[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200580035800.6

[45] 授权公告日 2009 年 2 月 4 日

[11] 授权公告号 CN 100458807C

[22] 申请日 2005.6.23
[21] 申请号 200580035800.6
[30] 优先权
[32] 2004.10.21 [33] US [31] 10/970,461
[86] 国际申请 PCT/EP2005/052937 2005.6.23
[87] 国际公布 WO2006/045644 英 2006.5.4
[85] 进入国家阶段日期 2007.4.19
[73] 专利权人 国际商业机器公司
地址 美国纽约
[72] 发明人 S·贝德 D·C·查利纳
[56] 参考文献
US2003/0188162A1 2003.10.2
US2003/0115453A1 2003.6.19
US2003/0056109A1 2003.3.20
US2003/0226040A1 2003.12.4

审查员 杜 军
[74] 专利代理机构 北京市中咨律师事务所
代理人 于 静 李 峥

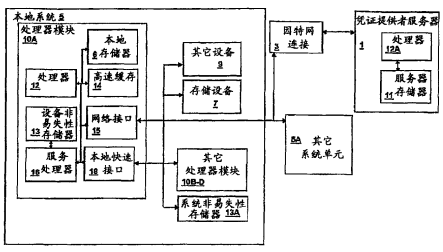
权利要求书 4 页 说明书 10 页 附图 5 页

[54] 发明名称

验证初始可信设备到被保护处理系统的绑定

[57] 摘要

一种用于验证初始可信设备到被保护处理系统的绑定的方法和系统，其绑定初始设备，或在没有任何来自所述系统中的另一设备的绑定信息可用时绑定替代。 仅当有效绑定被验证时，通过向例如制造商的凭证提供者发送绑定证明，平台凭证被发布。 所述方法防止了当设备在绑定过程中被从所述系统移除时可能发生的安全破坏。 所述绑定信息在设备安装时在设备中被生成，并且包括系统标识信息，以便在每次初始化时，当绑定信息从所述系统返回到所述设备时，所述设备可以确保其被安装到正确的系统中，并且如果所述系统不匹配则中止运转。



1. 一种保护处理系统的方法，所述处理系统包括多个设备，所述多个设备在初始化为运转状态前验证特定处理系统的身份，所述方法包括：使用由所述处理系统提供的系统特定标识符和仅对于所述设备中一个给定设备已知的第一私有信息，第一生成所述给定设备到所述处理系统的绑定；使用所述系统特定标识符、仅对于所述给定设备已知的第二私有信息以及唯一的设备标识符，第二生成对于所述绑定的证明；将所述证明从所述处理系统传送给凭证提供者；在所述凭证提供者处确定所述证明是否表明所述生成的绑定有效；以及响应于确定所述生成的绑定有效，发布所述处理系统的平台凭证。

2. 根据权利要求 1 所述的方法，其中所述第二私有信息包括所述第一私有信息。

3. 根据权利要求 1 所述的方法，还包括：响应于在所述凭证提供者处接收到所述证明，使所述处理系统的现有凭证无效。

4. 根据权利要求 1 所述的方法，还包括：将所述平台凭证传送给所述处理系统。

5. 根据权利要求 1 所述的方法，还包括：将所述平台凭证存储在服务器上，由此，所述处理系统的真实性和安全性可以通过访问所述服务器上的所述平台凭证被验证。

6. 根据权利要求 1 所述的方法，其中所述第一生成包括：用设备生成的随机值散列所述系统特定标识符，以产生已散列结果；用设备特定密钥签名所述已散列结果，以产生已签名结果；以及通过将所述已签名结果发送到所述处理系统的另一部分而将所述给定设备绑定到所述特定系统，由此，响应于所述已签名结果对所述给定设备的返回和验证，所述给定设备将仅在所述特定系统中初始化。

7. 根据权利要求 6 所述的方法，其中所述第二生成包括：散列至少所述系统特定标识符和唯一设备标识符的组合；以及用设备特定密钥签

名所述散列的结果，以产生已签名结果。

8. 根据权利要求 1 所述的方法，还包括：在实施所述绑定之前，将所述给定设备的状态设定为指示绑定过程正在进行；第二接收下述验证，即所述证明已由所述凭证提供者验证；仅响应于接收到所述验证，将所述状态设定为指示所述给定设备已绑定。

9. 根据权利要求 1 所述的方法，还包括：第二确定是否所述系统包括运转的可信设备；响应于确定所述系统不包括运转的可信设备，实施所述第一生成、第二生成、传送、接收、确定和发布。

10. 根据权利要求 1 所述的方法，还包括：在服务器处接收服务请求，该服务请求指示所述给定设备的前任已发生故障，并且其中，响应于在所述服务器处接收到所述服务请求，所述第二确定被实施；响应于确定所述系统不包括运转的可信设备，启动作为所述前任的替代的所述给定设备的运送；以及在所述服务器的数据库内生成关联于所述给定设备的服务记录。

11. 根据权利要求 10 所述的方法，其中所述确定是否所述生成的绑定有效依照存储在所述服务记录中的信息被实施，由此，作为所述被运送的设备的所述给定设备的身份在发布所述平台凭证之前被验证。

12. 一种保护处理系统的装置，所述处理系统包括多个设备，所述多个设备在初始化为运转状态前验证特定处理系统的身份，所述装置包括：

第一生成装置，用于使用由所述处理系统提供的系统特定标识符和仅对于所述设备中一个给定设备已知的第一私有信息，生成所述给定设备到所述处理系统的绑定；

第二生成装置，用于使用所述系统特定标识符、仅对于所述给定设备已知的第二私有信息以及唯一的设备标识符，生成对于所述绑定的证明；

传送装置，用于将所述证明从所述处理系统传送给凭证提供者；

确定装置，用于在所述凭证提供者处确定所述证明是否表明所述生成

的绑定有效；以及

发布装置，用于响应于确定所述生成的绑定有效，发布所述处理系统的平台凭证。

13. 根据权利要求 12 所述的装置，其中所述第二私有信息包括所述第一私有信息。

14. 根据权利要求 12 所述的装置，还包括：响应于在所述凭证提供者处接收到所述证明，用于使所述处理系统的现有凭证无效的装置。

15. 根据权利要求 12 所述的装置，还包括：用于将所述平台凭证传送给所述处理系统的装置。

16. 根据权利要求 12 所述的装置，还包括：用于将所述平台凭证存储在服务器上的装置，由此，所述处理系统的真实性和安全性可以通过访问所述服务器上的所述平台凭证被验证。

