式的位置中制造认证设备、组件和最终产品，这对管理秘密和认证设备提出了挑战。控制密钥的分发并审计产品量对于可能发生的大多数情况是有效的。然而，在已经并入认证设备之后，当要废弃组件时，例如当发现组件有故障时，具体的问题出现了。在该情况下，认证设备可能被从组件移除并被其他的（伪造）组件所使用，或者该组件可能作为伪造组件进入市场（虽然它不满足规范）。

[0015] 通过提供以下机制来解决以上问题：从认证设备删除在组件的认证中使用的秘密，并产生对已经删除秘密进行指示的证明消息。然后可向审计机构转发该证明消息，以说

明废弃的认证设备。秘密的删除确保了不可以使用认证设备来成功认证其他组件。

[0016] 优选地，在转发证明消息之前删除秘密，以及作为进一步的优选，证明消息使用要删除的秘密。

[0017] 可以通过基于每个设备或基于批量所提供的密码发起对证明消息的产生，并且为了防止无意间禁用组件，在并入产品后，可以关闭证明功能。

[0018] 可以将该机制与不同的加密协议（对称密钥和不对称密钥二者）一起使用。

[0019] 在通常意义上，在认证设备制造商 (ADM) 处产生用于并入到要向最终用户提供的组件中的认证设备。向组件制造商 (CM) 提供认证设备，组件制造商将认证设备与组件进行组合。然后，向缔约公司 (CC) 提供组件，以与最终产品一起使用。

[0020] 认证设备并入被用于向产品认证组件的秘密值（通常称为密钥），该认证设备拥有具有用于执行加密操作的安全存储器和逻辑单元 (LU) 的集成电路的形式。可以将与每个设备的密钥有关的信息与设备标识信息一起提供给缔约公司。该信息可以是针对于对称密钥协议的密钥，或者是针对不对称密钥协议的对应公钥。缔约公司对接收到的识别信息和针对于不对称密钥协议的认证设备公钥进行签名，以产生设备证书。设备证书在认证设备已离开认证设备制造商之后与其相关联，并被用在向产品认证组件中。

[0021] 组件制造商测试包括认证设备的组件，并且如果通过，根据需要向缔约公司或者其代理（其例如可以将组件装配到完成的产品中）提供该组件。如果设备测试失败，或者如果生产了过多的组件，组件制造商可发起确保认证设备无法被用来认证组件的废弃过程。向认证设备提供使其从其存储器中删除密钥的密码。认证设备还使用密钥来产生证明消息，指示密钥已被删除。向缔约公司或该公司的审计机构发送证明消息，审计机构检验该证明消息是使用设备密钥产生的。从而缔约公司满意于已从认证设备删除了密钥。当密钥被删除时，授权设备自身没有值，并且无法向产品认证组件。

[0022] 更具体地，参考图 1，具有电信设备形式的产品 10 具有屏幕 12、键盘 14 和补充输入设备（例如，轨迹球或轨迹板 16）。产品 10 包括未示出的通信模块，通信模块允许用户在通信信道上（无线地或基于陆地地）交换数据和信息。设备 10 可以采用很多不同的形式，并且仅出于示例性的目的提供以上细节。

[0023] 设备 10 包括电池 20，电池 20 是由组件制造商 (CM) 提供的组件。电池 20 具有固定在其上的认证设备 22，如以下将要更完整地描述的，认证设备 22 与设备 10 协作，以认证所述认证设备 22 的来源。

[0024] 从图 2 中可以更清楚地看出，认证设备 22 是包括与逻辑单元 (LU)26 接口连接的安全存储器 24 在内的集成电路。LU26 在存储器 28 中存储的非暂时性计算机可读指令的指导下或者直接通过认证设备硬件中部署的状态机来执行加密操作。取决于所实现的具体设计，安全存储器 24 可以是存储器 28 的一部分，或者与其分离。LU26 包括随机数产生器 30，随机数产生器 30 产生可被用作加密密钥或者加密算法所需的随机数 (nonce) 的数据串。通信模块 32 使认证设备与产品 10 接口连接，并且控制产品和认证设备之间的信息流。如果需要允许认证设备起作用，则包括电源 34，然而如果需要无源器件（例如，RFID 设备），可以提供外部功率。