17. 根据权利要求 12 所述的装置，其中第一生成装置包括：用于利用设备生成的随机值散列所述系统特定标识符，以产生已散列结果的装置；用于利用设备特定密钥签名所述已散列结果，以产生已签名结果的装置；以及用于通过将所述已签名结果发送到所述处理系统的另一部分而将所述给定设备绑定到所述特定系统的装置，由此，响应于所述已签名结果对所述给定设备的返回和验证，所述给定设备将仅在所述特定系统中初始化。

18. 根据权利要求 17 所述的装置，其中第二生成装置包括：用于散列至少所述系统特定标识符和唯一设备标识符的组合的装置；以及用于利用设备特定密钥签名所述散列的结果，以产生已签名结果的装置。

19. 根据权利要求 12 所述的装置，还包括：用于在实施所述绑定之前，将所述给定设备的状态设定为指示绑定过程正在进行的装置；用于第二接收下述验证的装置，即所述证明已由所述凭证提供者验证；以及用于仅响应于接收到所述验证，将所述状态设定为指示所述给定设备已绑定的装置。

20. 根据权利要求 12 所述的装置，还包括：用于第二确定是否所述

系统包括运转的可信设备的装置；以及响应于确定所述系统不包括运转的可信设备，用于启动所述第一生成、第二生成、传送、确定和发布的装置。

21. 根据权利要求 12 所述的装置，还包括：用于在服务器处接收服务请求的装置，该服务请求指示所述给定设备的前任已发生故障，并且其中，响应于在所述服务器处接收到所述服务请求，启动所述第二确定装置；响应于确定所述系统不包括运转的可信设备，用于启动作为所述前任的替代的所述给定设备的运送的装置；以及用于在所述服务器的数据库内生成关联于所述给定设备的服务记录的装置。

22. 根据权利要求 21 所述的装置，其中所述确定是否所述生成的绑定有效依照存储在所述服务记录中的信息被实施，由此，作为所述被运送的设备的所述给定设备的身份在发布所述平台凭证之前被验证。

验证初始可信设备到被保护处理系统的绑定

技术领域

本发明一般涉及处理系统中的安全性，并且特别涉及用于将绑定信息安装到被保护处理系统中的初始或替代可信设备中的方法。

背景技术

现在的计算系统，并且特别是大型服务器系统通常包括对运行多个虚拟机的支持。所述系统可以是这样的大型按需服务器系统，所述系统在单一硬件平台上执行数百个服务器实例以支持具有可变计算需求的客户。在这些系统中最灵活的系统中，可能在操作系统和应用组合上不同的多个分区同时出现在系统存储器中，并且在每个分区中执行的过程在支持其在访客（guest）操作系统上的执行的环境中运行。所述虚拟机提供了足够类似于实际硬件平台的环境，以致所述操作系统通过很少或不进行任何修改就可以运行。管理程序（hypervisor）（有时称为虚拟机监视器）管理所述虚拟机或分区的全部并且提取系统资源，以便每个分区为每个操作系统实例提供类似于机器的环境。

为实现上述体系结构目标，多个处理模块和其它设备被安装到系统中，并且每个设备一般支持一个或更多个上面描述的分区，尽管也可以在多个设备之间共享一个分区上的任务分配。设备组或单个设备可以关联于特定客户，并且希望保护由仅该客户到设备或组的访问，其包括保护所述设备免于来自系统或设备的制造商的风险。

为提供所述系统中的安全性，设备必须被绑定到该系统，其避免了移除和数据挖掘，其中，所述移除和数据挖掘通过或者从设备提取数据或者使用设备“模拟”其从中被提取的系统或其一部分而可能发生。绑定可以

是物理的，即设备被永久附接到所述系统，或者绑定可以加密地被完成，其允许可移除设备和连网系统。仅当凭证提供者确定可信设备已被有效绑定到系统时，平台凭证才被发布到系统（或系统中的特定可信设备组）。所述凭证证明所述平台包含一个或更多可信设备，并且因此具有关联于其的属性。典型地，所述证明在制造商处被实施，并且所述可信设备或者被永久物理绑定到所述系统，或在没有字段替代可能性的情况下被加密地绑定到所述系统。

上面提到的可移除和连网设备通过除非该设备被加密地绑定到该系统则拒绝在系统中进行初始化来提供对数据篡改或模拟的预防。关联于所述绑定的信息一般被制造商加密并且存储在所述设备中的非易失性存储器中。通过使用上面描述的机制，仅可信系统可以访问关联于特定设备或被存储在特定设备中的数据，其显著减小了可移除设备被盗用或误用的影响。另外，关联于设备的数据（例如所存储的上面提到的虚拟机之一的语境或“状态”）通过这样的加密机制被保护，该加密机制需要存储在所述关联的一个或多个设备中的密钥。该两层机制：硬件绑定和针对特定的一个或多个设备的数据加密对由可移除设备的盗用或误用引起的数据挖掘提供了高安全级别。

当所述设备中的一个发生故障或在可信设备初始安装到系统中时，该新设备必须被绑定到该系统，以便该设备根据上面描述的安全方法初始化。如果具有所希望的安全绑定的其它设备出现并且运转在系统中，则绑定信息可以从所述其它设备中的一个被传输。然而，如果没有任何具有所希望的绑定的其它设备可用，即，具有所述绑定的最后一个设备已发生故障，或者最初仅一个所述设备出现在所述系统中，则所述绑定需要通过其它方法被建立，其典型是通过将所述系统返回给其制造商。