[0025] 使用安全存储器 24 来存储表示安全值（称为密钥 d）的数据串。在图 3 中示出的认证设备制造商 (ADM) 处，密钥 d 可从随机数产生器 30 产生，或者可以在安全可控条件下

注入存储器 24 中。

[0026] ADM 参与到由组件制造商 (CM) 和缔约公司 (CC) 组成的制造组织中。ADM 的作用是制造认证设备 22，嵌入密钥 d 并向 CM 提供认证设备 22。

[0027] CM 制造组件（在所提供的示例中是电池 20），并将认证设备 22 并入到电池 20 中。然后，测试具有认证设备 22 的电池 20，并向缔约公司 CC 提供。组件的安全制造要求在 ADM、CM 和 CC 之间交换数据和物理单元。

[0028] 参考图 4，密钥 d 最初存储在安全存储器 24 中。还向每个认证设备 22 指派用于唯一地标识所制造的每个设备的标识信息（例如标识号 ID#）。当认证设备使用公钥加密协议时，LU26 对秘密值 d 进行操作，以获得对应的公钥 D，公钥 D 被存储在存储器 28 中。

[0029] 存储器 28 还存储被标识为启用 (ENABLE) 和删除 (DELETE) 的密码对 40、42。计算机可读指令集或硬件状态机包括对认证设备 22 进行密码保护的例程或机制，以使得直到使用 ENABLE 密码，认证设备 22 才可操作。DELETE 密码被使用来产生将在下面描述的证明消息。如果具体的应用需要，可以逐设备地改变密码，或者针对一个批次或具体的 ADM，密钥可以是公共密码。

[0030] 在向认证设备 22 供给相应的密钥 d 之后，ADM 以安全的方式向 CC 发送标识信息 ID#。ADM 还将发送与密钥 d 有关的信息。当所使用的协议是对称密钥协议时，信息包括其密钥，密钥是使用多个可用密钥传输协议中的一个以安全方式向缔约公司发送的。当使用公钥协议时，认证设备 22 向 CC 转发从密钥 d 推导出的对应公钥 D。

[0031] CC 使用其私钥 c 来对包括标识（在适用的情况下，还包括公钥 D）的消息签名，以针对每个认证设备 22 提供设备证书 44。向缔约制造商 (CM) 转发要被贴附到对应认证设备 22 的设备证书 44。不向 ADM 发送设备证书 44，因此 ADM 在任何时候都不具有完整提供的认证设备 22，或创建一个认证设备的能力。

[0032] ADM 向具有密码保护能力的缔约制造商 CM 转发认证设备 22。通过这种方式，即使设备 22 未添加有设备证书 44，并因此具有很少的价值，其也不可操作并且阻止了偷窃。

[0033] 在接收到认证设备 22 时，缔约制造商 CM 应用密码 ENABLE 以激活认证设备 22 并贴附设备证书 44。然后将认证设备 22 固定到由缔约制造商 CM 提供或固定的组件 20（在本示例中是电池）。测试所完成的组件 20 以确保正确的性能，并向协定公司 CC 发送被接受的组件以与产品 10 合并。

[0034] 当将组件 20 装配到产品中时，使用设备证书 44 来认证组件 20。可以使用与缔约公司的签名密钥 c 相对应的公钥 C 来检验设备证书 44。在使用公钥协议的情况下，可以使用挑战响应协议来要求认证设备 22 使用密钥 d 签名随机消息。可以由产品 10 使用设备证书中包含的已认证的公钥 D 来检验已签名的消息。

[0035] 当然，可以使用一般用于认证组件的其他检验协议。

[0036] 在组件 20 测试失败的情况下，或者当缔约公司 CC 指示不需要其他组件 20 时，废弃认证设备 22 是有必要的，即，使其不能认证组件。CM 通过应用第二密码 DELETE 来发起废弃。在通过通信模块 32 接收密码 DELETE 时，LU26 从安全存储器 24 调用用于删除密钥 d 的操作集，并且准备涉及密钥 d 的证明消息 46。向缔约公司 CC 发送证明消息 46，以证明密钥 d 的销毁。当 CM 不具有对认证设备 22 的密钥的访问时，其不可以准备假冒的证明消息，并因此必须提供对每个认证设备的精确记账。

[0037] 取决于所实现的协议，可以通过多种不同的方式执行对证明消息的产生。

[0038] 图 5 中示出了使用对称密钥协议的第一示例。在接收到密码 DELETE 时，LU26 使用密钥 d 产生 MAC（消息认证码）。MAC 是使用密钥 d 作为密钥并使用密码作为消息的密钥加密 (keyed) 散列功能。备选地，消息可以是意在指示密钥 d 被删除的特定消息，并且可以包括设备特有的信息，例如 ID#。

[0039] 在产生 MAC 之后，LU26 从安全存储器 24 删除密钥 d。

[0040] 一旦删除了密钥，向缔约公司 CC 发送包括 MAC 的证明消息 46。缔约公司使用其对称密钥备份来检验 MAC，并在检验后接受认证设备 22 已被禁用。

[0041] 优选地，将标识信息和证明消息存储在认证设备 22 的存储器 28 中，以使得可以执行后续审计。然而，当删除密钥 d 时，不可使用认证设备 22 来认证产品 10。

[0042] 图 6 中示出了用于不对称协议的过程。在本实施例中，应用密码 DELETE，并且 LU 使用密钥 d 来对密码（或者特定消息）签名，以指示密钥的删除。在签名之后，从安全存储器 24 删除密钥 d，并向缔约公司 CC 转发包括签名的证明消息 46。缔约公司 CC 可以检验证明消息 46 中的签名以确认删除。备选地，第三方审计者可以使用设备证书来检验签名，并确认秘密被删除。

[0043] 可以使用除了签名之外的加密操作来产生证明消息 46。例如，CM 可以向认证设备 22 提供对共享秘密的贡献 (contribution)，并且认证设备 22 使用密钥 d 和来自 CM 的贡献来将密码与共享秘密合并，以获得证书消息 46。认证设备 22 可以使用密钥推导功能、加密散列法或者 MAC 来产生证明消息，可由缔约公司 CC 使用可公开获得的信息来检验证明消息。

[0044] 图 7 示出了使用椭圆曲线加密的不对称密钥协议的特定示例。加密系统使用在有限域上定义的椭圆曲线组。该组具有产生组的各项的产生点 G。通常附加地表示组操作，因此被用作私钥的整数 d 具有对应的公钥 D ＝ dG，该公钥是椭圆曲线上的点。

[0045] 如上所述向认证设备 22 提供整数 d，并且 LU 计算点乘 dG 以用作公钥 D，然后将公钥 D 存储在存储器 28 中。向缔约公司 CC 转发公钥 D，缔约公司 CC 使用其私钥 c 来签名公钥 D。签名担当了设备证书 44。优选地，将设备标识信息 ID# 包括在设备证书 44 中。从而，可以使用公钥 C ＝ cG 来检验设备证书，该公钥是由缔约公司 CC 公开的。

[0046] 将设备证书贴附到认证设备 22，并且如果设备通过测试过程，则使用设备证书和私钥来认证组件。

[0047] 如果要废弃设备，向认证设备 22 应用密码 DELETE。然后使用密码或其他消息作为输入来执行 ECDSA 签名协议。LU 使用随机数产生器 30 来获得会话私钥 k，产生对应的会话公钥 K ＝ kG，并将会话密钥 K 的 x 坐标转换为整数，以提供第一签名分量 r。