用于替代可信设备的字段替代机制导致系统对于未授权或已修改硬件的潜在的暴露。因此，希望所述替代技术至少像所述运转安全方案一样安全，其典型是同样要求所述设备返回给其制造商。

攻击具有绑定设备的系统的一种方法是在绑定过程中移除设备，或使

设备呈现为“未绑定”，并试图将该设备安装到另一系统上。同时，故障可能在所述绑定过程中发生，其通过导致设备在其并不受保护时对于特定平台显现为受保护的而可能危及系统的完整性。

因此，希望提供一种字段替代机制，其用于，当没有任何其它具有所希望的绑定的设备出现在系统中时，以安全的方式将替代设备绑定到系统。还希望提供一种当初始可信设备被安装和仅当该可信设备已知被有效绑定到该系统时对于平台的有效凭证。还希望提供一种安全绑定方法，该方法容许绑定过程中的故障或移除。

发明内容

本发明提供了一种保护处理系统的方法和相应的装置，所述处理系统包括多个设备，所述多个设备在初始化为运转状态前验证特定处理系统的身份。所述方法包括：使用由所述处理系统提供的系统特定标识符和仅对于所述设备中一个给定设备已知的第一私有信息，第一生成所述给定设备到所述处理系统的绑定；使用所述系统特定标识符、仅对于所述给定设备已知的第二私有信息以及唯一的设备标识符，第二生成对于所述绑定的证明；将所述证明从所述处理系统传送给凭证提供者；在所述凭证提供者处确定所述证明是否表明所述生成的绑定有效；以及响应于确定所述生成的绑定有效，发布所述处理系统的平台凭证。

附图说明

本发明阐述了被认为是新颖特征的本发明的特性。然而，通过在结合附图阅读时参考下面对说明性实施例的详细描述，本发明其自身以及优选的使用模式、另外的目的及优点将被最好地理解，在附图中类似标号指示类似部件，并且：

图 1 是在其中本发明的实施例被实现的计算系统的框图。

图 2 是在根据本发明的实施例的系统中的存储器图像和信息流的框图。

图 3 是描述根据本发明的实施例的方法的若干部分的流程图。

图 4 是描述根据本发明的实施例的方法的另若干部分的流程图。

图 5 是描述根据本发明的实施例的方法的又若干部分的流程图。

具体实施方式

现在参考附图，并且特别参考图 1，描述了在其中本发明的实施例可以被实现的系统的框图。应当理解，所描述的实施例并不用于限制，而仅

示例了本发明的方法和技术可以应用于的处理系统的类型。所述系统包括具有四个处理器模块（处理器模块 10A 和三个其它等同的处理器模块 10B-D）的被保护的本地系统 5。本地系统 5 可以被连接到构成超标量处理系统的其它系统单元 5A。所述本地系统被经由因特网连接 3 或可选网络接口连接到凭证提供者服务器 1。凭证提供者服务器包括：用于执行根据本发明的实施例的服务器程序指令的处理器 12A，和用于存储所述程序指令和数据的服务器存储器 11。

每个处理模块 10A、10B-D 包括用于执行程序指令的处理器 12、一般被映射为可被其它处理器模块 10B-D 访问的系统存储器的本地存储器 6，以及用于存储数据和程序指令的高速缓存 14。处理模块 10A、10B-D 还每个包括非易失性存储器 13，其中，该非易失性存储器存储被本发明的方法用于验证处理器模块 10A、10B-D 被安装在它们被绑定的系统中的值。处理器模块 10A、10B-D 还每个可包括服务处理器 16，其中，该服务处理器可以实现本发明的安全功能，或者可选地，处理器 12 可以实施下面详细描述的任务。处理器模块 10A、10B-D 还包括：用于与本地系统 5 中的其它模块互通的本地快速接口 18，以及用于与其它系统单元 5A 和因特网连接 3 通信的网络接口 15。本地系统还包括存储设备 7 以及其它设备 9，其中，本发明的绑定技术可以被应用于所述设备。系统非易失性存储器 13A 也被包括，其用于存储绑定验证数据以及关联于本发明的安全技术的其它系统值，例如系统序列号或其它标识符。

在系统本地存储器 6 中，虚拟机监视器程序或“管理程序”提供了对执行多个虚拟机（VM）或“分区”的支持，其中，所述多个虚拟机或“分区”的每个都提供了用于操作系统和大量“访客”程序（由操作系统执行并运行在相关联 VM 中的应用和服务）的执行环境。

为确保整个本地系统 5 的安全，以及在上面提到的分区可属于需要在所述分区之间的数据保护的不同客户的情况下使用本地系统 5 的多个客户之间的安全，本发明提供了本地系统 5 中的设备的绑定，以便所述设备仅可以在本地系统 5 中被使用。作为所述绑定过程的结果，凭证提供者服务

器 1 向本地系统 5 提供凭证，所述凭证向其它系统证明该系统包括一个或更多可信设备并且因此具有关联于所述可信设备的属性。所述证明可以因而被其它系统用于验证其可以使用关联于可信平台设备的特征与系统 5 互操作。上面描述的装置是适用于这样的系统的例子，在所述系统中，处理器模块 10A、10B-D 是可移除模块，其可以经由机架或其它互连装置被插入本地系统 5 或从本地系统 5 移除。然而，本发明意义上的绑定可以扩展到其它装置，例如在本地系统 5 和其它系统单元 5A 之间示出的连网互连。本发明使用加密和公钥/私钥对来保护设备之间的与绑定相关的通信，并且因此，在其中被绑定到系统的设备可能实际位于物理上完全不同的位置的环境中可以维持安全。