[0048] 然后，LU 以 1/k[h(m)+dr] 的形式计算第二签名分量 s，其中，m 是密钥或相关消息，以及 h(m) 是消息 m 的加密散列。

[0049] 在删除密钥 d 之后，将签名 (r,s) 返回缔约公司 CC，缔约公司 CC 可以使用已知的消息和公钥 D 以及签名 (r,s) 来检验签名。

[0050] 另一非常适合的椭圆曲线签名方法是在 ANSI/x9x9.92-1-2009 中采用的 ECPVS，认证设备 22 设备可以使用该方法来签名挑战密码。使用 ECPVS 的一个优点是其避免了 ECDSA 中所需的倒置，该倒置增加了认证设备的成本，并且是临时密钥 k 的潜在泄露点。

[0051] 还可以使用椭圆曲线协议而无需签名。例如，可以将废弃密码嵌入到曲线上的点C中。该示例要求ADM已经向CC安全地发送了不对称秘密d。点C将废弃密码嵌入其坐标中，例如作为C的x坐标Cx的前缀。废弃密码自身应该足够长，以使得CM不可通过CM将会知道C的离散对数的方式来合理地计算包括废弃密钥的点C。例如，如果使用160比特的椭圆曲线，对于适当选择的椭圆曲线参数，将80比特的废弃密钥嵌入到由G产生的循环组中的点C中并确定离散对数c对于CM来说在加密学上将是困难的。在删除d之后，认证设备将在然后返回dC或者可能返回f(dC,I)，其中，f()是确定函数，并且I是CC已知的其他信息。这是对废弃的公钥证明。优选地，针对f()使用消息认证码，例如使用dC作为密钥的HMAC。知道d的CC可以检查dC或f(dC,I)是否正确，并且从而可以检验认证设备产生了证明消息。

[0052] 另一可能性将CC(或其代理)的公钥S嵌入到认证设备中，其中，S = sG。在该情况下，证明消息是共享密钥K = dS = sD的函数，即，f(K,I)，其中，f()是决定函数，以及I是CC已知的其他信息，并通常包含标识认证设备的信息。在该示例中，CC将不需要知道设备私钥d。

[0053] 进一步的增强提供了对于具有私钥d的特定设备特定的废弃命令。第一可能性使用关于废弃命令的公钥签名，允许设备在废弃其秘密之前认证已知公钥的发送者。

[0054] 做为第二可能性，当个性化设备时，ADM计算$C_0 = (d^{-1} \bmod n)A$，其中，A是被识别为隐含认证设备将要执行来(在本情况下)准备废弃认证设备的特定动作的点。动作点A可以将特定的子串嵌入到其坐标之一中，并且该子串可以具有短的规范，例如，可以要求A的x坐标的上半部分是0。仔细选择A的形式以使得其不能确定A的离散对数很重要。

[0055] 为了废弃认证设备，CM现在将需要首先向认证设备应用C_0。认证设备(注意到$A = dC_0$具有特定形式)将进入废弃模式，在废弃模式中，下一个通信删除密钥。

[0056] 在废弃模式中，当向认证设备提供C时，认证设备将废弃私钥并提供证明。如果认证设备不处于废弃模式，废弃或者产生证明都将不执行。

[0057] 将显而易见的是，在以上各个示例中，使用密码来发起对用于认证对应者(correspondent)的秘密的删除，并且使用秘密来产生证明消息。

[0058] 虽然在电信设备的上下文中进行了描述，然而可以将认证设备与其他组件一起使用，以例如认证在飞机引擎中使用的轴承或者其他服务关键组件。

[0059] 虽然以上描述预期在测试之前附加设备证书，将意识到的是，可以在初始测试之后附加设备证书，由此降低包含有效证书的无功能最终产品的数目。然后，CC可以基于逐个证书计费来针对CM计量证书，以进一步阻止生产过剩。

[0060] 可能针对每个认证设备使用唯一的废弃密码，或者针对设备集(例如，在具体批次中产生或由具体ADM产生的设备)使用公共密码。针对每个设备使用唯一的密码要求由CM来对密码和设备认证信息进行相关和维护。

[0061] 还期望在向缔约公司提供组件之后禁用DELETE密码功能，以禁止无意间或者恶意地删除密钥d。

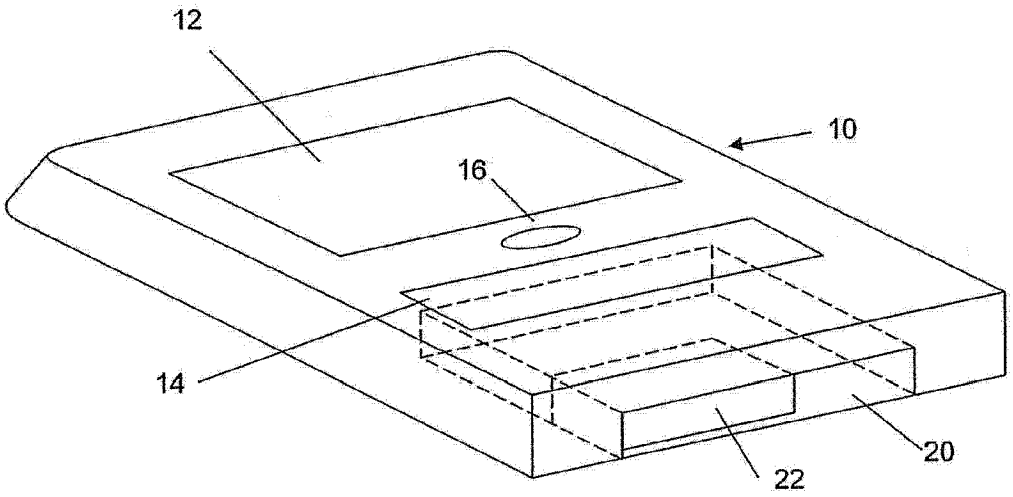

12
10
16
14
20
22

图 1

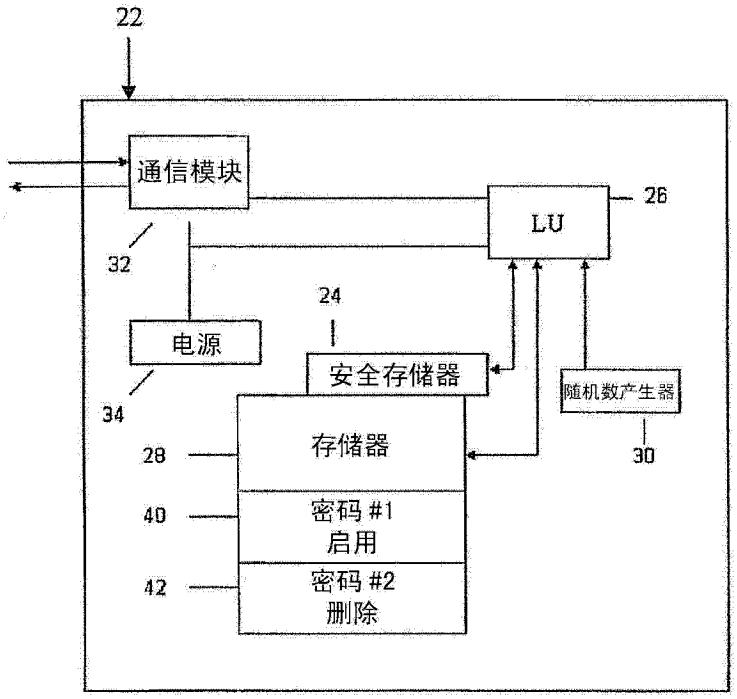

22
通信模块
LU
26
32
24
电源
安全存储器
随机数产生器
34
存储器
28
30
密码 #1
启用
40