另外，应当理解，本发明的技术不仅应用于处理器模块，而且应用于下述任意设备，对于其唯一绑定到系统是有益的，并且其中凭证的验证是有益的。例如，计算机系统中的存储设备可以被绑定到该系统，以便其将仅通过该系统操作，并且，在应用或操作系统例程信任存储在该设备上的数据或信任该设备为数据的汇点（sink）之前，凭证可以响应于查询被提供。因此，应当理解，尽管下面的描述出于说明性目的而涉及处理器模块 10A 到本地系统 5 的绑定，其也可应用于其它设备和其它系统。

现在参考图 2，所示框图描述图 1 的计算机系统中的存储器图像和信息流。在设备非易失性存储器 13 中，设备特定标识符与在设备制造时被安装的唯一的设备特定密钥对一起被存储。

在所述绑定过程中，处理器模块 10A 生成随机比特序列（设备生成机密级（secret）），其中，所述设备然后用由本地系统 5 提供的系统特定标识符将该随机位序列从系统非易失性存储器 13A 散列到处理器模块 10A（或者可以由处理器模块 10A 直接从系统非易失性存储器 13A 访问）。所述散列的结果“平台绑定记录”（PBR）被存储在处理器模块 10A 的非易失性存储器 13 中，以便将来用于验证本地系统 5 是被唯一绑定到处理器模块 10A 的系统。对于处理器模块 10A 唯一的私钥被用于签名所述 PBR，并且已签名 PBR 被发送到本地系统 5，其中，其被存储在系统非易失性存储器

13A 中。由于仅处理器模块 10A 知道其唯一的私钥，处理器模块可以在随后把所述已签名 PBR 返回到处理器模块 10A 时验证本地系统 5 是其被绑定到的系统，因为所述已签名 PBR 上的签名证实该已签名 PBR 已由处理器模块 10A 生成。当从处理器模块 10A 接收到所述 PBR 时，本地系统 5 使用由处理器模块 10A 的制造商提供的系统唯一公钥验证该已签名 PBR，并且存储该已签名 PBR，以便返回给处理器模块 10A，以用于当管理程序认为必要时在初始化和其它间隔时进行验证。

同样在所述绑定过程中，绑定验证记录被发送到凭证提供者服务器 1，其验证系统/设备组合是有效的并且现在被正确地绑定。所述绑定验证记录使用从数据库 22 检索的设备特定公钥来验证，其中，数据库 22 经由设备标识符和系统标识符进行索引。所述绑定验证记录通过包括可以仅在该设备内存在的各种信息而提供了特定设备被绑定到系统的证据。在所示的实施例中，这通过使用设备特定私钥签名几条信息的散列来实施，其中，所述信息包括设备特定公共签注密钥、在所述绑定过程中被提供的系统标识符以及唯一的设备标识符（一般为序列号）。在签名之前，上述信息基于一次使用设备机密级（不同于所述一次设备生成机密级）进行散列，其中，所述一次使用设备机密级在所述设备制造时被安装。所述一次使用设备机密级然后在所述绑定验证记录被生成之后“烧毁”（擦除）。该一次机密级还被存储在制造商的（凭证提供者的）数据库中，其提供了对所述设备已被绑定的验证。所述验证仅可以被实施一次，因为一旦所述设备已烧毁所述一次使用机密级，则如果下面描述的其它单向棘轮（ratchet）被克服，在没有依照所述一次使用设备机密级生成绑定验证记录的情况下，所述设备的绑定仍然无法被验证。

所述设备特定签注密钥对于初始可信设备也是唯一的，并且提供了对所述设备所绑定的是正确设备的进一步验证，因为所述签注密钥还由凭证提供者保留。所述签注密钥关联于所述凭证，并且随后被用于表明所述可信平台虚拟机正运行在关联于特定凭证（其将也包含所述签注密钥）的可信平台设备上。

数据库 22 维持所产生的用于所有设备的公钥信息，以便密钥可以被找到用于证实来自设备的消息以及所述设备一次使用机密级。如果所述绑定被证实，则凭证 20 被生成，并被发送到处理器模块 10A，该模块将其存储在设备非易失性存储器 13（其可以包括磁盘文件存储器）中，以用于将由处理器模块 10A 提供的平台标识为可信平台，其中，所述可信平台具有被凭证提供者（例如制造商或其它证明实体）证明的身份。

由于所述的唯一私钥仅被存储在处理器模块 10A 中，并且在该私钥在工厂被注入处理器模块 10A 中之后不被制造商保留，也不被存储在其它任何地方，所以另一设备在绑定过程中模拟处理器模块 10A 极其困难。因此凭证将被发布到除已知系统和已知设备集合外的设备和系统的任意组合的情形极不可能。除上述以外的其它技术可以被应用以便进一步增加其难度。

现在参考图 3，根据所示出的本发明的实施例的方法的一部分被描述。当未绑定设备被安装到（或耦合到）系统中（步骤 30）时，如果系统中存在另一可信设备（判决 31），则整合过程通过从另一可信设备迁移绑定信息被实施（步骤 32）。实质上，所述整合安全地共享被存储在另一设备中的散列结果（PBR），并且将其存储在所述未绑定设备的非易失性存储器 13 中，该未绑定设备可以然后通过用其自己的私钥签名来自另一设备的 PBR 而向本地系统 5 返回已签名 PBR，以存储在系统非易失性存储器 13A 中。当本地系统 5 在初始化时将所述已签名 PBR 发送到新被绑定的设备时，该新被绑定的设备可以与现有可信设备一样地验证所述系统。应当指出，每个设备的唯一私钥不需要被输出，而仅输出在现有可信设备的绑定期间被生成的散列值。

然而，如果系统中不存在任何其它可信设备（判决 31），则本发明的方法被用于在不实施步骤 32 的整合过程的情况下绑定该新设备。首先，例如系统序列号的系统特定标识符被发送到该设备（步骤 33）。该设备生成被用作机密级值的随机比特流，并且用所述系统特定标识符散列该值以产生散列结果（PBR）（步骤 34）。该设备存储所述 PBR，并且然后用该设备的唯一私钥签名所述散列结果以提供已签名 PBR（步骤 36），该已签名 PBR

然后被发送到所述系统，以在每个设备初始化时使用。

绑定的证明也被生成，并被与所述系统标识符一起发送到凭证提供者（步骤 37）。凭证提供者通过把系统和设备的身份验证为绑定的已签名证明中的签名而确定该绑定是否有效（判决 38）。凭证提供者具有每个设备的公钥，其中，所述公钥被用于证实绑定记录的已签名证明，以及验证其来自该特定设备。由于系统标识符也是绑定的已签名证明的基础的一部分，所以系统的身份也由此被标识，即使所述设备和系统标识符也可以被“明文地”发送。

如果所述绑定有效（判决 38），则该设备的凭证被发布，并且被发送回系统（步骤 39），以便系统可以证明其包含可信设备。然而，如上面所说明的，凭证不必非要被发送到系统，并且可以被维持在凭证提供者服务器上或存储在另一位置，只要其对于需要验证系统包含具有特定属性的可信设备的部件是可访问的即可。但是，如果所述绑定无效（判决 38），则该设备被通知中止所述绑定过程（步骤 40）。

现在参考图 4，根据所示出的本发明的实施例的方法的另一部分被描述。当设备被安装到系统中（步骤 50）时，状态值被从所述设备非易失性存储器读取（步骤 51）。三个状态是可能的：“已绑定”、“未绑定”和“正在绑定”。所述三个状态被用于单向“棘轮”方案中，其中，所述单向“棘轮”方案确保一旦所述绑定过程在设备上开始，该设备就无法返回未绑定状态，以及，一旦绑定被完成，该设备就无法从已绑定状况返回。

当设备被安装时如果该设备在“正在绑定”状态下（判决 51），则其表明，绑定过程以某种方式被中断，以及表明，在另一绑定过程中，通过移除该设备，篡改可能已发生。因此，如果该设备当安装时在正在绑定状态下（判决 51），则该设备被系统封锁（步骤 52），并且必须被返回给制造商以便重新使用。如果该设备在“已绑定”状态下（判决 53），则所述绑定被正常地验证（步骤 54），并且该设备被初始化。如果该设备在“未绑定”状态下（判决 53），则所述绑定交换和验证被实施（步骤 55），如由图 3 所示例的那样。如果所述绑定成功（判决 56），则该设备的状态被设定为

“已绑定”状态（步骤57），否则该设备被保持在“正在绑定”状态下（步骤 58），其防止了对该设备的进一步使用。由此，如果所述绑定过程中的任一点被中断，则该设备直到在工厂被重新编程之前都将被呈现为无用的，其防止了在安装期间通过移除而破坏所述绑定过程的企图。

现在参考图 5，根据所示出的本发明的实施例的方法的又一部分被描述。当可信设备的故障发生时，服务呼叫被制造商接收到（步骤 60）。如果所述系统还剩有一个运转可信设备（判决 61），则上面提到的整合过程通过使用该可信设备在替代设备上被实施（步骤 62）。然而，如果所述系统中不剩任何可信设备在运转（判决61），则使该系统凭证无效（步骤63），并且替代设备被可选地预绑定到发送所述服务呼叫的系统（步骤 64），并且该替代设备被运送到客户处（步骤 65）。一旦所述替代设备被安装到系统中，则上面描述的所述绑定过程被实施，如图 3 和 4 中所示的那样。如果所述设备在运送之前被预绑定到所述系统，则由凭证提供者服务器进行的绑定验证依照这样的数据库条目进行，其中，所述数据库条目表明所述替代设备准备安装在特定系统中，并且将仅在该设备绑定到正确系统时发布凭证。所述数据库包含这样的信息，例如设备标识符、该设备被分配到的系统标识符、以及关联于该系统和该设备的唯一公钥。