密码 #2
删除
42

图 2

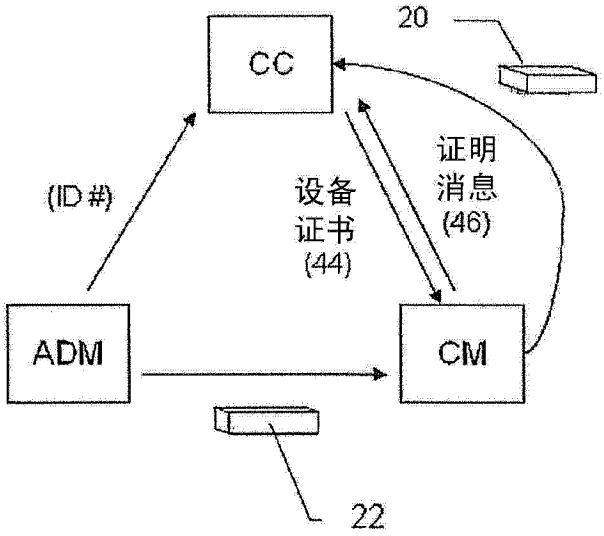


图 3

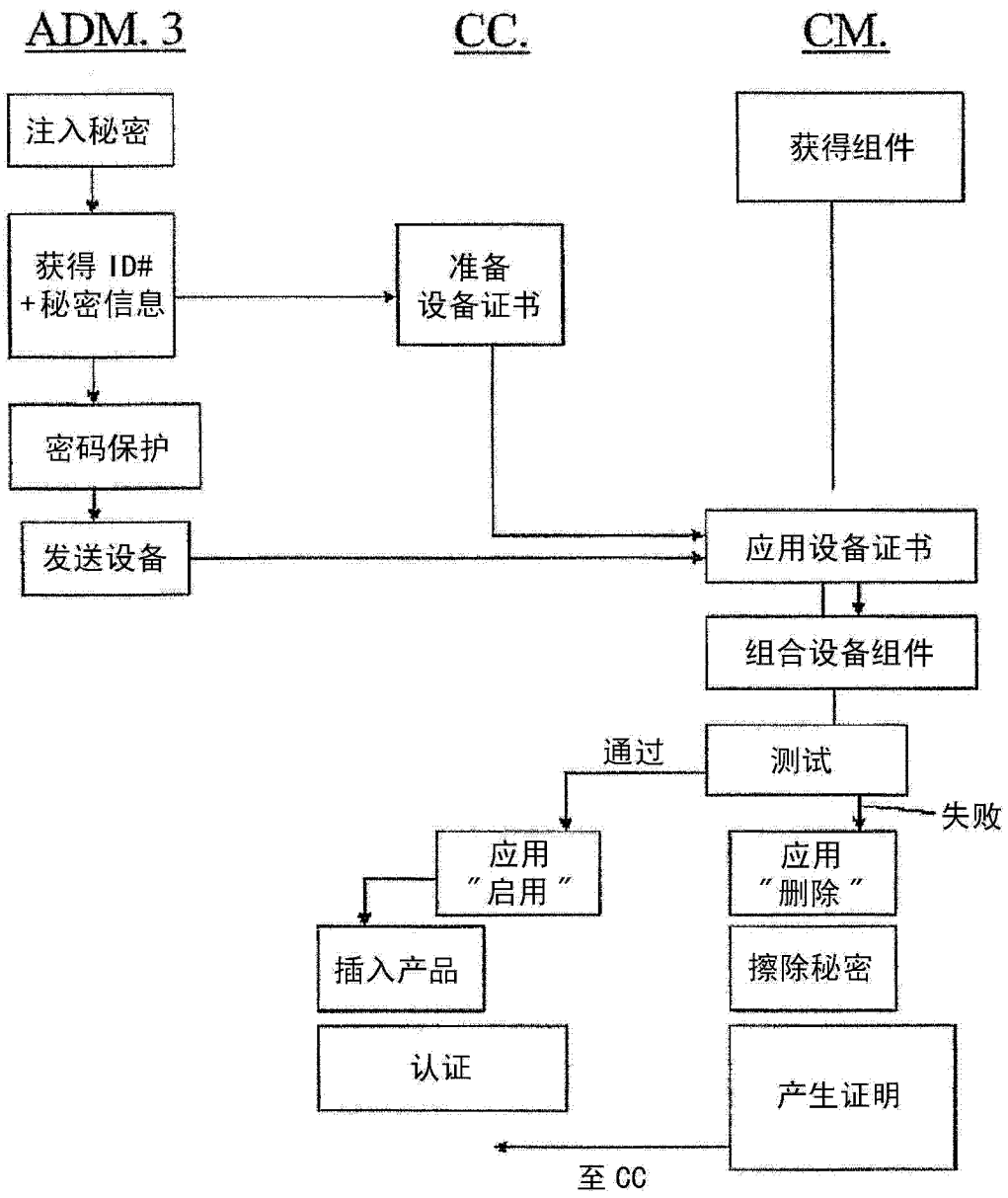

ADM. 3
CC.
CM.
注入秘密
获得 ID#
+秘密信息
密码保护
发送设备
准备
设备证书
获得组件
应用设备证书
组合设备组件
测试
通过
失败
应用
"启用"
应用
"删除"
插入产品
擦除秘密
认证
产生证明
至 CC