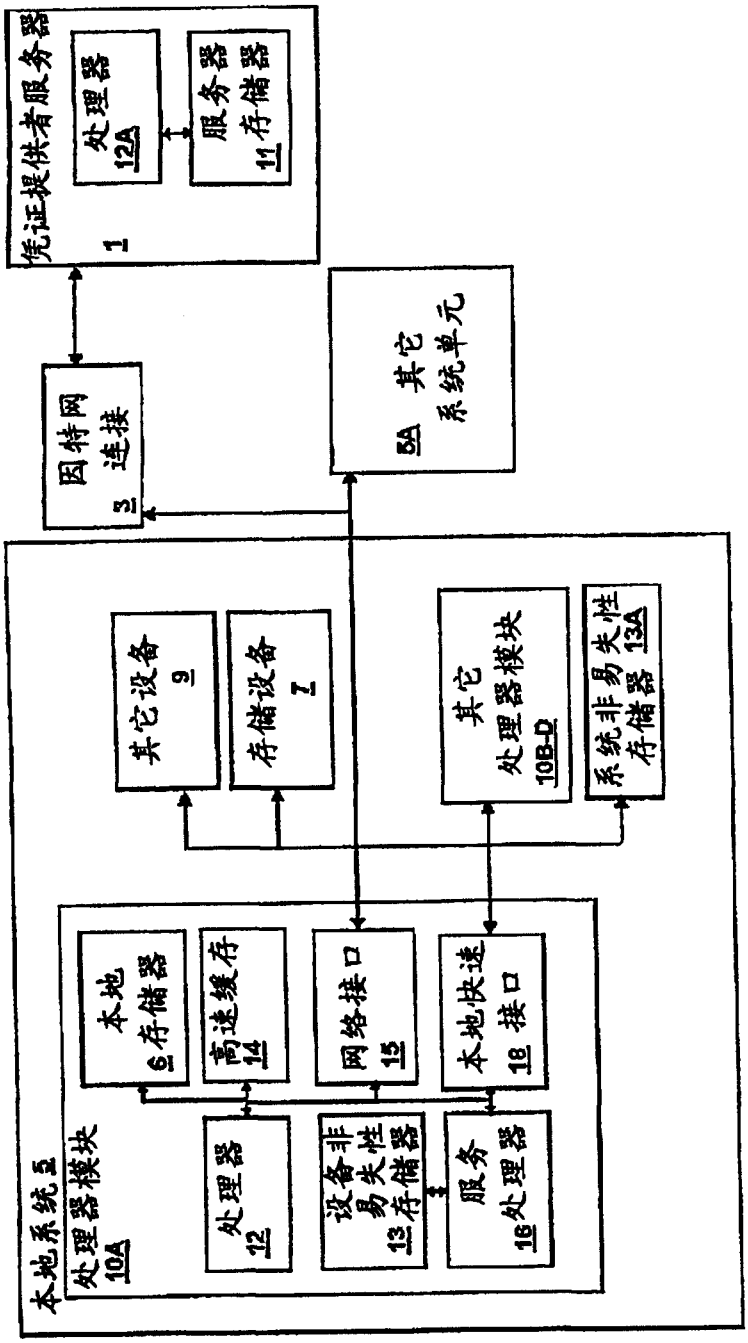

凭证提供者服务器
处理器 12A
服务器存储器 11
1
因特网连接 3
5A 其它系统单元
本地系统 5
处理器模块 10A
本地存储器 6
高速缓存 14
网络接口 15
本地快速接口 18
处理器 12
设备非易失性存储器 13
服务处理器 16
其它设备 9
存储设备 7
其它处理器模块 10B-D
系统非易失性存储器 13A

图 1

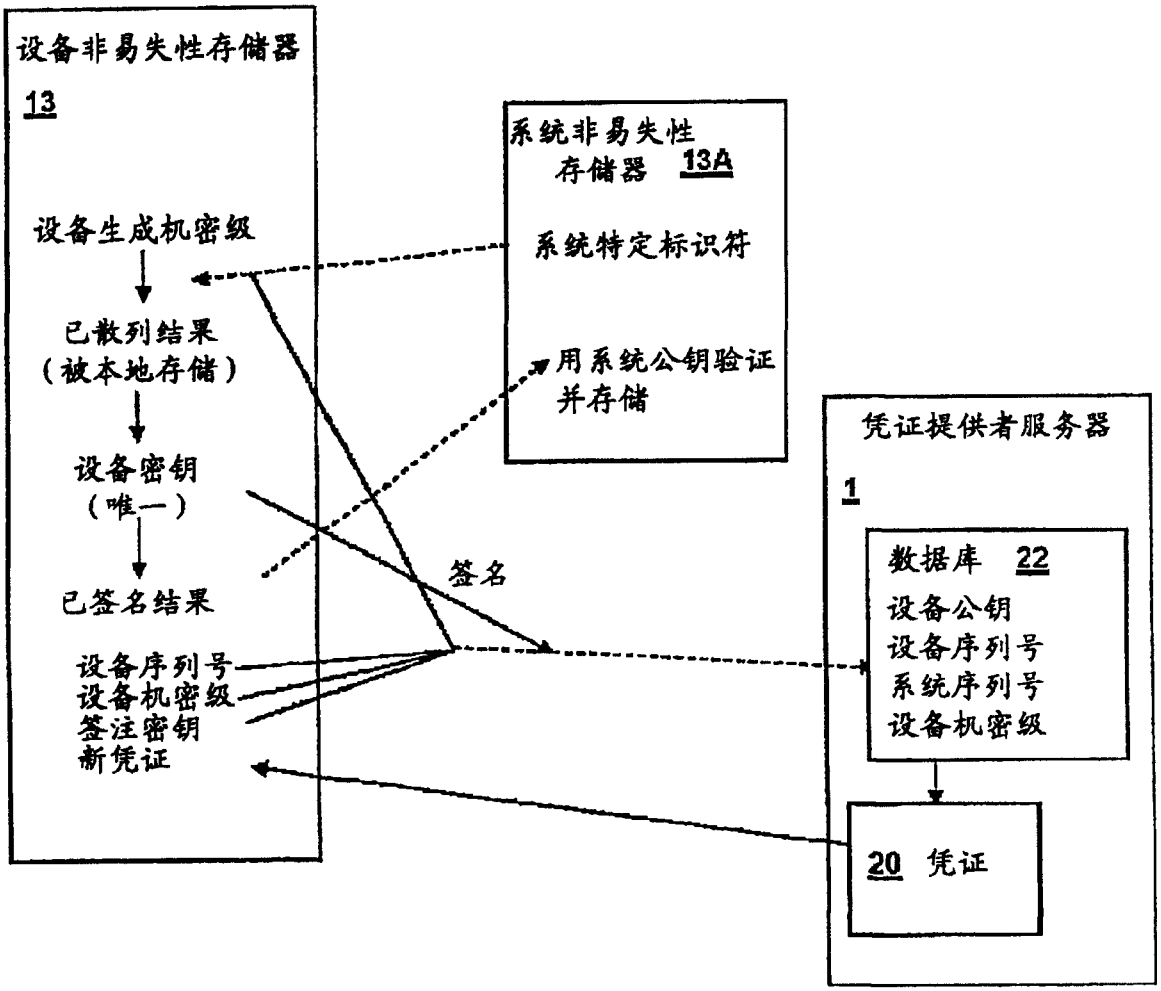

设备非易失性存储器
13
设备生成机密级
已散列结果
（被本地存储）
设备密钥
（唯一）
已签名结果
设备序列号
设备机密级
签注密钥
新凭证
系统非易失性
存储器 13A
系统特定标识符
用系统公钥验证
并存储
签名
凭证提供者服务器
1
数据库 22
设备公钥
设备序列号
系统序列号
设备机密级
20 凭证