图 4

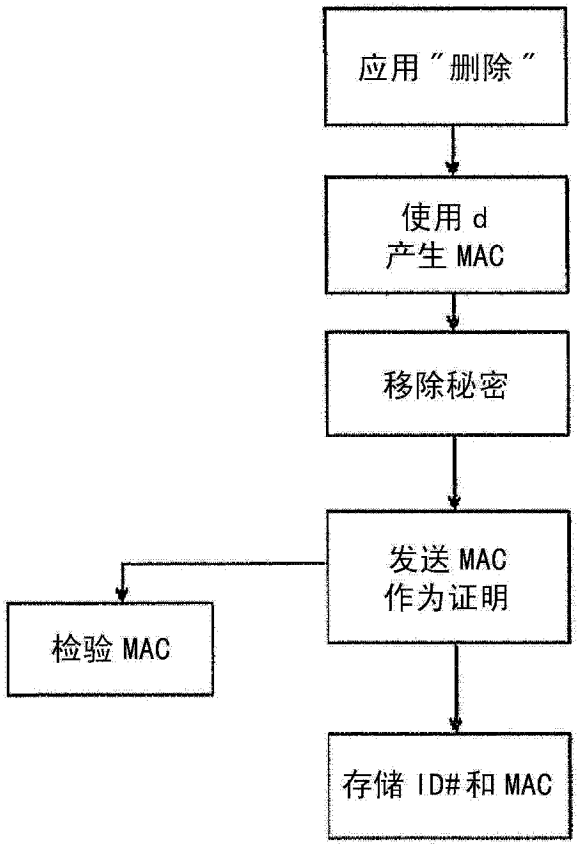


图 5

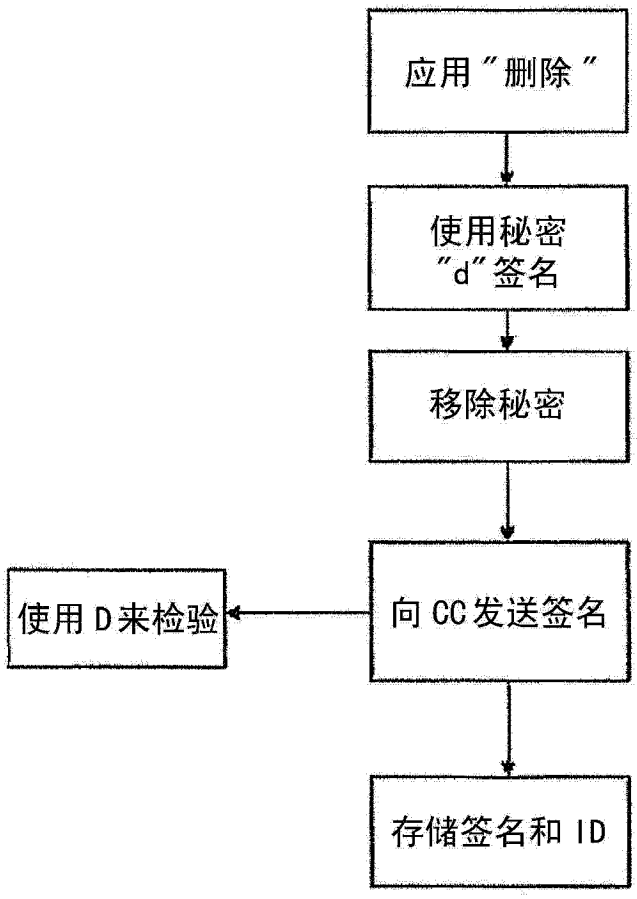


图 6

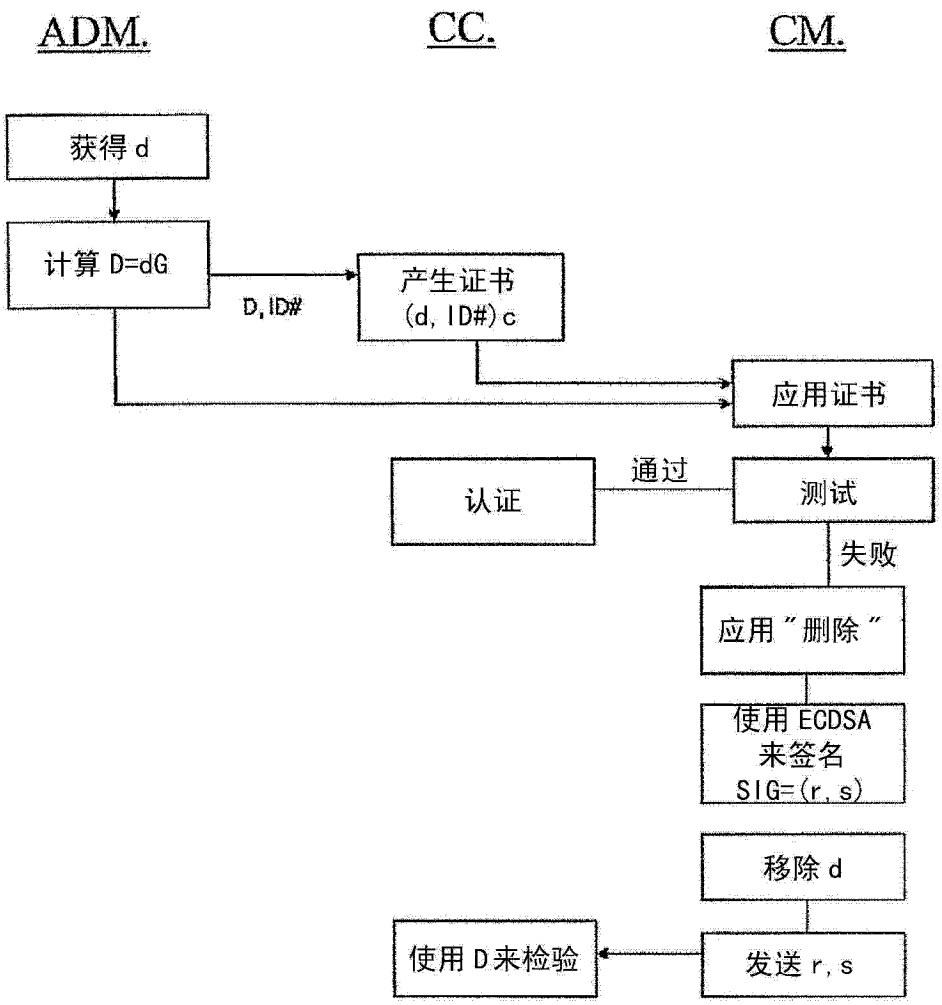

ADM.
CC.
CM.
获得 d
计算 D=dG
D,ID#
产生证书
(d, ID#)c
应用证书
认证
通过
测试
失败
应用"删除"
使用 ECDSA
来签名
SIG=(r, s)
移除 d
使用 D来检验
发送 r, s

图 7