图 2

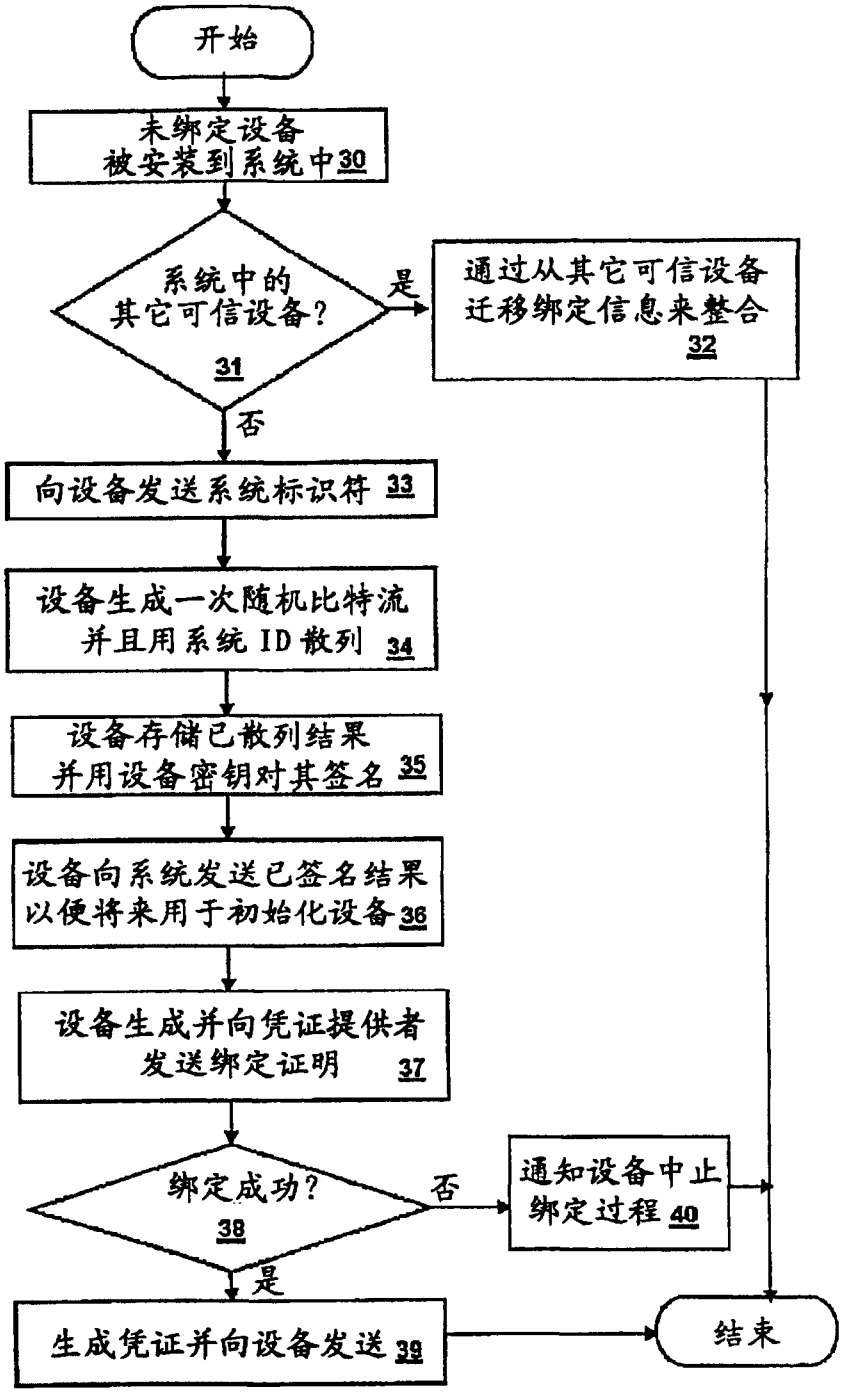

开始
未绑定设备
被安装到系统中30
系统中的
其它可信设备?
31
是
通过从其它可信设备
迁移绑定信息来整合
32
否
向设备发送系统标识符 33
设备生成一次随机比特流
并且用系统 ID 散列 34
设备存储已散列结果
并用设备密钥对其签名 35
设备向系统发送已签名结果
以便将来用于初始化设备36
设备生成并向凭证提供者
发送绑定证明 37
绑定成功?
38
否
通知设备中止
绑定过程 40
是
生成凭证并向设备发送 39
结束

图 3

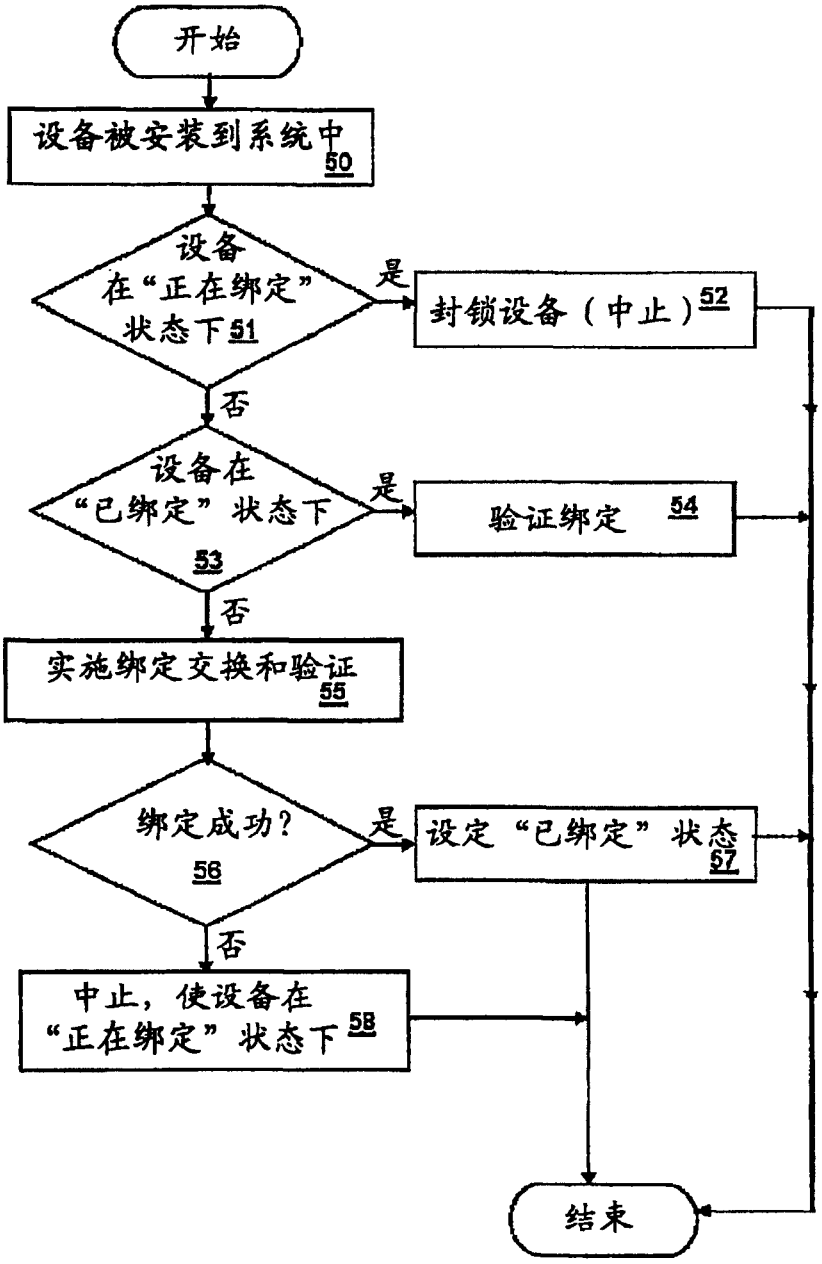

开始
设备被安装到系统中 50
设备在“正在绑定”状态下 51
是
封锁设备（中止） 52
否
设备在“已绑定”状态下 53
是
验证绑定 54
否
实施绑定交换和验证 55
绑定成功？ 56
是
设定“已绑定”状态 57
否
中止，使设备在“正在绑定”状态下 58
结束

图 4

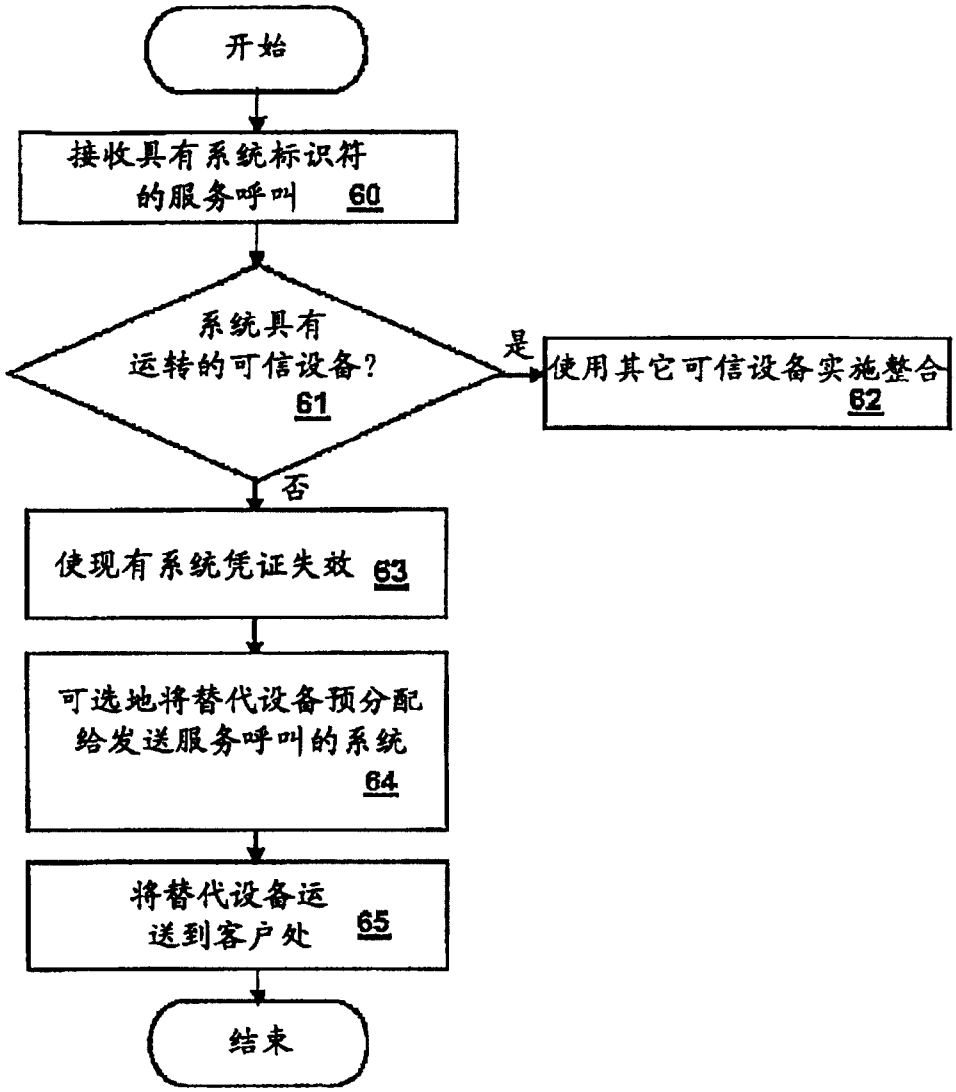

开始
接收具有系统标识符的服务呼叫 60
系统具有运转的可信设备? 61
是
使用其它可信设备实施整合 62
否
使现有系统凭证失效 63
可选地将替代设备预分配给发送服务呼叫的系统 64
将替代设备运送到客户处 65
结束

图 5